Città di Monopoli

AREA ORGANIZZATIVA I - AFFARI GENERALI E SVILUPPO LOCALE

Misure di sicurezza per la protezione dei dati e la prevenzione delle vulnerabilità – *Allegato n. 11*

A cura del Responsabile della Sicurezza informatica dell'Ente: Dott. Domenico Traversa

Misure minime di sicurezza ICT

Il presente documento descrive le misure minime di sicurezza ICT adottate dal Comune di Monopoli in attuazione delle disposizioni previste dalla Circolare n. 2/2017 dell'Agenzia per l'Italia Digitale (AgID). Tali misure rappresentano strumenti operativi essenziali per garantire un livello adeguato di sicurezza dei sistemi informativi, la protezione dei dati trattati e la continuità dei servizi erogati. L'applicazione delle misure minime consente di prevenire le principali vulnerabilità, tutelare la riservatezza e l'integrità delle informazioni e predisporre procedure efficaci per la gestione e il contenimento degli incidenti informatici.

Le misure sono articolate su tre livelli di attuazione:

- **Minimo** (M) - rappresenta il livello base che ogni pubblica amministrazione è obbligata ad adottare, indipendentemente dalla sua dimensione e complessità.
- **Standard** (S) - definisce un livello superiore e costituisce un obiettivo di riferimento per la maggior parte delle amministrazioni.
- **Alto** (A) - livello avanzato richiesto per le amministrazioni che trattano dati critici o erogano servizi essenziali di particolare rilevanza.

Comune di Monopoli
Via Garibaldi, 6 | 70043 Monopoli (BA) | Partita Iva 00374620722
Tel. +39 0804140200
PEC: comune@pec.comune.monopoli.ba.it
Web: www.comune.monopoli.ba.it

Per ciascuna misura minima prevista dalla Circolare AgID n. 2/2017, il Comune di Monopoli ha effettuato un'attenta analisi delle soluzioni tecniche e organizzative già in essere e delle eventuali integrazioni necessarie per assicurare la piena conformità ai requisiti di sicurezza richiesti.

Nella tabella di seguito riportata sono dettagliate le modalità di attuazione all'interno dell'Ente, indicando i controlli adottati, le procedure operative applicate, gli strumenti tecnologici utilizzati, le eventuali misure compensative in caso di soluzioni non attualmente implementabili. Tale attività di mappatura consente di garantire trasparenza, tracciabilità e responsabilizzazione nella gestione della sicurezza informatica e rappresenta un documento di riferimento costantemente aggiornabile.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'inventario delle risorse è gestito ed aggiornato manualmente dall'Ufficio Informatico.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico.	Al momento non è stato adottato alcuno strumento automatico per aggiornare l'inventario di tutti i beni ICT.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Nella rete è installato un dispositivo Deep Discovery Inspector (DDI). Questo strumento esegue un'analisi approfondita del traffico di rete per rilevare e segnalare in tempo reale la presenza di dispositivi sconosciuti, attività malevole e anomalie comportamentali, generando allarmi automatici.

1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Nella rete è installato un dispositivo Deep Discovery Inspector (DDI). Questo strumento esegue un'analisi approfondita del traffico di rete per rilevare e segnalare in tempo reale la presenza di dispositivi sconosciuti e qualificare i sistemi connessi alla rete.
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Il server DHCP registra le operazioni tramite log di sistema.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Le informazioni ricavate dal logging DHCP vengono utilizzate per migliorare l'inventario e identificare dispositivi non ancora censiti.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'inventario viene aggiornato manualmente quando nuovi dispositivi sono installati e configurati dall'Ufficio Informatico.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Al momento l'inventario viene aggiornato solo tramite operazioni manuali.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	L'inventario dei dispositivi di rete è gestito manualmente e contiene indirizzo IP, modello e collocazione.

1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	L'inventario contiene nome della macchina, IP, responsabile, ufficio di appartenenza e tipologia di dispositivo.
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	Tutti i dispositivi elettronici portatili dell'organizzazione (telefoni cellulari, tablet, laptop, ecc.) sono registrati e gli viene assegnato un numero di inventario univoco gestito dall'Ufficio Patrimonio.
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	Attualmente l'autenticazione 802.1x non è implementata.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Al momento non sono utilizzati certificati lato client per l'autenticazione in rete.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Gli utenti non possono installare software autonomamente. Solo l'Ufficio Informatico può installare applicativi attraverso le credenziali di amministratore. Il sopracitato ufficio detiene una lista interna di software autorizzati. Per esigenze specifiche, l'Ufficio valuta il software e, se idoneo, lo aggiunge all'elenco e procede all'installazione.
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	Questa misura non è necessaria in quanto tutti i software possono essere installati soltanto dall'Ufficio Informatico che detiene le credenziali di amministratore.
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	Questa misura non è necessaria in quanto tutti i software possono essere installati soltanto dall'Ufficio Informatico che detiene le credenziali di amministratore.

2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Questa misura non è necessaria in quanto tutti i software possono essere installati soltanto dall'Ufficio Informatico che detiene le credenziali di amministratore.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Nella rete è installato un dispositivo Deep Discovery Inspector (DDI). Questo strumento esegue un'analisi approfondita dei software installati su ciascun dispositivo.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	L'Ufficio Informatico mantiene un inventario aggiornato di tutti i software installati, suddivisi per tipologia di dispositivo, funzione e versione.
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	È in fase di valutazione l'adozione di strumenti automatici per l'inventario software e il monitoraggio delle patch installate.
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	Al momento non si sono mai rese necessarie soluzioni di isolamento tramite macchine virtuali o sistemi air-gapped. Qualora dovessero emergere esigenze specifiche, l'Ufficio Informatico è in grado di implementare tali soluzioni.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	L'implementazione e il mantenimento di queste baseline avvengono tramite Group Policy Objects (GPO) di Active Directory, che definiscono policy su password, account utente, configurazioni firewall e hardening del sistema operativo.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	L'Ufficio Informatico adotta configurazioni "hardened" per sistemi operativi e applicazioni, applicando le principali misure di sicurezza e mantenendo aggiornati i sistemi per ridurre le superfici di attacco.
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	I dispositivi acquistati dall'Ente sono forniti con sistema operativo preinstallato. In fase di inizializzazione viene applicata una procedura standardizzata che prevede la validazione e l'aggiornamento della configurazione di sicurezza. Tale procedura comprende l'installazione degli aggiornamenti più recenti del sistema operativo,

					l'applicazione delle ultime patch di sicurezza disponibili e l'implementazione delle configurazioni di hardening previste dalle policy interne
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	L'Ufficio Informatico configura tutti i dispositivi seguendo un'apposita procedura interna prima della messa in uso.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	In caso di compromissione, i sistemi vengono ripristinati sulla base dell'immagine standard validata e sicura.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Le modifiche alle configurazioni standard sono gestite tramite richiesta formale e autorizzazione dell'Ufficio Informatico.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	L'Ente utilizza sistemi operativi scaricati direttamente dai canali ufficiali Microsoft, che vengono aggiornati al momento dell'installazione. Non sono attualmente predisposte immagini personalizzate offline.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	L'Ente utilizza sistemi operativi scaricati direttamente dai canali ufficiali Microsoft, che vengono aggiornati al momento dell'installazione. Non sono attualmente predisposte immagini personalizzate offline.

3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	L'amministrazione remota avviene tramite connessioni protette e accesso autenticato con credenziali riservate.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Attualmente non sono adottati strumenti specifici per la verifica automatica dell'integrità dei file di sistema.
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	Attualmente non sono adottati strumenti specifici per la verifica automatica dell'integrità dei file di sistema.
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	Il sistema di segnalazione conserva la cronologia delle modifiche e registra l'autore di ogni intervento per supportare le attività di analisi.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	L'Ufficio Informatico monitora eventuali variazioni sospette ai permessi e alla struttura dei file di sistema.

3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Attualmente non è in uso un sistema centralizzato per il controllo automatico delle configurazioni e la rilevazione delle modifiche non autorizzate.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	La configurazione dei PC avviene tramite impostazioni manuali standardizzate e l'applicazione di regole centralizzate attraverso le Group Policy di Active Directory (GPO), che definiscono configurazioni di sicurezza e gestione utenti uniformi per tutta la rete comunale.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	L'Ufficio Informatico verifica e monitora costantemente le modifiche alle configurazioni dei sistemi e utilizza sistemi di protezione come il DDI e l'antivirus per rilevare eventuali anomalie o vulnerabilità in tempo reale. Ogni attività è tracciata e viene valutata la presenza di criticità attraverso strumenti e procedure consolidate.

4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Non sono attualmente impiegati strumenti automatici per la scansione immediata delle vulnerabilità a seguito di modifiche significative.
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	Non sono utilizzati strumenti SCAP per la validazione delle vulnerabilità.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non è in uso un sistema di correlazione tra log di sistema e risultati delle scansioni di vulnerabilità.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Non sono in uso sistemi di scanning delle vulnerabilità, pertanto non risultano log relativi a tali attività.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Non sono attualmente effettuate verifiche specifiche nei log per individuare attacchi pregressi verso target vulnerabili.
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	Non sono attualmente in uso scansioni di vulnerabilità né account dedicati a tali attività.

4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Non sono presenti sistemi di scansione di vulnerabilità configurati con restrizioni di origine o IP specifici.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il DDI e l'antivirus sono costantemente aggiornati per garantire la copertura contro le vulnerabilità più recenti. L'aggiornamento avviene automaticamente tramite le relative console di gestione.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	L'Ufficio Informatico consulta periodicamente fonti attendibili per aggiornarsi sulle nuove vulnerabilità.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Gli aggiornamenti dei software e del sistema operativo vengono applicati con regolarità. Gli aggiornamenti che richiedono privilegi amministrativi sono gestiti direttamente dall'Ufficio Informatico, che provvede tempestivamente all'installazione delle patch critiche.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Nell'infrastruttura comunale non sono presenti sistemi separati dalla rete o air-gapped. Tutti i dispositivi sono gestiti e aggiornati tramite le procedure in uso nella rete locale.

4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Attualmente non sono in uso sistemi automatici di scanning delle vulnerabilità. La verifica periodica delle attività di scansione verrà considerata in caso di futura adozione di tali strumenti.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Le vulnerabilità rilevate sono gestite dall'Ufficio Informatico attraverso l'immediata applicazione delle patch disponibili o tramite l'adozione di misure compensative. L'eventuale rischio residuo viene valutato, documentato e accettato formalmente.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	L'Ufficio Informatico riesamina periodicamente i rischi accettati per verificare l'esistenza di nuove soluzioni o aggiornamenti correttivi.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	L'Ufficio Informatico riesamina periodicamente i rischi accettati per verificare l'esistenza di nuove soluzioni o aggiornamenti correttivi.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio	La priorità nell'applicazione delle patch è assegnata in funzione della gravità del rischio, con intervento immediato per le vulnerabilità più critiche.

				associato. In particolare, applicare le patch per le vulnerabilità a partire da quelle più critiche.	
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	Quando le patch non sono disponibili o applicabili nei tempi richiesti, l'Ufficio Informatico adotta misure provvisorie di mitigazione per contenere il rischio.
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Le patch di software personalizzato o non standard vengono testate in ambiente dedicato prima della distribuzione sui sistemi in produzione.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Gli utenti standard non dispongono di privilegi amministrativi. Le modifiche alle configurazioni di sistema sono effettuate esclusivamente dall'Ufficio Informatico tramite l'utenza amministrativa dedicata.

5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Le utenze amministrative sono utilizzate esclusivamente per attività che richiedono privilegi elevati. Ogni accesso amministrativo è tracciato nei log di sistema.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Ciascun'utenza possiede soltanto i privilegi necessari per svolgere le attività previste per essa.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Le attività svolte con utenze amministrative sono registrate nei log di sistema e monitorate tramite controlli periodici dell'Ufficio Informatico. Il Deep Discovery Inspector contribuisce alla rilevazione di eventuali anomalie di comportamento tramite il monitoraggio del traffico di rete.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'Ente mantiene un inventario aggiornato delle utenze amministrative, ciascuna delle quali è formalmente autorizzata.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Attualmente l'inventario è gestito manualmente. Si valuta l'adozione di uno strumento automatico per segnalare variazioni.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito	Prima di collegare un dispositivo alla rete, l'Ufficio Informatico provvede a sostituire la password predefinita

				con valori coerenti con quelli delle utenze amministrative in uso.	dell'account amministratore locale con credenziali robuste e conformi alle policy interne.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	L'aggiunta o la rimozione di utenze amministrative viene registrata nei log di sistema per garantirne la tracciabilità.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Questa funzionalità non è ancora implementata, ma è in programma l'attivazione di alert automatici per nuove utenze.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Questa funzionalità non è ancora implementata, ma è in programma l'attivazione di alert automatici per variazioni di privilegi amministrativi.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	I tentativi falliti di accesso con utenze amministrative vengono rilevati tramite il Deep Discovery Inspector (DDI), che monitora il traffico di rete e segnala quando un utente inserisce una password errata. Questo permette di individuare anche i tentativi falliti relativi ad utenze amministrative.
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart	L'autenticazione a più fattori non è attualmente implementata. Le credenziali amministrative utilizzano comunque password di elevata robustezza.

				card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Le credenziali amministrative sono configurate per rispettare i requisiti di elevata robustezza.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Le credenziali amministrative sono gestite esclusivamente dall'Ufficio Informatico, che adotta password robuste e periodicamente aggiornate, garantendo il rispetto dei requisiti di sicurezza.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le credenziali dell'utenza amministrativa vengono sostituite frequentemente, rispettando gli standard di robustezza.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Nelle policy di dominio è previsto che ogni qualvolta le password scadono, la nuova password deve essere diversa dalle ultime password utilizzate.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Dopo la modifica delle credenziali, deve trascorrere un determinato lasso di tempo per poterla modificare nuovamente. Soltanto l'Ufficio Informatico può dare la possibilità di modificarla in anticipo, ad esempio in caso di dimenticanza.

5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Le credenziali amministrative vengono modificate periodicamente e non possono essere riutilizzate prima di sei mesi. L'Ufficio Informatico garantisce la creazione di password diverse da quelle precedenti.
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	L'accesso ai sistemi avviene tramite utenze standard. Le operazioni che richiedono privilegi amministrativi sono eseguite tramite apposita elevazione dei privilegi.
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	L'Ente non dispone di postazioni dedicate per le attività amministrative privilegiate.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Gli amministratori dispongono di credenziali distinte per l'accesso standard e per l'accesso con privilegi amministrativi.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutte le utenze, comprese quelle amministrative, sono nominative e riconducibili in maniera univoca ad un singolo soggetto
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere	Le utenze amministrative anonime, quali "Administrator" di Windows, non sono attive sui dispositivi dell'Ente.

				utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	L'account "Administrator" di Windows, creato automaticamente dal sistema operativo, rimane disabilitato per garantire una maggiore sicurezza.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Per eseguire operazioni amministrative vengono utilizzate esclusivamente utenze di dominio. L'uso di utenze amministrative locali è evitato salvo specifiche eccezioni.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate in un database protetto con crittografia AES-256, gestito tramite il software KeePass.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Per l'autenticazione non sono attualmente utilizzati certificati digitali.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Su tutti i sistemi su cui è consentita l'installazione di software è presente un antivirus. Inoltre, nella rete è operativo un dispositivo Deep Discovery Inspector (DDI), che esegue un'analisi approfondita del traffico di rete per rilevare tempestivamente dispositivi sconosciuti, attività

					malevole e anomalie comportamentali, generando allarmi automatici.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Ogni dispositivo dispone del firewall locale attivo e aggiornato. A livello di rete è presente un firewall perimetrale, oltre al dispositivo Deep Discovery Inspector (DDI) per il monitoraggio avanzato del traffico di rete.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Gli eventi rilevati possono essere consultati tramite le console di gestione centralizzate del firewall, dell'antivirus e del DDI.
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Gli strumenti di sicurezza sono gestiti centralmente dall'Ufficio Informatico e gli utenti non hanno la possibilità di modificarne la configurazione.
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	Tramite Active Directory è possibile forzare manualmente l'aggiornamento degli antivirus installati sui dispositivi e verificarne l'effettiva esecuzione dalla console centrale.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata.

8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L’uso dei dispositivi esterni è consentito solo per esigenze lavorative. Ogni dispositivo collegato alla rete viene immediatamente analizzato dall’antivirus e dal DDI, che ne controllano la sicurezza e ne monitorano il traffico in tempo reale.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Ogni dispositivo esterno viene controllato dall’antivirus e dal DDI al momento della connessione per prevenire rischi di infezione.
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Le funzionalità di sicurezza integrate nei sistemi operativi, come DEP e ASLR, sono attivate su tutti i dispositivi in cui risultano disponibili, al fine di limitare lo sfruttamento di vulnerabilità note.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Si dispone di un firewall a livello di rete. Inoltre, sulle macchine è installato un antivirus e e nella rete è installato un dispositivo Deep Discovery Inspector (DDI). Questo strumento esegue un'analisi approfondita del traffico di rete per rilevare e segnalare in tempo reale la presenza di dispositivi sconosciuti, attività malevole e anomalie comportamentali, generando allarmi automatici.

8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Il traffico di rete è monitorato e filtrato sia dal firewall perimetrale sia dal Deep Discovery Inspector (DDI), che analizza in tempo reale tutto il flusso per bloccare codice malevolo.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Oltre ai sistemi di protezione attivi, l'installazione dei software è riservata esclusivamente all'Ufficio Informatico, che dispone di una whitelist dei programmi autorizzati.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Il firewall di rete, il DDI e le funzionalità di sicurezza integrate nei browser contribuiscono al monitoraggio e al blocco degli accessi a siti web e indirizzi noti per avere una cattiva reputazione.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'esecuzione automatica dei contenuti da dispositivi removibili è disattivata su tutti i sistemi.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'esecuzione automatica dei contenuti dinamici, come le macro, è disattivata su tutti i dispositivi.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	L'apertura automatica dei messaggi di posta elettronica è disattivata.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	L'anteprima automatica dei contenuti dei file è disattivata.

8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Ogni volta che un supporto rimovibile viene collegato ai dispositivi aziendali, l'antivirus esegue automaticamente una scansione per rilevare eventuali minacce.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Il filtraggio dei messaggi di posta elettronica, compreso il controllo antispam, è gestito direttamente dal provider del servizio di posta elettronica in cloud, prima che i messaggi vengano recapitati alle caselle dei destinatari.
8	9	2	M	Filtrare il contenuto del traffico web.	Il traffico web è filtrato dal firewall di rete e dal Deep Discovery Inspector (DDI), che ne analizza costantemente il contenuto per individuare minacce.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Il sistema di filtraggio e il DDI monitorano costantemente il traffico web, bloccando file e contenuti pericolosi o potenzialmente dannosi. Il provider del servizio di posta elettronica in cloud provvede al blocco di tipologie di file potenzialmente dannose prima che i messaggi vengano recapitati alle caselle dei destinatari.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Il dispositivo Deep Discovery Inspector (DDI) rileva attività sospette non solo tramite firme, ma anche mediante tecniche di analisi comportamentale e individuazione di anomalie.

8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	Attualmente non è presente una procedura formalizzata per la trasmissione dei campioni di software sospetto al provider di sicurezza, ma l'Ente si impegna a svilupparne una per migliorare la gestione degli incidenti.

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Il sistema di backup effettua quotidianamente copie di sicurezza incrementali dei file contenuti nelle cartelle condivise in uso agli uffici dell'ente. Ogni domenica viene eseguito un backup completo che sostituisce la copia totale della settimana precedente.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Attualmente le procedure di backup riguardano la parte dati, ovvero i file contenuti nelle cartelle condivise in uso agli uffici. I sistemi operativi e le applicazioni software possono essere ripristinati tramite supporti di installazione dedicati.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Il sistema mantiene copie multiple dei backup: quelli incrementali giornalieri, che si conservano per almeno 7 giorni, e quelli completi settimanali. Questo approccio

					consente di recuperare i dati anche in caso di malfunzionamento di uno dei backup intermedi.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Al termine di ogni backup, il sistema esegue automaticamente una verifica di integrità per accertarsi che la copia sia valida e utilizzabile.
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	I backup sono memorizzati in ambienti protetti e accessibili solo agli amministratori di sistema. Inoltre, le copie sono cifrate per garantire la riservatezza delle informazioni.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I backup vengono memorizzati su supporti logicamente separati e non permanentemente connessi al sistema principale, per prevenire la compromissione simultanea dei dati e delle loro copie di sicurezza in caso di attacco.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e	L'Ufficio Informatico monitora e gestisce le cartelle condivise dell'Ente e ha già individuato le tipologie di dati

				segnatamente quelli ai quali va applicata la protezione crittografica.	trattati, evidenziando quelli aventi carattere riservato o sensibile. Tali dati sono protetti tramite adeguate misure di sicurezza e, ove necessario, tramite cifratura.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti.	I dispositivi portatili sono protetti da password di accesso. La cifratura dei dati viene attivata su richiesta o in caso di gestione di informazioni rilevanti.
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	Il firewall perimetrale e il Deep Discovery Inspector (DDI) monitorano e analizzano il traffico in uscita per rilevare e bloccare utilizzi non autorizzati di canali crittografici e tentativi di accesso a siti potenzialmente pericolosi per la sicurezza dei dati.
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	Al momento non sono attivi sistemi automatizzati per la scansione periodica dei dati rilevanti in chiaro sui server.
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	Attualmente l’utilizzo di dispositivi esterni non è limitato.

13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	Attualmente l'Ufficio Informatico non dispone di un sistema centralizzato di autorizzazione dei dispositivi esterni basato su identificazione univoca e cifratura dei dati.
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	La rete è costantemente monitorata attraverso il Deep Discovery Inspector (DDI), che permette di individuare e segnalare eventuali anomalie nel flusso dei dati, contribuendo alla prevenzione della perdita di informazioni.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi offline.	Tutte le anomalie rilevate dai dispositivi di sicurezza, incluso il DDI e il firewall, vengono registrate e conservate nei log di sistema, rendendo possibile l'analisi successiva per scopi investigativi e di miglioramento della sicurezza.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Il firewall perimetrale e il DDI monitorano il traffico uscente per rilevare eventuali connessioni cifrate non autorizzate, con la possibilità di bloccarle o segnalarle tempestivamente.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	La funzione integrata nei browser, il firewall e il DDI bloccano automaticamente il traffico verso e da URL conosciuti per essere associati ad attività malevole.

13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	L'accesso ai file condivisi è regolato tramite permessi granulari e Access Control List (ACL) gestiti tramite Active Directory. I permessi vengono mantenuti anche in caso di copia dei file all'interno dell'ambiente di rete.

DOMENICO TRAVERSA
2025.06.28 09:36:23
CN=DOMENICO TRAVERSA
C=IT
2.5.4.4=TRAVERSA
2.5.4.42=DOMENICO
RSA/2048 bits