

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA		
<b>ISTITUTO COMPRENSIVO "DANIELE SPADA"</b>		
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO		
<b>www.icsovere.gov.it</b>		
Via Silvestri, 1 24060 SOVERE (BG)	E-mail bgic87800n@istruzione.it Pec bgic87800n@pec.istruzione.it Telefono 035 981233	C.M. BGIC87800N C.F. 96005640162

## PIANO DI ADOZIONE DELLE MISURE MINIME DI SICUREZZA AGID

Il presente documento definisce le misure minime di sicurezza ICT adottate dall'ISTITUTO COMPRENSIVO DANIELE SPADA DI SOVERE (BG) in attuazione della direttiva del Presidente del Consiglio dei ministri 1° agosto 2015, definendo il livello di protezione all'organizzazione informatica comunale, individuando gli interventi idonei per il suo adeguamento.

L'aumento degli eventi cibernetici a carico della pubblica amministrazione determina l'esigenza di consolidare un sistema di reazione efficiente, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica locale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi.

L'elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Le misure preventive, devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte.

Diviene pertanto fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure, nonché la protezione della configurazione, che è quella immediatamente successiva.

Le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace.

Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute ed evidenziare un attacco in corso, inoltre l'individuazione della presenza di codice malevolo può impedirne l'esecuzione.

Le misure di protezione sono quindi necessarie per impedire l'obiettivo primario di alcuni attacchi e cioè la sottrazione delle informazioni o l'indisponibilità delle stessa mediante criptazione.

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

ABSC_ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'Allegato 1 - RISORSE AMMINISTRAZIONE contiene l'inventario di tutte le risorse attive individuate per indirizzo Ip, tipo risorsa e ubicazione	Predisposizione inventario delle risorse amministrative di segreteria. In fase di studio il censimento degli IP di tutti i devices presenti nell'istituto (laboratori fissi e mobili, aule, etc.)
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	NON IMPLEMENTABILE	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	NON IMPLEMENTABILE	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	NON IMPLEMENTABILE	
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	NON IMPLEMENTABILE	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	NON IMPLEMENTABILE	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'aggiornamento avverrà quando saranno aggiunte nuove risorse	Aggiornare l'elenco delle risorse quando si inserirà un nuovo dispositivo utilizzato dall'amministrazione che risulti essere connesso alla rete
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	NON IMPLEMENTABILE	
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.	I dati relativi all'inventario delle risorse attive sono inseriti nell'ALLEGATO 1. Alcuni dispositivi sono configurati con indirizzo IP fisso, mentre altri sono impostati con DHCP	Verifica e aggiornamento annuale degli indirizzi IP nell'inventario. Da implementare con l'utilizzo di un software che faccia l'inventario delle risorse in automatico
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	NON IMPLEMENTABILE	

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

ABSC_ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
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.	Allegato 2: Lista software autorizzati Gli utenti sono semplici "utenti" della macchina e non possono installare software. L'installazione dei software viene effettuata dagli incaricati	Stilare la whitelist dei software autorizzati
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.	Si definisce un pacchetto di software installabile (vedi allegato 2) e si stabiliscono i privilegi limitati per proteggere nuove installazioni l'attivazione di un account amministratore	Dotare tutti i dispositivi di account utente e account amministratore con password e privilegi di installazione
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).	NON IMPLEMENTABILE	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	NON IMPLEMENTABILE	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Gli utenti non hanno diritti di amministratore e pertanto non possono installare software non autorizzato	Da implementare con sistemi di sicurezza Endpoint
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.	Da implementare mediante l'utilizzo del modulo di riferimento (allegato 1)	Richiedere a tutti i responsabili di plesso e dei laboratori di informatica la compilazione e l'aggiornamento periodico del modulo predisposto
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.	NON IMPLEMENTABILE	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	NON IMPLEMENTABILE	

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

ABSC_ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Gli utenti non hanno diritti di amministratore e possono effettuare solamente operazioni sicure. Sono rispettate tutte le configurazioni indicate nell'Allegato B del Dlgs. 196	Utilizzo accurato di account correttamente configurati (account admin e account user con privilegi limitati)
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.	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Lato workstation: SO aggiornato, patch sicurezza, antivirus aggiornato, accesso agli utenti con diritti limitati Lato Server SO aggiornato, credenziali dell'utente Amministratore opportunamente custodite, disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte non utilizzate	Da implementare mediante creazione di dischi di ripristino
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	I ripristini verranno eseguiti rispettando le configurazioni standard	Da implementare mediante creazione di dischi di ripristino
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Implementabile mediante utilizzo di procedure e configurazioni standard e account admin con privilegi	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Per le nuove attrezzature, al termine della procedura di configurazione, verranno create le immagini e memorizzate offline	Salvataggio e conservazione delle immagini ISO del sistema su supporti di memorizzazione removibili
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Conservazione delle immagini ISO su supporti di memorizzazione esterna custoditi in cassaforte	
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).	Le connessioni remote potranno essere effettuate tramite utilizzo del protocollo https con specifici software intrinsecamente sicuri	
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.	NON IMPLEMENTABILE	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	

3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	NON IMPLEMENTABILE	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	NON IMPLEMENTABILE	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	NON IMPLEMENTABILE	

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

ABSC_ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
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.	Si mantengono aggiornati i sistemi operativi, gli antivirus ed il firewall. Dove presente, tramite il software Windows Defender è possibile rilevare per ogni PC le vulnerabilità dei software	Aggiornamento periodico dei sistemi operativi, antivirus e firewall
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Gli antivirus, i sistemi operativi ed i firewall si aggiornano automaticamente	Controllo periodico dei sistemi e dei dispositivi
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	NON IMPLEMENTABILE	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	NON IMPLEMENTABILE	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	NON IMPLEMENTABILE	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	NON IMPLEMENTABILE	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	NON IMPLEMENTABILE	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	NON IMPLEMENTABILE	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Il sistema aggiorna regolarmente il database ed il software	Controllo periodico dei sistemi e dei dispositivi
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	NON IMPLEMENTABILE	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Gli aggiornamenti e le patch del sistema operativo vengono gestite dal sistema operativo. Gli aggiornamenti degli applicativi vengono effettuati con le tempistiche di rilascio da parte delle SoftwareHouse proprietarie	Controllo periodico dei sistemi e dei dispositivi
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.	Non sono presenti sistemi separati dalla rete	Nessuna
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.	Implementabile mediante attivazione di un registro con data e azione svolta	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Le vulnerabilità rilevanti vengono risolte impiegando le idonee misure necessarie, vulnerabilità minori vengono invece valutate singolarmente. L'aggiornamento della versione di Java viene valutato in funzione della compatibilità con i software installati	Controllo periodico dei sistemi e dei dispositivi
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	Implementabile mediante attivazione di un registro con data e azione svolta	
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 gestione dei rischi prevede il monitoraggio periodico degli apparati e delle patch rilasciate	Controllo periodico dei sistemi e dei dispositivi
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 priorità degli interventi verrà programmata in base al rischio derivante dalla vulnerabilità	Controllo periodico dei sistemi e dei dispositivi

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.	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	

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

ABSC ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
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.	La modifica delle configurazioni del sistema è affidata esclusivamente ad account admin con privilegi rilasciati a utenti autorizzati con adeguate competenze tecniche	Gestione, autorizzazione e monitoraggio account admin con privilegi al personale di segreteria e a docenti formati in merito
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Tutti gli accessi e tutte le operazioni di amministrazione relative a Protomail (segreteria digitale), registro elettronico, sito web e piattaforma e-learning (Google Suite For Education) sono registrati in log visibili, non modificabili e conservati a norma di legge	Nessuna
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Attuata per tutte le operazioni di amministrazione relative a Protomail (segreteria digitale), registro elettronico, sito web e piattaforma e-learning (Google Suite For Education)	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Implementabile per tutte le operazioni di amministrazione relative a Protomail (segreteria digitale), registro elettronico, sito web e piattaforma e-learning (Google Suite For Education) sono registrati in log visibili, non modificabili e conservati a norma di legge	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Le credenziali degli utenti con diritti amministrativi sono conservate e custodite in cassaforte. Con la nomina di Amministratore di sistema sono stati individuati gli incaricati e attribuite le opportune autorizzazioni	Gestione, autorizzazione e monitoraggio account admin con privilegi al personale di segreteria e a docenti formati in merito
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	NON IMPLEMENTABILE	
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.	Le credenziali sui nuovi dispositivi vengono adeguate con quelle in uso e mediante impostazione password protetta admin e user	Gestione, autorizzazione e monitoraggio account admin e user
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Attuata per tutte le operazioni di amministrazione relative a Protomail (segreteria digitale), registro elettronico, sito web e piattaforma e-learning (Google Suite For Education)	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Attuata per tutte le operazioni di amministrazione relative a Protomail (segreteria digitale), registro elettronico, sito web e piattaforma e-learning (Google Suite For Education) mediante creazione di profili "inferiori" e monitoraggio con log di tutti gli accessi e le operazioni svolte	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Attuata per tutte le operazioni di amministrazione relative a Protomail (segreteria digitale), registro elettronico, sito web e piattaforma e-learning (Google Suite For Education) mediante privilegio limitato all'amministratore nella creazione di diritti di utenza e monitoraggio dei log	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Attuata per tutte le operazioni di amministrazione relative a Protomail (segreteria digitale), registro elettronico, sito web e piattaforma e-learning (Google Suite For Education) mediante tracciatura dei log di accesso e eventuale blocco di accesso all'utente in caso di tentativo di accesso con credenziali non autorizzate e segnalazione dell'IP che ha tentato di violare l'accesso	
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.		



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 password delle utenze amministrative deve essere generata rispettando i seguenti criteri: almeno una lettera minuscola, almeno una lettera maiuscola ed almeno un numero. SOGI consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi: 1. Verifica o meno del doppio accesso 2. Inserimento data generale di scadenza password 3. Numero di gg massimi per la validità del codice di accesso 4. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso 5. Lunghezza minima del codice di accesso (in questo caso 14) 6. Numero minimo dei caratteri minuscoli 7. Numero minimo dei caratteri maiuscoli 8. Numero minimo dei caratteri numerici 9. Numero minimo dei caratteri speciali 10. Tempo minimo cambio password 11. Possibilità o meno di riutilizzare vecchie password	Configurare i parametri della password per le utenze amministrative secondo i seguenti criteri di sicurezza: almeno una lettera minuscola, almeno una lettera maiuscola ed almeno un numero
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Gestione dei criteri password attraverso parametri definiti	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Implementazione mediante configurazione dei parametri SOGI e Google Suite For Education. I sistemi dei dispositivi di segreteria sono inoltre configurati con la richiesta di cambio di password periodica	Configurare i parametri della password per le utenze amministrative secondo i criteri di sicurezza accettabili
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Implementazione mediante configurazione dei criteri di password history con impedimento di riutilizzo della stessa password prima di 3 cicli	Configurare i parametri della password per le utenze amministrative secondo i criteri di sicurezza accettabili
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Vedi punto 5.7.1	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Vedi punto 5.7.1	
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.		
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.	NON IMPLEMENTABILE	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Vengono individuate utenze amministrative con privilegi limitati	
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le credenziali degli utenti con diritti amministrativi sono univoche e nominative, conservate in e custodite in cassaforte	
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.	Le credenziali sono conservate e custodite in cassaforte	
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).		
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali degli utenti con diritti amministrativi sono conservate e custodite in cassaforte. Per la parte SOGI le credenziali non vengono mai cancellate ma oscurate e conservate per 10 anni	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non vengono utilizzati certificati digitali ma solo username e password criptate	

### ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
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.	Si utilizza di antivirus e firewall. Utilizzo di software Windows Defender dove presente	
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	E' attivo un firewall a protezione della rete	
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.		
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.	NON IMPLEMENTABILE	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.		
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	NON IMPLEMENTABILE	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Alla rete vengono abilitati all'accesso esclusivamente i dispositivi necessari allo svolgimento delle attività della segreteria	
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.		
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.	NON IMPLEMENTABILE	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.		
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.		
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	NON IMPLEMENTABILE	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.		

8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'esecuzione automatica è disabilitata nei sistemi operativi	Disattivazione della funzione di esecuzione automatica nei sistemi operativi e controllo periodico
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'esecuzione automatica è disabilitata nei software gestionali	Disattivazione della funzione di esecuzione automatica nei software gestionali e controllo periodico
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Attività svolta dall'antivirus e firewall	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Attività svolta dall'antivirus e firewall	
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Attività svolta dall'antivirus e firewall	
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.	Attività svolta dall'antivirus e firewall e filtri antispam dei client di posta	
8	9	2	M	Filtrare il contenuto del traffico web.	Attività svolta dall'antivirus e firewall con black list (solo sede centrale e scuola secondaria)	Estendere a tutti i plessi il controllo filtrato con blacklist
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).	A livello di mail server sono impostati filtri relativi a tipologie di allegati pericolosi.	
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	

### ABSC 10 (CSC10): COPIE DI SICUREZZA

ABSC_ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	E' attivo un sistema di Backup giornaliero automatico (incrementale) e manuale (due volte a settimana). Per la parte SOGI, i server effettuano il backup dei file giornaliero conservandone copia per 7 giorni, il backup dei database è fino a 15 giorni giornaliero, dal 16 giorno è settimanale, per un massimo di 52 copie. Le copie dei file si trovano presso la sede della SOGI in via Pietro di sacco 8, Verona ed identica copia è presente in via Adda 16, Verona Ogni amministratore può in qualunque momento scaricarne copia e conservarla in locale accedendo all'area amministrazione, backup, lì troverà le copie di 15 giorni. Le copie vengono generate una volta al giorno alle 00,20	
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.	Attività svolta dall'antivirus e firewall. Per la parte SOGI, il backup è diviso in 2 parti: i dati delle scuole come descritte nel punto 10.1.1, il backup del server nel sistema operativo presente presso Aruba spa ad Arezzo, tempo di ripristino in caso di danneggiamento del server 24/28 ore, in ogni caso si attiverebbe una macchina muletto che garantirebbe la continuità del servizio	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Attività svolta dall'antivirus e firewall. Per la parte SOGI, vedi punto 10.1.1	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Per la parte SOGI, l'azienda verifica quotidianamente la situazione del backup attraverso log inviati automaticamente, inoltre periodicamente la SOGI estrapola dei backup per verificarne l'efficacia	
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.	Predisposizione di n. 2 dischi di backup, uno da conservare in cassaforte e l'altro collegato al server. Per la parte SOGI, le copie di backup sono criptate e protette da password	
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.	Predisposizione di n. 2 dischi di backup, uno da conservare in cassaforte e l'altro collegato al server. Per la parte SOGI, vedi punto 10.1.1	

### ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Liv.	Descrizione	Modalità di implementazione	Azioni previste
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.	I dati con requisiti di riservatezza sono salvati sul server che è protetto da password	
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	
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.	NON IMPLEMENTABILE	
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.		
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.		
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.	NON IMPLEMENTABILE	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.		
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	NON IMPLEMENTABILE	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il controllo viene effettuato tramite le FIREWALL CONFIGURATO	Estendere la protezione a tutti i plessi
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	NON IMPLEMENTABILE	

**ALLEGATO 1 INVENTARIO RISORSE AMMINISTRAZIONE**

ID RISORSA	N.	TIPO RISORSA	ubicazione	IP	SISTEMA OPERATIVO	PROTEZIONE ANTIVIRUS	GESTIONALE	APPLICATIVI INSTALLATI	note
Dirigente	1	NOTEBOOK	Ufficio dirigenza	DHCP	Windows 10 Pro	Win Defender	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
DSGA	2	PC	Ufficio DSGA - Area Amministrazione e Contabilità	DHCP	Windows 10 Pro	Win Defender	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
Amministrazione 01	3	PC	Ufficio DSGA - Area Amministrazione e Contabilità	IPv6: 192.168.1.21/24	Windows 10 Pro	Win Defender	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
Supporto	4	PC	Ufficio DSGA - Area Amministrazione e Contabilità	IPv4: 192.168.1.63	Windows 7	Avast Free	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
Didattica 03	5	PC	Ufficio Segreteria - Area Didattica e Alunni	DHCP	Windows 10 Pro	Win Defender	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
Didattica 02	6	PC	Ufficio Segreteria - Area Didattica e Alunni	IPv4: 192.168.1.56/24	Windows 10 Pro	Win Defender	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
Personale 02	7	PC	Ufficio Segreteria - Area Personale	DHCP	Windows 10 Pro	Win Defender	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
Personale 01	8	PC	Ufficio Segreteria - Area Personale	IPv4: 192.168.1.4	Windows 8	Win Defender	Protomail e registro elettronico di Sogi Snc	Vedi allegato 2	
Router	9	ROUTER	Ufficio Segreteria	IP 192.168.1.254	Nessuno	Firewall con filtro contenuti e Black List e protezione base attacchi esterni	Nessuno		
Server	10	SERVER	Ufficio Segreteria	IPv4: 192.161.1.2	Windows Server 2012	Protezione standard Windows	Windows Server 2012		

## ALLEGATO 2 software consentiti dispositivi amministrativi e segreteria

ID		N.	DENOMINAZIONE SOFTWARE	funzione	note
	A	1	Windows XP, 7, 8, 10	Sistemi operativi	
	A	2	Suite Windows Office	Gestione documenti, fogli di calcolo, presentazioni, etc.	
	A	3	Suite Adobe (Acrobat Reader e Creator, Photoshop)	Lettura e creazione PDF, grafica	
	A	4	Win Zip e RAR	Programmi di compressione file	
	A	5	Mozilla Firefox, Google Chrome, Windows Explorer	Browser	
	A	6	Suite Open Office	Gestione documenti, fogli di calcolo, presentazioni, etc.	
	A	7	AVAST, AVG, Avira, NOD, MacAfee	Antivirus	
	A	8	Piattaforma JAVA	Ambiente di esecuzione di programmi in linguaggio Java	
	A	9	SOGI Protomail (in remoto)	Segreteria Digitale	
	A	10	SOGI Registro elettronico (in remoto)	Registro elettronico	
	A	11	SOGI sito web (in remoto)	Gestione sito web	
	A	12			
	A	13			
	A	14			
	A	15			