

UFFICIO	Indice trattamento	Misure informatiche
Ambiente - Trasporti	Scheda n. 14_ac - Ambiente/Trasporti - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di tariffe agevolate	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative</p> <p>- MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p>
Ambiente - Trasporti	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Ambiente - Trasporti	autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente - MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative - MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
Anagrafe - Leva	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente - MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative - MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
		- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

UFFICIO	Indice trattamento	Misure informatiche
Anagrafe - Leva	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attività relativa all'elettorato attivo e passivo	<div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Anziani ed adulti con disagio	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attività di assistenza domiciliare	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>

UFFICIO	Indice trattamento	Misure informatiche
Anziani ed adulti con disagio	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' digestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Anziani ed adulti con disagio	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti,	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
	pluriminorati o gravi disabili o con disagi psico-sociali)	<div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Anziani ed adulti con disagio	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Anziani ed adulti con disagio	Scheda n. 50 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Asilo Nido	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Biblioteca	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Biblioteca	Scheda n. 23 - Istruzione e cultura - Trattamento di dati relativi alla gestione delle biblioteche e dei centri di documentazione	<div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Biblioteca	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Centro Elaborazione Dati	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attività di gestione hardware, software, server, personal computer clients, rete	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>test LL</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Contratti	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalità di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Contratti	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attività contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Cultura	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Cultura	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attività ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	<p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Economato	Scheda n. 50 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Edilizia Privata	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Edilizia Privata	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Elettorale	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
	Scheda n. 06 - Servizi	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Elettorale	demografici/Elettorale - Trattamento di dati relativi all'attività di tenuta degli albi degli scrutatori e dei presidenti di seggio	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Elettorale	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attività di tenuta dell'elenco dei giudici popolari	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>

UFFICIO	Indice trattamento	Misure informatiche
Famiglie	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Giovani	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
	Occupazioni di ruolo pubblico	<div><div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità' operativa dei servizi informativi e continuità' della disponibilità' di informazioni costantemente aggiornate</div><div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div><div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div><div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div><div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità' (RID) , agevolare le attività' di operation e soddisfare le crescenti disponibilità' elaborative</div><div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div></div>
Manutenzioni	Scheda n. 01 - Personale/Trattamento di dati relativi all'attività' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	<div><div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div><div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div><div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div><div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità' operativa dei servizi informativi e continuità' della disponibilità' di informazioni costantemente aggiornate</div><div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div><div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div><div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div><div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità' (RID) , agevolare le attività' di operation e soddisfare le crescenti disponibilità' elaborative</div><div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div></div>
		<div><div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div></div>

UFFICIO	Indice trattamento	Misure informatiche
Manutenzioni	Scheda n. 42 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di controllo, di ispezione, comprese le attività di validazione dei progetti e di sopralluogo	<p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Manutenzioni	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attività di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarietà)	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Manutenzioni	Scheda n. 64 - Tutti gli uffici - Attività trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p>

UFFICIO	Indice trattamento	Misure informatiche
		- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
Minori e persone diversamente abili	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Minori e persone diversamente abili	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audilesi, non vedenti,	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
	pluriminorati o gravi disabili o con disagi psico-sociali)	<div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Minori e persone diversamente abili	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Museo	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attività di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarietà')	<p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Opere e Lavori pubblici	Scheda n. 42 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di controllo, di ispezione, comprese le attività di validazione dei progetti e di sopralluogo	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Opere e Lavori pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Opere e Lavori pubblici	Scheda n. 45 - Segreteria e tutti gli Uffici-Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento di	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Opere e Lavori pubblici	progettazione, ammdamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Opere e Lavori pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Partecipazioni	Nessun trattamento - Assenza dati personali da trattare	

UFFICIO	Indice trattamento	Misure informatiche
Partecipazioni	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attività di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza</p> <p>- MS-ICT-10 - CONTRASSEGNO: funzionalità di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, così da sopperire a bisogni di manutenzione e accresciute disponibilità elaborative</p> <p>- MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di fault e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato</p>
Patrimonio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attività di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarietà)	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Patrimonio	Scheda n. 45 - Segreteria e tutti gli Uffici- Attività trasversale - Trattamento di dati relativi all'attività di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p>

UFFICIO	Indice trattamento	Misure informatiche
	amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente - MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative - MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
Patrimonio	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate - ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente - MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative - MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
		- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare) - ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

UFFICIO	Indice trattamento	Misure informatiche
Piano diritto allo Studio e programmazione	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	<div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Piano diritto allo Studio e programmazione	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div>

UFFICIO	Indice trattamento	Misure informatiche
		- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
Piano diritto allo Studio e programmazione	Scheda n. 50 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Polizia cimiteriale	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
		<p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Polizia cimiteriale	Scheda n. 64 - Tutti gli uffici - Attività trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Polizia giudiziaria	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attività di polizia annonaria, commerciale ed amministrativa	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Polizia giudiziaria	Trattamento dati relativo ad attivita' d'indagine di Polizia Giudiziaria e comunicazione di notizie di reato inoltrate all'Autorita' Giudiziaria	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Polizia locale	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	<p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Polizia locale	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p>

UFFICIO	Indice trattamento	Misure informatiche
		<p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Polizia locale	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
		<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Polizia stradale	Scheda n. 24 - Polizia municipale - Trattamento di dati relativi all'infortunistica stradale	<p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Polizia stradale	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attività di polizia annonaria, commerciale ed amministrativa	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p>

UFFICIO	Indice trattamento	Misure informatiche
		- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
Polizia stradale	Scheda n. 28 - Polizia municipale - Trattamento di dati relativi all'attività di rilascio di permessi per invalidi	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Polizia stradale	Scheda n. 42 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di controllo, di ispezione, comprese le attività di validazione dei progetti e di sopralluogo	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
	progetti di amministrazione	<div><div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div><div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div><div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div><div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div><div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div><div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div></div>
Polizia stradale	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attività di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	<div><div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div><div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div><div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div><div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div><div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div><div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div><div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div><div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div><div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div><div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div></div>
		<div><div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div></div>

UFFICIO	Indice trattamento	Misure informatiche
Polizia stradale	Scheda n. 50 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Polizia stradale	Scheda n. 64 - Tutti gli uffici - Attività trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
		<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Prevenzione della corruzione e illegalita'	Scheda n. 45 - Segreteria e tutti gli Uffici-Attività trasversale - Trattamento di dati relativi all'attività di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	<div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Prevenzione della corruzione e illegalita'	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalità (Obbligo di DPIA)	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Programmazione e pianificazione	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Protezione Civile	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
	Scheda n. 45 - Segreteria e tutti gli Uffici-	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Protezione Civile	Attività' trasversale - Trattamento di dati relativi all'attività' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	<div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attività' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Protezione Civile	Scheda n. 50 - Tutti gli uffici/Attività' trasversale - Trattamento di dati relativi all'attività' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attività' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Protocollo e Archivio - Notifiche	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attività di protocollo e archiviazione	<p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di rimodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Qualità e innovazione	Scheda n. 45 - Segreteria e tutti gli Uffici- Attività trasversale - Trattamento di dati relativi all'attività di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p>

UFFICIO	Indice trattamento	Misure informatiche
		<p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Segreteria	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
	Scheda n. 32 - Trattamento di dati relativi	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Segreteria	agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Segreteria	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>

UFFICIO	Indice trattamento	Misure informatiche
Segreteria	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Segreteria Sindaco	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Segreteria Sindaco	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Servizi Vari	Scheda n. 13 - Servizi sociali - Trattamento di dati relativi all'attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	<p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Servizi Vari	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attività di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audilesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p>

UFFICIO	Indice trattamento	Misure informatiche
		<p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Servizi Vari	Scheda n. 45 - Segreteria e tutti gli Uffici-Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Servizi Vari	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, inclusa la prevenzione	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Sindaco	protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici-Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Sindaco	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento (Obbligo DPIA)	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Sindaco	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Sport e tempo libero	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attività trasversale - Trattamento di dati relativi all'attività di conferimento di onorificenze e ricompense nonché concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	<div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riaménagemento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Sport e tempo libero	Scheda n. 50 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Sportello unico per le attivita' produttive	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Statistica e Toponomastica	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	<div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Statistica e Toponomastica	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>

UFFICIO	Indice trattamento	Misure informatiche
Stato civile	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivit� di gestione dei registri di stato civile	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilit� di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilit� (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cos� da consentirne il ripristino in caso di necessit� (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrit� delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuit� operativa dei servizi informativi e continuit� della disponibilit� di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessit�, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalit� di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilit� (RID) , agevolare le attivit� di operation e soddisfare le crescenti disponibilit� elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Stato civile	Scheda n. 64 - Tutti gli uffici - Attivit� trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cos� da consentirne il ripristino in caso di necessit� (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessit�, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalit� di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilit� (RID) , agevolare le attivit� di operation e soddisfare le crescenti disponibilit� elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
		<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Trasparenza e Web	Scheda n. 50 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Trasparenza e Web	Scheda n. 56 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
		<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Tutti gli uffici - Attivita' trasversale	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	<p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Tutti gli uffici - Attivita' trasversale	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Tutti gli uffici - Attivita' trasversale	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita' (Obbligo di DPIA)	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Tutti gli uffici - Attivita' trasversale	transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento (Obbligo DPIA)	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Tutti gli uffici - Attivita' trasversale	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>

UFFICIO	Indice trattamento	Misure informatiche
Tutti gli uffici - Attività trasversale	Scheda n. 51 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Tutti gli uffici - Attività trasversale	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all'attività di tenuta dell'albo e delle notifiche dell'Ente	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
		<p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Ufficio amministrativo	Scheda n. 24 - Polizia municipale - Trattamento di dati relativi all'infortunistica stradale	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
		<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Ufficio amministrativo	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	<p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Ufficio amministrativo	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p>

UFFICIO	Indice trattamento	Misure informatiche
		<p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Ufficio amministrativo	Scheda n. 28 - Polizia municipale - Trattamento di dati relativi all'attivita' di rilascio di permessi per invalidi	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-09 - DISCIPLINARE TECNICO: tutte le misure minime di sicurezza prescritte per i trattamenti con strumenti elettronici dal disciplinare tecnico allegato B al D.Lgs. 196/2003, incluse le misure di tutela e di garanzia nei confronti dei soggetti esterni alla struttura organizzativa del titolare che effettuano interventi relativi alla adozione di misure di sicurezza</p> <p>- MS-ICT-10 - CONTRASSEGNO: funzionalita' di contrassegnare i dati in attesa di determinazioni ulteriori, prevedendo nei sistemi informativi elettronici, e al fine di garantire il diritto alla limitazione, la relativa funzione</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>- MS-ICT-12 - Piano di riammodernamento del parco macchine con particolare riferimento alla Server Farm, cosi' da sopperire a bisogni di manutenzione e accresciute disponibilita' elaborative</p> <p>- MS-ICT-13 - Realizzazione di ambienti di recovery virtuali per tutti i sistemi critici in caso di minimizzare il tempo di fermo operativo in caso di faul e realizzazione, per ogni sistema, di una 'tabella di marcia' con tipo e tempo di ripristino a seguito di fermo accidentale o programmato</p>
		<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Ufficio amministrativo	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attività di consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione	<div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Ufficio amministrativo	Scheda n. 50 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Ufficio amministrativo	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Ufficio amministrativo	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Ufficio Gestione economica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div>

UFFICIO	Indice trattamento	Misure informatiche
		<p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Ufficio Gestione economica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
		<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
Ufficio Gestione economica del personale dipendente	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attività di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	<div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attività di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità', volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div>

UFFICIO	Indice trattamento	Misure informatiche
		- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault
Ufficio gestione giuridica del personale dipendente	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Ufficio gestione giuridica del personale dipendente	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
		<div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuita' operativa dei servizi informativi e continuita' della disponibilita' di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Ufficio per le relazioni con il pubblico	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Ufficio per le relazioni con il pubblico	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessita', volta a limitare e/o a mininizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalita' di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilita' (RID) , agevolare le attivita' di operation e soddisfare le crescenti disponibilita' elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi	<div>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilita' di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</div>

UFFICIO	Indice trattamento	Misure informatiche
Ufficio stampa	all'attività di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	<p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Ufficio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>

UFFICIO	Indice trattamento	Misure informatiche
Ufficio Tributi	Scheda n. 42 - Tutti gli uffici/Attività trasversale - Trattamento di dati relativi all'attività di controllo, di ispezione, comprese le attività di validazione dei progetti e di sopralluogo	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</p> <p>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</p> <p>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</p> <p>- MS-ICT-CDB-12 - Fasi di riammodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</p> <p>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</p>
Ufficio Tributi	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attività di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a	<p>- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 03 (CSC 3) - proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server: istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare)</p> <p>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</p>

UFFICIO	Indice trattamento	Misure informatiche
	persone fisiche	<div>- ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- MS-ICT-11 - Piano di disaster recovery avente lo scopo di garantire il business continuity, da intendersi come continuità operativa dei servizi informativi e continuità della disponibilità di informazioni costantemente aggiornate</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di rimodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici-Attività trasversale - Trattamento di dati relativi all'attività di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di rimodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>
Urbanistica	Scheda n. 54 - Ufficio Tecnico - Trattamento di dati relativi all'assetto del territorio ed edilizia abitativa - edilizia residenziale pubblica e locale e piani di edilizia economico-popolare	<div>- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)</div> <div>- ABSC 02 (CSC 1) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" e relative implementazioni effettuate dal titolare)</div> <div>MS-ICT-CDB-09-01 - AUTENTICAZIONE E AUTORIZZAZIONE : Componente SW della Soluzione , commisurata alla necessità, volta a limitare e/o a minimizzare l'accesso ai dati personali</div> <div>MS-ICT-CDB-09-02 - DISCIPLINARE Per definire le modalità di accesso e di utilizzo degli strumenti informatici aziendali nell'ambito dello svolgimento delle proprie mansioni e compiti da parte di amministratori, dipendenti e collaboratori dell'Ente</div> <div>- MS-ICT-CDB-12 - Fasi di rimodernamento del parco macchine e delle infrastrutture (hw e sw) per mantenere buoni livelli la stabilità (RID) , agevolare le attività di operation e soddisfare le crescenti disponibilità elaborative</div> <div>- MS-ICT-CDB-13 - Realizzazione di ambienti di recovery virtuali per i sistemi critici ove occorra minimizzare il tempo di fermo operativo a seguito di fault</div>