

Revisione Gennaio 2019

Storico delle revisioni

- 2019-01 : ABSC_ID=1.1.1 aggiornati i riferimenti ai sistemi di sicurezza di rete
- 2019-01 : ABSC_ID=1.1.2 aggiornati i riferimenti ai sistemi di sicurezza di rete
- 2019-01 : ABSC_ID=1.3.1 aggiornati i riferimenti ai sistemi di sicurezza di rete
- 2019-01 : ABSC_ID=1.4.1 aggiornati i riferimenti ai sistemi di sicurezza di rete
- 2019-01 : ABSC_ID=10.1.1 aggiornati i sistemi di sicurezza in utilizzo (o in futuro utilizzo) in vista anche della piena compliance al GDPR.
- 2019-01 : ABSC_ID=13.1.1 aggiornati i sistemi di sicurezza in utilizzo (o in futuro utilizzo) in vista anche della piena compliance al GDPR.
- 2019-01 : ABSC_ID=13.8.1 aggiornati i riferimenti ai sistemi di sicurezza di rete

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	<p>L'inventario delle risorse attive è implementato nei modi descritti in ABSC1.4.1, ABSC1.4.2 e ABSC1.4.3</p> <p>Durante il corso del 2018 sono stati raccolti i dati (MAC address) delle risorse attive nella rete di Istituto.</p> <p>L'accesso al database è riservato alle autorità (polizia postale), su richiesta esplicita.</p> <p>E' stato inoltre implementato un meccanismo di autenticazione degli utenti, a prescindere dalla risorsa di rete utilizzata.</p>
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	<p>L'inventario di cui alla ABSC1.1.1 è implementato in maniera automatica grazie ad un apposito apparato di rete programmabile (network appliance), denominato NetSecurity, attivato nella rete di Istituto.</p> <p>L'appliance si occupa del reperimento automatico dei dati</p>

					<p>necessari e del loro immagazzinamento in database locali. Durante il corso del 2018 sono stati raccolti i dati (MAC address) delle risorse attive nella rete di Istituto. Considerato l'utilizzo di dispositivi privati da parte dei docenti, al fine di utilizzare il registro elettronico attraverso la rete dell'Istituto, l'automatismo è assolutamente necessario.</p> <p>N.B. La misura è implementata nonostante sia di livello superiore al minimo.</p>
1	1	3	A	<p>Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.</p>	<p>Il discovery dei dispositivi collegati alla rete è implementato in maniera automatica grazie ad un apposito apparato di rete programmabile (network appliance), denominato NetSecurity, attivato nella rete di Istituto. L'appliance si occupa del reperimento automatico dei dati necessari e del loro immagazzinamento in database locali. Gli allarmi non sono attualmente attivati.</p> <p>N.B. La misura è implementata, seppur parzialmente, nonostante sia di livello superiore al minimo.</p>
1	1	4	A	<p>Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.</p>	<p>Misura non implementata.</p>
1	2	1	S	<p>Implementare il "logging" delle operazione del server DHCP.</p>	<p>Le operazioni DHCP sono demandate ad un apposito apparato di rete programmabile (network appliance), denominato NetSecurity, attivato nella rete di Istituto, il quale si occupa anche del loro logging. L'appliance si occupa del reperimento automatico dei dati necessari e del loro immagazzinamento in database locali.</p> <p>N.B. La misura è implementata nonostante sia di livello superiore al minimo.</p>
1	2	2	S	<p>Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.</p>	<p>Le informazioni ricavate dal logging del DHCP mantenuto dall'apparato NetSecurity di cui al ABSC1.2.1 sono utilizzate per migliorare in maniera automatica l'inventario delle risorse presenti in rete l'inventario delle risorse ed identificare risorse non ancora censite. L'appliance si occupa del reperimento automatico dei dati</p>

					<p>necessari e del loro immagazzinamento in database locali.</p> <p>N.B. La misura è implementata nonostante sia di livello superiore al minimo.</p>
1	3	1	M	<p>Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.</p>	<p>L'approvazione degli apparati connessi alla rete è demandata ad un apposito apparato di rete programmabile (network appliance), denominato NetSecurity.</p> <p>L'appliance si occupa del reperimento automatico dei dati necessari e del loro immagazzinamento in database locali.</p> <p>L'aggiornamento dell'inventario, quando nuovi dispositivi approvati vengono collegati in rete, è automatizzato.</p> <p>Durante il 2018 è stato implementato un aggiornamento continuo e automatico dell'inventario. Considerato l'utilizzo di dispositivi privati da parte dei docenti, al fine di utilizzare il registro elettronico attraverso la rete dell'Istituto, l'automatismo è assolutamente necessario.</p>
1	3	2	S	<p>Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.</p>	<p>L'aggiornamento dell'inventario, quando nuovi dispositivi approvati vengono collegati in rete, è automatizzato.</p> <p>Il tutto come descritto in ABSC1.3.1.</p> <p>N.B. La misura è implementata nonostante sia di livello superiore al minimo.</p>
1	4	1	M	<p>Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.</p>	<p>L'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP, è implementato in maniera automatica grazie ad un apposito apparato di rete programmabile (network appliance), denominato NetSecurity, attivato nella rete di Istituto.</p> <p>L'appliance si occupa del reperimento automatico dei dati necessari e del loro immagazzinamento in database locali.</p> <p>Durante il 2018 è stata registrata continuamente l'associazione MAC-IP-Utente. Tali tracciati sono illeggibili e ad esclusiva disposizione delle autorità (polizia postale).</p>
1	4	2	S	<p>Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema,</p>	<p>Misura non implementata.</p>

				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.	
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.	Misura non implementata.
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 non implementata.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Misura non implementata.

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.	E' stato stilato un elenco di software autorizzati per ciascun tipo di sistema. L'elenco è continuamente aggiornato, al fine di soddisfare le differenti specificità dei sistemi in utilizzo in segreteria e nella didattica.
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.	Misura non implementata.
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).	Misura non implementata.
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Misura non implementata.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Al fine di rilevare la presenza di software non autorizzato nei PC, saranno eseguite scansioni semestrali sui sistemi PC e Server grazie all'ausilio di tool software free (a titolo esemplificativo e non esaustivo si cita VoodooShield, SecureAPIus e CryptoPrevent).
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.	Misura non implementata.
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.	Misura non implementata.
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	Misura non implementata.

				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.	<p>L'Istituto utilizza configurazioni standard per la protezione dei sistemi operativi. Le configurazioni sono salvate in file denominati "immagini", creati solo dopo l'esecuzione di tool open-source di hardening (ad esempio: "hardentools", pubblicato in GitHub). I tool utilizzati hanno permesso la disattivazione di (l'elenco che segue è puramente indicativo e non esaustivo):</p> <ul style="list-style-type: none"> - esecuzione di VBScript and Javascript - esecuzione di autorun e autoplay - esecuzione di powershell - estensione di file utilizzati principalmente a scopi malevoli - esecuzione di Macro Office - esecuzione di oggetti OLE - esecuzione activeX - esecuzione Javascript in documenti PDF - esecuzione di oggetti embedded in documenti PDF <p>L'utilizzo di firewall personali completa la configurazione sicura standard di ogni sistema dell'Istituto.</p>
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.	Misura non implementata.
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 non implementata.

CTIC83400C - REGISTRO PROTOCOLLO - 0000160 - 11/01/2019 - A/35 - sicurezza - U

3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	La definizione e l'impiego delle configurazioni standard è implementata nei modi descritti in ABSC3.1.1
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Eventuali sistemi in esercizio che vengano compromessi saranno ripristinati utilizzando le configurazioni standard descritte in ABSC3.1.1
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Misura non implementata.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione sono memorizzate in appositi DVD. N.B. La misura è implementata nonostante sia di livello superiore al minimo.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Misura non implementata.
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).	Tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature sono effettuate per mezzo di connessioni protette, grazie all'adozione di un apposito apparato di rete programmabile (network appliance), denominato NetSecurity, attivato nella rete di Istituto. L'apparato permette la proiezione in rete locale attraverso VPN crittografate (L2TP+IPSEC / IPSEC).
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 non implementata.
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.	Misura non implementata.
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 implementata.

CTIC83400C - REGISTRO PROTOCOLLO - 0000160 - 11/01/2019 - A/35 - sicurezza - U

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

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

ABSC_ID			LIVELLO	DESCRIZIONE	MODALITÀ DI IMPLEMENTAZIONE
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	La ricerca delle vulnerabilità su tutti i sistemi in rete è effettuata regolarmente e ad ogni modifica significativa della configurazione dei sistemi con strumenti automatici, alcuni dei quali open source: Metasploit è quello utilizzato alla data di stesura del presente documento. I tool utilizzati forniscono agli amministratori di sistema e ai tecnici preposti report con indicazioni delle vulnerabilità più critiche.
4	1	2	S	Eeguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Misura non implementata.
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).	Misura non implementata.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Misura non implementata.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Misura non implementata.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Misura non implementata.
4	3	1	S	Eeguire 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.	Misura non implementata.
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche	Misura non implementata.

				macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Gli strumenti di scansione delle vulnerabilità utilizzati, indicati in ABSC4.1.1, si compongono di una parte locale (demone e client) e di una parte cloud, quest'ultima contenente le informazioni relative ai parametri di sicurezza (le "definizioni"). La parte cloud è costantemente aggiornata dal provider (nel caso di tool open source ciò viene garantito dalle community. L'Istituto si occupa, invece, dell'aggiornamento regolare delle componenti locali.
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	Implementata così come descritto in ASBC4.1.1. N.B. La misura è implementata nonostante sia di livello superiore al minimo.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Ogni sistema è impostato in modo da attivare automaticamente il download e la successiva installazione di patch e aggiornamenti. Ciò vale sia per il Sistema Operativo (SO) che per le applicazioni installate nei sistemi.
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.	Il livello di criticità tipico dei sistemi in Istituto non motiva l'adozione di misure particolarmente stringenti per il loro aggiornamento in ambienti air-gapped. Ciò nonostante alcuni aggiornamenti, in particolar modo quelli dei SO, sono effettuati con i sistemi scollegati dalla rete, semplicemente isolando via software l'apparato concentratore (switch) in prossimità.
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.	Misura non implementata.
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 implementata reiterando le scansioni descritte in ABSC4.1.1. Sono anche eseguite verifiche manuali a campione sui sistemi aggiornati.
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	Misura non implementata.

				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.).	Il piano di gestione dei rischi è quello offerto in automatico dai tool descritti per la implementazione della ABSC4.1.1.
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.	Il livello di priorità delle azioni per la risoluzione delle vulnerabilità è offerto in automatico dai tool descritti per la implementazione della ABSC4.1.1.
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.	Misura non implementata.
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.	Misura non implementata.

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

ABSC_ID			LIVELLO	DESCRIZIONE	MODALITÀ DI IMPLEMENTAZIONE
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	I privilegi di amministratore sono garantiti al solo personale tecnico incaricato e all'Animatore Digitale. Le credenziali sono gestite in ottemperanza a quanto disposto dal D.Lgs. 196/2003 e dal GDPR.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Ogni utente dei sistemi dell'Istituto ne utilizza i servizi a partire da un account con privilegi limitati. L'account amministratore è utilizzato unicamente per scopi che ne richiedono espressamente i privilegi. Ogni accesso amministratore è loggato nel registro log di sistema.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Misura non implementata.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Misura non implementata.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	In Istituto esistono solo due utenze amministrative: una per i sistemi di segreteria e una per i sistemi dedicati alla didattica. Entrambe sono autorizzate dal Dirigente Scolastico.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Misura non implementata.
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.	Ogni dispositivo acquistato o acquisito dall'Istituto viene inizializzato, in modo che ogni impostazione predefinita è contestualizzata. La misura è, quindi, implementata manualmente.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Ogni aggiunta o soppressione di utenza con privilegi di amministratore è loggato nel registro log di sistema. N.B. La misura è implementata nonostante sia di livello superiore al minimo.

CTIC83400C - REGISTRO PROTOCOLLO - 0000160 - 11/01/2019 - A/35 - sicurezza - U

5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Misura non implementata.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Misura non implementata.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	I tentativi falliti di accesso con una utenza amministrativa sono loggati nel registro log di sistema. N.B. La misura è implementata nonostante sia di livello superiore al minimo.
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.	Misura non implementata.
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).	Misura implementata, scegliendo credenziali che includano anche caratteri maiuscoli, numerici e speciali.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Misura implementata come descritto in ABSC5.7.1 pur senza l'ausilio di un sistema bloccante automatico.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	I sistemi chiedono automaticamente, su base periodica, la sostituzione delle credenziali amministrative. Le nuove credenziali sono memorizzate ai sensi di quanto disposto dal D.Lgs. 193/2003 e ss.mm.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	I sistemi impediscono automaticamente il riutilizzo di credenziali a breve distanza di tempo.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Misura non implementata.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Misura non implementata.
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	Misura non implementata.

				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.	Misura non implementata.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Nei sistemi sono previste esclusivamente le credenziali di amministratore e di utente a bassi privilegi. La completa distinzione è quindi soddisfatta.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze amministrative sono assegnate unicamente al tecnico incaricato dell'amministrazione di sistema.
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 utenze amministrative sono assegnate al tecnico incaricato dell'amministrazione di sistema e sono utilizzate unicamente per scopi che ne richiedono espressamente i privilegi
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).	Misura non implementata.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le nuove credenziali sono memorizzate ai sensi di quanto disposto dal D.Lgs. 193/2003 e ss.mm.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Per l'autenticazione non si utilizzano certificati digitali.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			LIVELLO	DESCRIZIONE	MODALITÀ DI IMPLEMENTAZIONE
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Su tutti i sistemi connessi alla rete locale sono installati strumenti antivirus e anti malware locali. Tali strumenti sono mantenuti aggiornati in modo automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i sistemi connessi alla rete locale sono installati i firewall personali di Windows.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Misura non implementata.
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.	Misura non implementata.
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.	Misura non implementata.
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Misura non implementata.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'uso di dispositivi esterni è consentito solo a quelli necessari per le attività didattiche e, comunque, sono soggetti alle misure di controllo e restrizione degli accessi alla rete indicati nel documento.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Misura non implementata.
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.	Misura non implementata.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Misura non implementata.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga	Misura non implementata.

CTIC83400C - REGISTRO PROTOCOLLO - 0000160 - 11/01/2019 - A/35 - sicurezza - U

				gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Misura non implementata.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Misura non implementata.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Misura implementata nei modi descritti in ABSC3.1.1
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Misura implementata nei modi descritti in ABSC3.1.1
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Misura implementata nei client di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Misura implementata nei modi descritti in ABSC3.1.1
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Gli strumenti indicati in ABSC8.1.1 eseguono automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
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.	Gli strumenti antispam sono integrati nel provider di posta elettronica (MIUR).
8	9	2	M	Filtrare il contenuto del traffico web.	Il contenuto del traffico web è filtrato grazie all'adozione di un apposito apparato di rete programmabile (network appliance), denominato NetSecurity, attivato nella rete di Istituto.
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).	Misura implementata nei client di posta elettronica.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Misura non implementata.
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.	Misura non implementata.

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.	<p>Le copie di sicurezza delle informazioni strettamente necessarie per il ripristino del sistema sono effettuate attraverso l'ausilio di un programma gratuito di backup e ripristino, denominata Cobian Backup.</p> <p>L'Istituto ha pianificato – per le risorse informatiche di segreteria – l'utilizzo di software di lavoro collaborativo e sincronizzato (esempio: OwnCloud e NextCloud). Tali sistemi permetteranno la replica automatica dei dati su molteplici sistemi, anche delocalizzati, al fine di portare all'estremo le capacità di recupero di dati.</p>
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.	Misura non implementata.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Misura non implementata.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Misura non implementata.
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.	Misura implementata automaticamente con software di backup di cui al ABSC10.1.1.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I supporti contenenti le copie sono accessibili unicamente da personale autorizzato e scollegate dal sistema.

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	L'analisi è implementata automaticamente con i software di cui al ABSC4.1.1 Inoltre l'Istituto ha pianificato l'utilizzo, per i PC di segreteria, di software di cifratura che miglioreranno ulteriormente gli standard in vista della piena compliance al GDPR.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Misura non implementata.
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.	Misura non implementata.
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.	Misura non implementata.
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.	Misura non implementata.
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.	Misura non implementata.
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.	Misura non implementata.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Misura non implementata.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Misura non implementata.

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	<p>Il blocco del traffico da e verso url presenti in una blacklist è effettuato grazie all'adozione di un apposito apparato di rete programmabile (network appliance), denominato NetSecurity, attivato nella rete di Istituto.</p> <p>La lista è continuamente popolata ed aggiornata.</p> <p>Inoltre, durante il corso del 2018, il NetSecurity è stato interfacciato ad un servizio di WEB-Filtering basato su DNS.</p>
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.	Misura non implementata.