Modulo di implementazione delle Misure Minime di Sicurezza

Comune di Banari
12.07.2024

Il presente modello fornisce un ausilio per determinare il livello di copertura prodotto dalle misure poste in essere dall'amministrazione attraverso l'indicazione, nella colonna 'Modalità di implementazione', dello strumento effettivamente utilizzato per realizzare lo ABSC riferito alla riga.
Per misura si intende non solo lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.
Pertanto, al fine di fornire tutte le principali informazioni identificative e descrittive relative alle singole misure può essere utile fare riferimento anche alle informazioni contenute in procedure, eventualmente, già approvate e adottate dall'Amministrazione che si raccomanda di fornire in allegato in caso di segnalazione di incidente informatico al CERT-PA.
Le indicazioni delle modalità di implementazione possono essere ulteriormente utili anche come punto di riferimento dello stato della sicurezza dei servizi/sistemi dell'Amministrazione.

Il modulo deve essere compilato e firmato digitalmente con marcatura temporale dal Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, dal dirigente allo scopo designato e dal Responsabile Legale della struttura.
Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Il Responsabile Legale

Il Responsabile per la Transizione al Digitale

ABSC 1 (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.

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	-	L'inventario riporta i dispositivi informatici collegati in rete in modo permanente poiché espressamente autorizzati dall'Amministrazione Comunale. I dispositivi inventariati risultano essere: server fisici, macchine virtuali, personal computer, stampanti, stampanti multifunzione, apparati di rete, ovvero tutti i dispositivi dotati di indirizzo IP. Per la realizzazione dell'inventario delle risorse attive si è ricorso all'utilizzo delle informazioni disponibili sul Controller di Dominio (DNS), attraverso il software RMM e attraverso la rilevazione manuale. Nell'elenco sono riportati, ove disponibili, almeno i seguenti elementi: • Tipologia di apparato; • Denominazione ovvero nome Netbios; • Indirizzo IP (assegnato staticamente); • Se inserito in domino Active Directory; • Sistema Operativo.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	-	Nel regolamento comunale è fatto divieto ai dipendenti di utilizzare / collegare alla rete dispositivi non autorizzati. Sulla rete dell'Ente è attivo uno strumento RMM con funzione integrata per l'analisi della rete locale, l'individuazione delle apparecchiature informatiche attive e l'inventariazione delle stesse. L'analisi della rete locale viene eseguita automaticamente e per ciascuna apparecchiatura vengono riportati i seguenti elementi: • Tipologia di apparato (ove disponibile); • Denominazione ovvero nome Netbios (ove disponibile); • Indirizzo IP e MAC Address; • Nic Vendor; • Data di primo e ultimo rilevamento sulla rete. L'nventario di cui alla misura 1.1.1 viene aggiornato contestualmente all'inserimento di nuovi dispositivi in rete.
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.	-	Vedi ABSC 1.1.1 e 1.3.1

ABSC 2 (CSC 2): 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

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	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.	2025 - 2	• Attualmente non è presente un inventario definito dei software installati sui dispositivi dell'Ente. Il Comune dovrà predisporre l'elenco dei software autorizzati. Attualmente sui dispositivi dotati di agent RMM con funzione integrata per l'analisi del software installato localmente, è disponibile l'elenco dei software presenti. L'installazione del software sui sistemi critici dell'Ente (server) è consentito unicamente all'Amministratore di Sistema ovvero all'Amministratore di sottosistemi (suite gestionali). I permessi di installazione del software sui personal computer sono concessi ai singoli utenti che possono installare i software coerenti con la propria attività lavorativa istituzionale. Sono state comunque impartite istruzioni agli utenti affinché essi comunichino la necessità, di installazione di software non compreso nell'elenco, all'Amministratore di Sistema, che provvederà all'autorizzazione ovvero al diniego. Implementare apposito strumento automatizzato sui client. • Il Regolamento sulla Sicurezza delle Informazione vieta l'installazione di software non autorizzato sulle postazioni di lavoro. Su tutte le postazioni dovranno essere configurate apposite policies di dominio per impedire l'installazione di software da parte dell'utente. L'utente è attualmente amministratore del proprio pc. el RTD.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	2025 - 2	•Su alcuni sistemi Microsoft (server) è attivo il software Datto RMM che consente di avere report in tempo reale dei software installati su ogni sistema e relative versioni. •L'amministratore di sistema (o il RTD) effettua verifiche periodiche, documentando il risultato. •Vedi ABSC 2.1.1

ABSC 3 (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.

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	-	Vengono utilizzate unicamente le immagini di installazione dei Sistemi Operativi rilasciate dal produttore del software, ovvero dal produttore dell'hardware in caso di Sistema Operativo preinstallato. In ogni caso, prima dell'inserimento nel ciclo produttivo, server, personal computer e laptop, devono avere una configurazione standard che risponda ai seguenti criteri minimi di sicurezza: • installazione software antivirus; • abilitazione firewall personale (di sistema o di terze parti); • installazione degli ultimi aggiornamenti disponibili per il Sistema Operativo in uso; • rimozione del software non necessario; • disabilitazione servizi non necessari.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	-	Vedi 3.1.1
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	-	In caso di compromissione di una postazione PC si provvede alla formattazione e alla ricreazione ex novo con le modalità suddette e alla reinstallazione dei software specifici. Eventuali dati salvati in locale (e non in rete come suggerito dalle direttive dell'ente) sulla postazione, saranno successivamente ripristinati da un back-up, se disponibile. In caso di compromissione di un server è fondamentale capire quando è avvenuta la compromissione e qual è il livello di gravità/invasività.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	2025 - 2	Le immagini dei pc non sono memorizzate offline ma vengono costruite con un processo che le rende altrettanto sicure. L'immagine finale è infatti costruita in modo dinamico partendo dall'ISO del sistema operativo ed applicando una Task sequence. All'immagine standard si aggiungono dinamicamente policies di dominio modificabili solo dagli amministratori del dominio stesso.
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).	-	Per le attività di amministrazione remota dei sistemi primari (server, NAS, apparati di rete) sono impiegati appositi strumenti software RMM che utilizzano l'autenticazione a 2 fattori e protocolli sicuri oltre che, il collegamento remoto tramite VPN IPSEC. Sui dispositivi client sono utilizzati software per l'accesso remoto in modalità di acceso vigilato.

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

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	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'Ente è dotato del sistema antivirus Bit Defender con gestione centralizzata in cloud, che permette di effettuare la scansione delle vulnerabilità sui dispositivi (personal computer e server) dotati di apposito agent. La gestione del sistema antivirus centralizzato è affidata all'Amministratore di Sistema. In caso di modifiche significative ad una configurazione viene eseguita detta scansione. La funzione di monitoraggio delle vulnerabilità viene eseguita ad intervalli di tempo prestabiliti dal sistema antivirus.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	-	•Vedi ABSC 4.1.1 Il sistema antivirus di cui alla misura 4.1.1 è dotato di questa funzione.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	-	I sistemi quali server e personal computer sono configurati per l'istallazione automatica delle patch di sicurezza "critiche" rilasciate dal produttore del Sistema Operativo. Per quanto concerne i software di terze parti, ovvero quelli non ricompresi nel sistema operativo, l'installazione degli aggiornamenti viene eventualmente eseguita su una macchina campione per testarne l'impatto sui software gestionali e sui software "istituzionali". Qualora l'aggiornamento del software di terze parti non causi un malfunzionamento delle applicazioni "critiche", questo viene installato sulle restanti postazioni di lavoro.
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.	-	•Vedi ABSC 4.1.1 •All'interno del comune non esistono sistemi air-gapped •Per i portatili, il Regolamento sulla Sicurezza delle Informazioni impone il collegamento alla rete almeno ogni 15 giorni. In questo modo si garantisce che ricevano dai sistemi centrale gli aggiornamenti predisposti per tutte le postazioni client
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.	-	•Vedi ABSC 4.1.1. Inoltre, è competenza dell'amministratore di sistema verificare che le vulnerabilità emerse dalle scansioni dei software siano effettivamente sanate dopo l'installazione di patch o di azioni correttive che ne limitano il possibile rischio •Tra le vulnerabilità le più critiche sono quelle legate a sistemi operativi, sia client che server, dichiarati fuori supporto dal produttore e per cui non vengono più rilasciate patches di sicurezza. Qualora non sia possibile risolvere le vulnerabilità emerse in seguito ad una scansione del sistema, viene valutata la singola problematica ed eventualmente accettata, se non risolvibile nel breve periodo, qualora sia determinante per l'erogazione di un servizio essenziale da parte dell'Ente.

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.).	2025 - 2	•Vedi ABSC 4.1.1 Attualmente non è presente un piano di gestione dei rischi formalmente definito. Sistematicamente le eventuali criticità vengono comunque segnalate dall'Amministratore di Sistema. •L'amministratore di sistema predisponga un documento in cui elencare quali apparati sono esposti a maggior rischio rispetto ad altri, indicando precisamente il livello di rischio corrispondente (Alto, Medio e Basso). Per rischio si intende il tipo di criticità, che al verificarsi dell'evento malevolo, potrebbe influire gravemente sul funzionamento della struttura o di una sua parte.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	-	Vedi ABSC 4.8.1 e 4.1.1

ABSC 5 (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.

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	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.	2025 - 2	L'accesso ai sistemi con privilegi amministrativi è consentito solo all'Amministratore di sistema e al Responsabile per la Transizione Digitale (o un suo delegato che abbia le competenze ed effettive necessità di modificare la configurazione dei sistemi). Come regola generale si cerca di evitare di dare i privilegi amministrativi, ma eventualmente di dare l'accesso con ruolo "user" o di abilitare solo le funzioni necessarie (es: accesso a cartelle specifiche, possibilità di eseguire alcuni task, possibilità di riavviare alcuni servizi). Gli utenti non hanno privilegi amministrativi sui pc. L'aggiornamento dell'elenco dei software è gestito con il software RMM. Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata al RTD che autorizza l'installazione da parte dell'Amministratore di Sistema, che prove affinché sia installato, come pure che venga aggiornato l'elenco. Le abilitazioni all'installazione del software sono concesse solamente all'amministratore di sistema. Per i server in gestione alle ditte esterne qualora la ditta debba avere accessi amministrativi questi saranno limitati solo al server in gestione.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	2025 - 2	Le utenze amministrative vengono utilizzate unicamente per operazioni di monitoraggio, verifica e implementazione dei sistemi critici dell'Ente. Su server, personal computer, firewall è attivata la funzione integrata nel sistema che registra automaticamente gli accessi logici degli utenti amministratori. Per quanto concerne gli accessi logici effettuati sui server, tramite utenze amministrative, i log di sistema di tali apparati veranno esportati su un repository esterno e conservati per un periodo non inferiore ai 6 mesi. Tale misura dovrà essere implementata attraverso l'adozione di specifici software per il monitoraggio e la conservazione dei log relativi agli accessi logici effettuati delle utenze amministrative sui sistemi dell'Ente. I log collezionati sono relativi agli eventi di login, logout, errore.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	2025 - 2	•IL RTD mantiene un documento denominato "Amministratori di sistema autorizzati" contenente il riepilogo in elenco degli amministratori di sistema autorizzati. Questi ultimi verranno autorizzati attraverso specifica comunicazione inviata via mail È presente un elenco delle utenze amministrative autorizzate e suddivise per tipologia di apparato e sistema. •Le utenze amministrative sono rilasciate nominalmente. Da Active Directory si possono ricavare tutte le utenze amministrative rilasciate. L'Amministratore di sistema è nominato formalmente con un atto da parte del Sindaco (d'intesa con il RTS) oppure direttamente dal Responsabile per la Transizione al Digitale.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	-	•Prima di collegare alla rete un dispositivo le password di default degli utenti amministratori vengono sostituite con altre corrispondenti alle regole dell'ente. •Prima di collegare alla rete un dispositivo le password di default degli utenti amministratori vengono sostituite con altre corrispondenti alle regole dell'ente: questo può essere fatto in modo automatico (es: procedura di distribuzione dell'immagine standard, creazione nuovo server da template) o manualmente.

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).	-	•Questa misura è rispettata dall'adozione della password policy contenuto nel Regolamento per la sicurezza delle informazioni
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	-	•Il Regolamento per la sicurezza delle informazioni prevede che le utenze amministrative vengono sostituite ogni tre mesi.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	-	•Il Regolamento per la sicurezza delle informazioni prevede che le vecchie password non possono essere riutilizzate prima di sei modifiche
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	-	Vedi 5.1.2
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	-	Le utenze sono nominative e riconducibili alla singola persona
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere 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.	-	È stata data istruzione agli amministratori di sistema di utilizzare le credenziali amministrative anonime solo in caso di emergenza o per eseguire servizi o attività pianificate che debbano avere questo tipo di privilegi per funzionare. In quest'ultimo caso è in corso di verifica la possibilità di configurarle in modo da poter essere usate solo per quello scopo e non per attività interattive o per connettersi ai server.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	-	•Le utenze amministrative sono rilasciate nominalmente. •Da Active Directory si possono ricavare tutte le utenti amministrative rilasciate
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	-	•I certificati digitali per l'accesso a portali Istituzionali sono conservati separatemente dalla password

ABSC 8 (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

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	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.	-	A protezione del sistema informatico dell'Ente è presente il software antivirus Bitdefender Gravity Zone con gestione centralizzata in cloud. Il relativo agent risulta installato su tutti i personal computer e i server operativi sulla rete comunale. Le policy di sicurezza sono gestite in maniera centralizzata e, fra l'altro, prevedono l'aggiornamento automatico delle definizioni virus, del prodotto e la scansione periodica dei dispositivi. Sui personal computer e sui server è disabilitata per gli utenti la funzione di disattivazione della protezione in tempo reale ed è inibita la possibilità di disinstallazione. Dalla console di gestione del software antivirus è possibile verificare lo stato di protezione dei dispositivi dotati di agent, nonché analizzare la reportistica relativa alle vulnerabilità individuate dal software di protezione. La console di amministrazione del software antivirus e le policy di sicurezza sono gestite dall'Amministratore di Sistema formalmente incaricato dall'Ente.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	-	Su tutti i server e i computer è attivo il firewall di sistema, inoltre su tutti i personal computer è attiva la funzione firewall propria del software antivirus.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	-	Ai dipendenti è stata data disposizione di non utilizzare dispositivi esterni, ovvero dispositivi personali e comunque non censiti nell'elenco di cui alla misura ABSC 1.1.1 •Il regolamento per la sicurezza delle informazioni vieta l'uso ed il collegamento in rete di dispositivi non autorizzati.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	-	•Attiva una Group Policy Object sul dominio che disattiva su tutti i PC l'esecuzione automatica dei contenuti sui dispositivi removibili
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	-	Microsoft Office è stato configurato in modo che arrivi un messaggio di accettazione prima di eseguire qualsiasi macro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	-	•Impostata la sola visualizzazione delle intestazioni
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	2025 - 2	Verrà mpostata la configurazione standard dei PDL con l'opzione Disattiva l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	-	Il software antivirus di cui alla misura 8.1.1 è configurato in tal senso.
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 fornitore del servizio di posta elettronica (Aruba.) garantisce la presenza di un filtro antispam industriale antispam sui flussi di tutta la posta in ingresso

8	9	2	M	Filtrare il contenuto del traffico web.	2025 - 2	• Da Attivare il filtro del contenuto del traffico web per mezzo del firewall perimetrale comunale. Si consiglia di bloccare le seguenti categorie: - P2P, - Lottery, - Sexual Subject - Streaming media, - Forum, - Vulgar/gruesome, - Gambling, - Drugs, - Malicious WebSites, - Pornography Web Sites - Tutto il traffico da e verso Cina, Russia, Corea Nord Sul software antivirus di cui alla misura 8.1.1 è stata implementata la funzione di scansione del traffico web.
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).	-	• attivare policies sulle appliance Antispam per rimuovere allegati potenzialmente pericolosi. Sul firewall sono attive regole per evitare il download di file con estensioni (es: exe, zip, jar, ecc.) che possono avere contenuti malevoli

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.

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	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.	-	Le copie di sicurezza dei dati trattati sui sistemi critici dell'Ente (server) sono eseguite in modalità asincrona e su base oraria, con cadenza codificata giornaliera, tramite specifici software. Le copie dei dati (applicativi gestionali, database, documenti informatici, immagini di sistemi VM) sono archiviate su un repository differente rispetto a quello di produzione. Le copie di sicurezza garantiscono un retention time almeno fino a 4 settimane. Oltre alle copie di sicurezza dei dati, a protezione del sistema informatico dell'Ente, è presente un sistema di backup avanzato che consente l'esecuzione delle immagini delle Macchine Virtuali, in ambiente VMware, su repository differente rispetto a quello di produzione (Veeam), Le copie di sicurezza garantiscono un retention time almeno fino a 16 settimane.
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.	2025 - 2	•I dispositivi su cui vengono effettuate tutte le copie di sicurezza devono essere custoditi in locali con accesso controllato e consentito solo all'Amministratore di sistema o il RTD. I dispositivi di backup dovranno essere collati in ambiente differente rispetto ai sistemi che sono oggetto di backup.
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 dispositivi su cui vengono fatte le copie presso l'ente non sono direttamente accessibili come unità di rete.

ABSC 13 (CSC 13): PROTEZIONE DEI 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

ABSC_ID			Livello	Descrizione	Previsione anno-trimestre implementazione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	2024 - 4	è in corso il passaggio del SI. Gestionale in infrastruttura Cloud (bando PNRR 1.2). A seguito del passaggio, la sicurezza e la riservatezza dei dati sensibili saranno assicurati dai contratti con il fornitore del S.I. (in modalità SaaS).
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	2025 - 2	Vedi ABSC 8.9.2