



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
 Servizio Innovazione, Sistemi Informativi

STATO DI ATTUAZIONE DELLE MISURE MINIME DI SICUREZZA INFORMATICA COMUNE DI MONZA

(Circolare n. 2 del 18 aprile 2017 dell'AGENZIA PER L'ITALIA DIGITALE)

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 attive è realizzato attraverso l'utilizzo di appositi sistemi, in particolare: A. postazioni Desktop tramite LANDesk B. dispositivi mobili tramite AIRWATCH C. Thin Client tramite ThinMan D. stampanti tramite inventario Office365 e Code di stampa E. apparati di rete attivi tramite HPE IMC F. Access Point WiFi tramite CISCO wireless controller G. Altri apparati di rete tramite Sharepoint

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Tutti i sistemi indicati al punto 1.1.1 sono automatici ad eccezione delle lettere D e G
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	L'infrastruttura di networking dispone di sistemi di discovery dei dispositivi collegati alla rete che evidenziano anomalie attraverso HPE IMC e AdRem NetCrunch
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Misura al momento non ancora attivata, è prevista la sua parziale attivazione nell'anno 2018
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Misura già implementata tramite DHCP di Microsoft
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Vedi punto 1.1.2 e 1.2.1
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Gli strumenti citati al punto 1.1.1 consentono l'aggiornamento automatico dell'inventario
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Vedi punto 1.3.1
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.	Misura attivata tramite DHCP (punto 1.2.1) e gli strumenti di cui al punto 1.1.1
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	La misura è attivata per la quasi totalità delle specifiche indicate fatta eccezione per il responsabile della risorsa (comunque ricavabile dalla struttura organizzativa dell'Ente)

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

				creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
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.	La misura è parzialmente attivata tramite l'utilizzo del sistema software MDM, in particolare AIRWATCH. Si prevede la copertura totale entro il 2019
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.	Misura attivata solo per la WiFi di backoffice (accesso a risorse in LAN) e per accesso extranet tramite NetScaler di Citrix alle postazioni virtuali
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Misura attivata solo per dispositivi che si collegano alla WiFi di backoffice

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.	La misura minima è attivata non consentendo a nessun utente installazione di software in autonomia se non tramite sistemi di software distribution self service già attivi

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi

Servizio Innovazione, Sistemi Informativi

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.	Al momento la misura non è ancora implementata a causa della mole di applicazioni interessate
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).	Vedi punto 2.2.1
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Vedi punto 2.2.1
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	La misura è attivata tramite LANDesk e SCCM che consente software inventory
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.	La misura è attiva per i client in forma automatica; per la parte server è attivata mediante l'isolamento degli applicativi su server dedicati
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.	Vedi punto 2.3.1
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per	La misura è attiva tramite DMZ, vLAN, firewall e virtual machine

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



				operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	
--	--	--	--	--	--

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.	Misura attiva tramite policy di Active Directory (utenti non amministratori), software antivirus, firewall perimetrale e firewall software
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.	La misura è realizzata nel caso in cui sia automatizzabile (ad es. ottimizzazione pre-provisioning di client virtuali), mentre negli altri casi viene effettuata all'occorrenza (ad es. eliminazione account e servizi non necessari)
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.	Misura attivata tramite MS SCCM e Citrix PVS

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi

Servizio Innovazione, Sistemi Informativi

3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Vedi punto 3.1.3
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Vedi punto 3.1.3
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Vedi punto 3.1.3
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini base usate dai sistemi di cui al punto 3.1.3 sono soggette a backup
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Misura attivata tramite storage locali e remoti e su nastri magnetici collocati in cassaforte ignifuga
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).	Misura attivata tramite VPN, SSH e HTTPS e protocolli proprietari
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.	Misura attivata tramite funzionalità avanzate di antivirus
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per	Vedi punto 3.5.1

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

				qualunque alterazione di tali file deve essere generato un alert.	
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.	Misura non ancora attiva, in fase di studio
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Vedi punto 3.5.3
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Vedi punto 3.5.3
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Misura attivata tramite strumenti di backup e ripristino

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	La misura viene attivata tramite opportuni software di scansione dei sistemi in rete

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969

**Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi**

Servizio Innovazione, Sistemi Informativi

				amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	La misura sarà attivata prossimamente
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).	La misura non è attiva
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	La misura non è attiva
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	La misura non è attiva
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	La misura viene eseguita all'occorrenza su sistema antivirus e su firewall
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.	La misura non è attiva
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.	La misura non è attiva

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi

Servizio Innovazione, Sistemi Informativi

4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	La misura viene eseguita automaticamente dai sistemi di antivirus e firewall
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	La misura è attivata tramite registrazione ad appositi sistemi di aggiornamento (antivirus, content filtering e firewall)
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	La misura viene attivata periodicamente non in maniera automatica. Il sistema antivirus copre in ogni caso automaticamente le vulnerabilità da eventuali patch non ancora installate
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.	La misura è attiva: viene eseguita internamente o fornendo ai soggetti deputati la possibilità di farlo
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.	La misura è attiva mediante policy differenziate su specifiche funzionalità
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.	La misura è attivata tramite le metodologie indicate
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	La misura è attiva rivalutando progressivamente le condizioni di vulnerabilità

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

				le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
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.).	La misura è attivata tramite prassi consolidata (ad es. restore dei file corrotti, ripristino server danneggiati, sostituzione postazioni guaste, ecc.)
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.	La misura è attivata tramite prassi consolidata
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.	La misura è attivata definendo opportuni workaround
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.	La misura è attivata tramite opportuno versioning delle macchine e/o la realizzazione di ambienti virtuali di test dedicati

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

ABSC_ID	Livello	Descrizione	Modalità di implementazione
---------	---------	-------------	-----------------------------

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

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.	Misura attivata tramite opportuna definizione dei profili
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Vedi punto 5.1.1
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Misura attivata tramite definizione dei privilegi in Active Directory
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Misura attivata sui server più critici
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Misura attivata tramite Active Directory
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	La misura non è attiva
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.	La misura è attivata tramite policy Active Directory
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	La misura non è attiva

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	La misura non è attiva
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	La misura non è attiva
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	La misura è attiva per tutti gli utenti tramite Active Directory
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 card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	La misura è attiva solo per accessi extranet tramite Citrix NetScaler
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).	La misura non è attiva, in fase di implementazione per il 2018
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	La misura è implementata per tutti gli utenti tramite Active Directory
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	La misura è attivata tramite policy Active Directory
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Vedi punto 5.7.3
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Vedi punto 5.7.3

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi

Servizio Innovazione, Sistemi Informativi

5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Vedi punto 5.7.3
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.	La misura è attivata ove possibile
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.	La misura non è attiva
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	La misura è attivata tramite policy Active Directory
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	La misura è attivata su tutte le macchine di recente creazione, ove possibile per quelle meno recenti
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.	Vedi punto 5.10.2
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).	La misura è attivata tramite policy Active Directory

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	La misura è implicitamente implementata tramite la presenza di utenze amministrative diverse e personali
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	La misura è in fase di implementazione nel corso del 2018 (riguarda esclusivamente la rete di WiFi di backoffice)

ABSC 8 (CSC 8): DIFESA 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.	La misura è attivata tramite apposito sistema antivirus
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	La misura è presente su tutti i dispositivi, viene attivata dove opportuno
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	La misura è attivata utilizzando sistemi diversi (syslog server, mail, ecc.)
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.	La misura è attivata: solo le utenze amministrative sono autorizzate ad alterare la configurazione.
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su	La misura è attivata tramite console centrale del sistema antivirus

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

				ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	La misura verrà attivata nel corso del 2018
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	La misura è attivata (ad es. limitando uso di chiavette USB o devices personali)
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	La misura è attiva tramite sistema antivirus
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.	La misura è implementata in parte dal sistema operativo, in parte dal sistema antivirus e in parte dalla gestione infrastrutturale
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	La misura è in fase di studio a livello di sistema operativo, mentre è stato implementato il Behaviour Monitor
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.	La misura è attivata da e verso reti pubbliche a livello di antivirus, IPS, application control, content filtering, ecc.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	La misura è in fase di implementazione nel corso del 2018 mediante utilizzo della funzionalità Sandbox fornita dai nuovi firewall

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi

Servizio Innovazione, Sistemi Informativi

8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	La misura è attivata tramite firewall
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	La misura è attivata tramite funzionalità dell'antivirus
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Vedi punto 8.7.1
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	La misura è attivata via policy
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	La misura è attivata via policy
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	La misura è attivata tramite funzionalità dell'antivirus laddove non siano completamente bloccati
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.	La misura è attivata sul sistema di posta aziendale
8	9	2	M	Filtrare il contenuto del traffico web.	La misura è attivata tramite apposito motore di content filtering
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).	La misura è attivata tramite apposito motore di content filtering e firewall
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	La misura è attivata tramite funzionalità dell'antivirus

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

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.	La misura è attivata tramite funzionalità dell'antivirus
---	----	---	---	--	--

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.	La misura è attivata tramite appositi sistemi di backup
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.	La misura è attivata tramite sistemi di backup
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	La misura è attivata tramite diversi sistemi di backup e restore
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	La misura è attivata
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	Le misure sono attivate, fatta eccezione per la cifratura, benché la riservatezza sia comunque garantita dall'impiego di un particolare software di backup

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969

**Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi**

Servizio Innovazione, Sistemi Informativi

				effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	
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.	La misura è attivata poiché una delle copie è offline e un'altra è salvata presso un altro site senza connessione permanentemente accessibile

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 segnatamente quelli ai quali va applicata la protezione crittografica	La misura è in fase di analisi
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	La misura non è attiva
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.	La misura è attiva tramite sistemi di controllo perimetrale

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

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.	La misura non è attiva
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.	La misura è attiva tramite blocco o sblocco mirato della possibilità di utilizzare devices esterni
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.	La misura non è attiva
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 misura verrà sperimentata nel corso del 2018
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	La misura è parzialmente attiva, nel corso del 2018 verrà attivata completamente
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	La misura verrà sperimentata nel corso del 2018
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	La misura è attiva tramite content filtering e firewall

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969



Settore Organizzazione, Risorse Umane, Servizi Demografici, Sistemi Informativi
Servizio Innovazione, Sistemi Informativi

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.	La misura è parzialmente attiva
----	---	---	---	---	---------------------------------

Monza, 22 dicembre 2017

LA DIRIGENTE DEL SETTORE

ORGANIZZAZIONE, RISORSE UMANE, SERVIZI DEMOGRAFICI,
SISTEMI INFORMATIVI

dott.ssa ANNAMARIA IOTTI

Servizio Innovazione e Sistemi Informativi

Piazza Trento e Trieste | 20052 Monza | Tel. 039.2372272-2450 | Fax 039.2372534

Email innovazione@comune.monza.it

Orari: da lunedì a venerdì 8.30-13.00 / pomeriggio solo telefonicamente

Sede Municipale: Piazza Trento e Trieste | 20052 Monza | Tel. +39.039.2372.111 | Fax +39.039.2372.558

Email protocollo@comune.monza.it | PEC monza@pec.comune.monza.it

Codice Fiscale 02030880153 | Partita IVA 00728830969