MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI
ULTIMO AGGIORNAMENTO – FEBBRAIO 2025

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 segna- lazione 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/si- stemi 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.

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 #			Descrizione	Modalità di Implementazione	L
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Implementato: oltre all'inventario fisico/contabile dell'HW, viene gestito un inventario per singola macchina attiva da parte della società titolare della manutenzione HW e SW. Regolarmente aggiornato.	M
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Viene effettuato in maniera semi automatica via server	S
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalia	Non implementato	A
		4	Qualificare i sistemi connessi alla rete **a**ttraverso l'analisi del loro traffico.	Implementato: gestione della società titolare della manutenzione HW e SW	A
	2	1	Implementare il "logging" delle operazione del server DHCP.	Implementato: gestione della società titolare della manutenzione HW e SW.	S
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Implementato: gestione della società titolare della manutenzione HW e SW	S
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Non implementato.	S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	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.	Implementato: viene indentificato l'IP macchina/nome macchina e utente. Il titolare/responsabile ufficio viene identificato dalla macro e microstruttura amministrativa dell'ente. Di pari passo è possibile identificare se il dispositivo è portatile/personale.	S
		3	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.	Implementato: correlato con il punto 1.4.2 Per i cellulari che si collegano alla rete sono identificati con IP e nome dispositivo. Per i cellulari non collegati nessuna identificazione	A
	5	1	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.	Implementato: tutti i dispositivi per accedere alla rete locali devono sottostare a procedure di autenticazione. Tutti i dispositivi connessi via cavo sono autorizzati ad andare in internet, cosi come i dispositivi wifi previa password. Un firewall si occupa degli accessi e dei log.	A

	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Non implementato l’accesso mediante certificati digitali. Tuttavia, nessuno può collegarsi da remoto alla rete locale in quanto protetta da firewall con accessi limitati.	A

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 #			Descrizione	Modalità di Implementazione
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, work-station e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.	Implementato: esiste un elenco del software autorizzato. Teoricamente ogni utente è amministratore della propria postazione ed è a conoscenza che l'installazione di altro software non è consentita se non previo accordo con il soggetto responsabile della rete. In ogni caso, eventuali danni all'infrastruttura è diretta responsabilità dell'utente.
	2	1	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.	Implementato su server: gestione della società titolare della manutenzione HW e SW Non implementato su configurazioni locali
		2	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).	Implementato su server: gestione della società titolare della manutenzione HW e SW. Non implementato su configurazioni locali
		3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Non implementato.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Implementato: gestione della società titolare della manutenzione HW e SW. Regolarmente (tempistiche stabilite dalla stessa società) viene eseguita regolare scansione antivirus e malware.	M
		2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Implementato: gestione della società titolare della manutenzione HW e SW.	S
		3	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.	Eseguito in maniera non automatica ma da parte di operatore.	A
	4	1	Utilizzare macchine virtuali e/o sistemi air-gapped[1] 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.	Reverse Proxy situato in una rete DMZ isolata dalla rete del comune, per gestire gli accessi ai vari portali messi a disposizione dall'ente.	A

1 Air-gapped: isolato. Tecnica informatica solitamente utilizzata per mettere in sicurezza sistemi o reti che richiedono maggior attenzione rispetto ad altre: basti pensare alle reti classificate come militari, ai sistemi di controllo di grande aziende e industrie sensibili (ad esempio centrali nucleari o industrie chimiche) o *network* che gestiscono e processano pagamenti attraverso carte di credito e bancomat.

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 #			Descrizione	Modalità di Implementazione	Liv
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	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.	Implementato: gestione della società titolare della manutenzione HW e SW. Limitatamente ai server.	S
		3	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.	Implementato: gestione della società titolare della manutenzione HW e SW. Limitatamente ai server.	A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
3	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Implementato: gestione della società titolare della manutenzione HW e SW.	M
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Implementato: gestione della società titolare della manutenzione HW e SW.	M
		3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Non implementato.	S
	3	1	Le immagini d'installazione devono essere memorizzate offline.	Implementato in passato. Eventualmente da implementare dopo futura valutazione	M
		2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti	Non implementato. In esito alla valutazione di cui al punto 3.3.1, in caso di valutazione positiva, verrà implementato.	S
	4	1	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).	Implementato: gestione della società titolare della manutenzione HW e SW. Connessioni protette via VPN.	M

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	5	1	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.	Non implementato	S
		2	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.	Non implementato	A
		3	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.	Implementato: gestione della società titolare della manutenzione HW e SW solo su apparati HW Server	A
		4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Implementato: gestione della società titolare della manutenzione HW e SW solo su apparati HW Server	A

	6	1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Non implementato	A
	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Non implementato	A

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 #			Descrizione	Modalità di Implementazione	Liv
4	1	1	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.	Non implementato. Tuttavia va considerato che l'accesso è protetto da firewall con accessi molto limitati.	M
		2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Non implementata con carattere periodico. In caso di notizie di potenziali minacce si procede ad analisi sulla base dei bollettini di sicurezza internet.	S
		3	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 implementato.	A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non implementato	S
		2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Non implementato	S
		3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile	Non implementato	S
	3	1	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.	Implementato: gestione della società titolare della manutenzione HW e SW nel caso di controllo antivirus	S
		2	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.	Implementato: gestione della società titolare della manutenzione HW e SW nel caso di controllo antivirus	S

	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Implementato: antivirus e antimalware vengono periodicamente aggiornati	M
		2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione.	Implementato: gestione della società titolare della manutenzione HW e SW (aggiornamento con servizi di bollettini sulla sicurezza informatica)	S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applica-zioni.	Implementato: gestione della società titolare della manutenzione HW e SW sui server. Sulle singole postazioni l'onere è sul singolo operatore. I SW applicativi vengono aggiornati dalle rispettive case madri.	M
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non esiste la fattispecie	M
	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Implementato: gestione della società titolare della manutenzione HW e SW	S

	7	1	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.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	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.	Non implementato	S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
		1	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.).	Implementato: gestione della società titolare della manutenzione HW e SW	M

4		2	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 prioritarie	Implementato: gestione della società titolare della manutenzione HW e SW	M
	9	1	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.	Non implementato	S
	10	1	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.	Non implementato	S

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 #			Descrizione	Modalità di Implementazione	Liv
5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Implementato: gestione della società titolare della manutenzione HW e SW limitatamente ai server	M
		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Implementato: gestione della società titolare della manutenzione HW e SW limitatamente ai server	M
		3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Implementato: gestione della società titolare della manutenzione HW e SW	S
		4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Non implementato	A
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Non implementato	A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
5	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Implementato: gestione della società titolare della manutenzione HW e SW	M
	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Non implementato	S
		2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Non implementato	S
		3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Non implementato	S
	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Implementato: gestione della società titolare della manutenzione HW e SW	S
	6	1	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 card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	Non implementato	A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Non implementato: attualmente utilizzate password a 6/8 caratteri	M
		2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Non implementato	S
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Non implementato	M
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non implementato	M
		5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Non implementato	S
		6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Non implementato	S

	8	1	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.	Non implementato	S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	9	1	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.	Non implementato	S
		1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Implementato: gestione della società titolare della manutenzione HW e SW. Implementato nelle utenze degli applicativi. A livello di server non esiste distinzione	M
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Implementato: gestione della società titolare della manutenzione HW e SW	M

	10	3	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.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		4	Evitare l’uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Implementato: ogni macchina è nel dominio e tutti gli account sono nel dominio.	S
5	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non implementato: nel caso di ricorso all’autenticazione con certificati digitali, il servizio verrà implementato.	M

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 #			Descrizione	Modalità di Implementazione	Liv
8	1	1	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.	Implementato: gestione della società titolare della manutenzione HW e SW.	M
		2	Installare su tutti i dispositivi firewall ed IPS personali.	Implementato: gestione della società titolare della manutenzione HW e SW anche se il firewall è periferico, non agisce su ogni dispositivo ma sulla rete globale.	M
		3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Implementato: gestione della società titolare della manutenzione HW e SW – Log anche su firewall	S
	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Implementato: gestione della società titolare della manutenzione HW e SW	S
		2	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.	Implementato: gestione della società titolare della manutenzione HW e SW	S
		3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Non implementato.	A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
8	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Non implementato	A
	4	1	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.	Non implementato	S
		2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Implementato: gestione della società titolare della manutenzione HW e SW mediante tre scansioni	A
	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Implementato: gestione della società titolare della manutenzione HW e SW Per il software esiste un firewall che protegge la rete locale (server e pc) da intrusioni esterne	S
		2	Installare sistemi di analisi avanzata del software sospetto.	Non implementato	A
	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Implementato: gestione della società titolare della manutenzione HW e SW mediante "blocco" di alcuni indirizzi	S
ABSC_ID #			**Descrizione**	**Modalità di Implementazione**	**Liv**

8	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Implementato: gestione della società titolare della manutenzione HW e SW. Automaticamente dal S.O. Windows	M
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Implementato: gestione della società titolare della manutenzione HW e SW. Effettuato su file provenienti dall'esterno (es. Internet)	M
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Implementato: gestione della società titolare della manutenzione HW e SW di default	M
		4	Disattivare l'anteprima automatica dei contenuti dei file.	Implementato: gestione della società titolare della manutenzione HW e SW di default	M
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Non implementato	M
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Filtrare il contenuto del traffico web.	Non implementato. Effettuato in passato ma poi disattivato.	M
		3	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).	Non implementato	M
ABSC_ID #			**Descrizione**	**Modalità di Implementazione**	**Liv**

8	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Non implementata la scansione euristica	S
	11	1	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.	Non implementata	S

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 #			Descrizione	Modalità di Implementazione	Liv
	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Implementato: gestione della società titolare della manutenzione HW e SW quotidianamente. le copie vengono fatte giornalmente su un dispositivo di rete NAS, settimanalmente riversa i dati su un disco esterno. Il disco esterno viene custodito in cassaforte.	M
		2	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.	Implementato: gestione della società titolare della manutenzione HW e SW. Solo server. Giornalmente viene effettuata la copia delle macchine virtuali.	A
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Non implementato	A
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Implementato: gestione della società titolare della manutenzione HW e SW. Verificato e testato il funzionamento del ripristino macchine virtuali	S
	3	1	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.	Implementato: gestione della società titolare della manutenzione HW e SW. Viene assicurata la protezione fisica. Non si effettua la cifratura dei dati.	M

	4	1	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.	Implementato: gestione della società titolare della manutenzione HW e SW. Il disco viene fisicamente distaccato dall'unità.	M

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 #			Descrizione	Modalità di Implementazione	Liv
13	1	1	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	Non implementato: non viene effettuata la scrittura crittografica	M
	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Non implementato	S
	3	1	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.	Non implementato	A
	4	1	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.	Non implementato	A

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	5	1	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.	Non implementato	A
		2	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.	Non implementato dato che non è consentito alcun accesso a dispositivi esterni	A
	6	1	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.	Non implementato	A
		2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Non implementato	A
	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Non implementato	A
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	Implementato: gestione della società titolare della manutenzione HW e SW	M

	9	1	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..	Non implementato	A