



United Nations
Educational, Scientific and
Cultural Organization

ISTITUTO COMPRENSIVO STATALE PORTO CESAREO
Via Piccinni, 10 Tel. e Fax 0833-569105 C.F. 91012680756
mail leic831006@istruzione.it
mail certificata leic831006@pec.istruzione.it
sito: www.icportocesareo.gov.it



ISTITUTO COMPRENSIVO STATALE-PORTO CESAREO
Prot. 0009249 del 29/12/2017
01-04 (Uscita)

MISURE MINIME DI SICUREZZA ICT

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	Esiste un inventario delle risorse interne (macchine e apparati di rete) basato sull'indirizzo MAC. La gestione e configurazione delle risorse esterne (server in cloud) è eseguita esclusivamente da personale Argo. Questa azienda esterna si affida esclusivamente a server farm di comprovata affidabilità ed esperienza in materia di sicurezza informatica, e comunque previa verifica delle misure fisiche, logiche e organizzative poste in capo alle infrastrutture informatiche fornite. Ad ogni fornitore è richiesta come requisito la certificazione ISO 27001 e uno SLA di connettività di almeno il 95% su base annua e una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	La configurazione di nuovi server (risorse esterne) è eseguita con procedure semi-automatiche e controllate da Argo.
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Ad ogni fornitore di server farm esterne, Argo richiede come requisito uno SLA di connettività di almeno il 95% su base annua e una disponibilità dei servizi 24 ore su 24 per 365 giorni all'anno.
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Le risorse interne (macchine) sfruttano il protocollo DHCP e il logging è gestito a livello del server DHCP interno. Per quanto riguarda le risorse esterne , con cadenza mensile viene eseguito il controllo sui log degli accessi degli amministratori Argo da parte del responsabile della gestione privacy Argo. I log delle operazioni e degli accessi sono marcati temporalmente e archiviati per un periodo di 18 mesi.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Le risorse interne (macchine) possono essere collegate solo previa registrazione dell'indirizzo MAC in inventario
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Le risorse interne (macchine) possono essere collegate solo previa registrazione dell'indirizzo MAC in inventario. L'indirizzo IP è gestito via DHCP. Per quanto riguarda le risorse esterne , gli accessi ai server e ai

					servizi di gestione degli stessi sono monitorati. L'accesso da parte degli amministratori Argo è eseguito sempre attraverso utenze di dominio
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.	Le risorse interne impiegate per l'accesso ai dati sensibili sono macchine di tipo Desktop connesse a rete cablata. Non sono utilizzati dispositivi portatili e/o personali. Le risorse esterne sono organizzate secondo un'architettura di tipo "3 tier". Le applicazioni, i dati in produzione e i backup risiedono presso datacenter dislocati in diversi siti geografici, all'interno dell'Unione Europea, sono tutti registrati e sono posti a grande distanza gli uni dagli altri, al fine di fornire maggiori garanzie di protezione in caso di calamità naturali.
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.	
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.	Le risorse interne impiegate per l'accesso ai dati sensibili sono connessi solo a specifici switch dedicati allo scopo (sottorete cablata). Le risorse esterne sono dislocate in una rete geografica.
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

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.	L'installazione di software su tutte le risorse interne è bloccata per tutti gli utenti. Eventuali nuovi software sono installati esclusivamente dagli amministratori dopo verifica della tipologia e della funzionalità.
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.	
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).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Tutte le risorse interne sono protette con antivirus e software che rimuovono automaticamente eventuali installazioni non autorizzate L'infrastruttura Argo, oltre ad essersi dotata di un sistema di auditing interno finalizzato a rilevare eventuali criticità nel sistema di sicurezza dei dati, sfrutta anche il servizio di un'azienda esterna specializzata nel settore della sicurezza informatica i servizi di Vulnerability Assessment e Penetration Test.
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.	L'inventario è presente
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.	
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.	

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.	Tutte le macchine sono protette da password e hanno un antivirus installato. Gli utenti operativi non hanno privilegi di amministratore.
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.	
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.	Il software utilizzato nelle risorse esterne viene regolarmente aggiornato e rilasciato in accordo a un sistema di versioning
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Risorse interne: le macchine omogenee per tipo e sistema operativo hanno delle configurazioni standardizzate. L'architettura 3-tier impiegata come risorsa esterna include due tipi di server, data server e application server: server dello stesso tipo sono configurati in modo analogo
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Sì
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Il software utilizzato nelle risorse esterne è regolarmente aggiornato e rilasciato in accordo a un sistema di versioning
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini delle risorse interne sono conservate su DVD. Vengono effettuate copie dei database delle risorse esterne più volte al giorno, a intervalli regolari, e con modalità differenti (full e incrementali). Le copie full vengono mantenute presso i server delle infrastrutture per sette giorni. Quotidianamente una copia dei dati viene riversata in un sistema di storage, dove viene mantenuta per 2 mesi. Delle suddette copie, una copia settimanale viene mantenuta per un ulteriore periodo di 2 mesi, mentre una copia mensile viene mantenuta per un periodo complessivo di 6 mesi.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Le copie degli applicativi impiegati nelle risorse esterne vengono fatte ad ogni aggiornamento e mantenute presso i server dell'infrastruttura primaria.
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).	In riferimento alle macchine interne , le operazioni di amministrazione da remoto sono impedito. In caso di necessità vengono abilitate temporaneamente connessioni attraverso protocolli sicuri e disabilitate al termine dell'intervento. Le operazioni di amministrazione delle risorse esterne sono intrinsecamente di tipo remoto, ma sfruttano protocolli sicuri (SSL)
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per	Il sistema di gestione dei servizi e dei dati adottato da Argo (risorse)

				assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	esterne) è improntato a criteri di ridondanza dei sistemi informatici e di replicazione dei dati al fine di preservare i clienti da rischi di interruzione prolungata dei servizi e/o di perdita dei dati. L'integrità delle copie di sicurezza nell'operazione di trasmissione verso il sistema di storage è garantita da un sistema di hashing che controlla l'impronta del file di destinazione con quello di origine. Con cadenza mensile, vengono effettuate prove di ripristino dei backup.
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.	L'infrastruttura Argo è configurata per essere agevolmente convertita da sussidiaria a primaria e viceversa, e i database vengono replicati, in maniera asincrona con un delay ridotto ai tempi necessari alla trasmissione delle transazioni, presso i server delle altre infrastrutture (replicazione speculare dei dati).
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.	Risorse esterne: con cadenza mensile viene eseguito il controllo sui log degli accessi degli amministratori di sistema da parte del responsabile della gestione privacy Argo. Eventuali variazioni critiche sono così associate al relativo amministratore che le ha apportate
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	L'infrastruttura Argo utilizzata come risorsa esterna è dotata di uno strumento di monitoraggio continuo degli applicativi web che fornisce in tempo reale, indicatori sulle prestazioni degli stessi, inclusi eventuali picchi di carico.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	A tal fine ogni infrastruttura Argo è configurata per essere agevolmente convertita da sussidiaria a primaria e viceversa, e i database vengono replicati, in maniera asincrona con un delay ridotto ai tempi necessari alla trasmissione delle transazioni, presso i server delle altre infrastrutture (replicazione speculare dei dati).

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	In caso di modifiche nella configurazione delle risorse interne si procede alla riconfigurazione dei firewall e ad una scansione

				automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	completa dei sistemi
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	L'infrastruttura Argo utilizzata come risorsa esterna è dotata di uno strumento di monitoraggio continuo degli applicativi web che fornisce in tempo reale, indicatori sulle prestazioni degli stessi, inclusi eventuali picchi di carico.
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).	L'infrastruttura Argo, oltre ad essersi dotata di un sistema di auditing interno finalizzato a rilevare eventuali criticità nel sistema di sicurezza dei dati, sfrutta anche il servizio di un'azienda esterna specializzata nel settore della sicurezza informatica i servizi di Vulnerability Assessment e Penetration Test.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
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.	
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.	
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 antivirus configurati sulle macchine interne sono abilitati per l'aggiornamento automatico
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	Il sistema Argo si avvale di un servizio di early warning per il monitoraggio continuo delle vulnerabilità.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	I dispositivi sono configurati per l'aggiornamento automatico del sistema operativo
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 vi sono risorse interne separati dalla rete cablata
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.	
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.	
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.	
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.).	Esistono procedure automatizzate di backup per la salvaguardia dei dati residenti in sede. In riferimento all'infrastruttura esterna, Il sistema di gestione dei servizi e dei dati adottato da Argo è improntato a criteri di ridondanza dei sistemi informatici e di replicazione dei dati al fine di preservare i clienti da rischi di interruzione prolungata dei servizi e/o di perdita dei dati. A tal fine ogni infrastruttura Argo è configurata per essere agevolmente convertita da sussidiaria a primaria e viceversa, e i database sono replicati, in maniera asincrona con un delay ridotto ai tempi necessari alla trasmissione delle transazioni, presso i server delle altre infrastrutture (replicazione speculare dei dati).
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.	Tutte le patch relative a vulnerabilità vengono immediatamente implementate appena disponibili
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.	
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.	

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.	Sono identificati tra il personale 3 tecnici specializzati per le attività di amministrazione.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso alle utenze amministrative è limitato al minimo indispensabile. È in via di estensione una procedura di registrazione degli accessi.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'inventario è presente.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
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 vengono sostituite prima dell'allacciamento in rete.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
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.	Il sistema Argo include un sistema di autenticazione basato su OTP, ma viene utilizzato solo il tradizionale sistema basato su credenziali
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).	Le password devono includere lettere maiuscole e minuscole, caratteri speciali e numeri.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate	Sì

				credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Per le password viene imposta una scadenza trimestrale o semestrale in funzione del grado di criticità.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non è possibile riutilizzare password precedentemente utilizzate.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Dopo tre tentavi falliti da una postazione, il sistema impedisce l'accesso per un'ora da quella postazione
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
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.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	La distinzione è assicurata nella configurazione dai server Argo
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Sono associate a nome e cognome degli utenti ad ogni credenziale di accesso.
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 disponibili solo per i tecnici autorizzati.
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.	L'elenco cartaceo delle password è custodito in cassaforte ed accessibile solo al responsabile della struttura ed al DSGA.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

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.	Presenti su tutte le risorse interne L'infrastruttura Argo, oltre ad essersi dotata di un sistema di auditing interno finalizzato a rilevare eventuali criticità nel sistema di sicurezza dei dati, sfrutta anche il servizio di un'azienda esterna specializzata nel settore della sicurezza informatica i servizi di Vulnerability Assessment e Penetration Test.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Presenti su tutte le risorse interne
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.	
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.	L'infrastruttura Argo, oltre ad essersi dotata di un sistema di auditing interno finalizzato a rilevare eventuali criticità nel sistema di sicurezza dei dati, sfrutta anche il servizio di un'azienda esterna specializzata nel settore della sicurezza informatica i servizi di Vulnerability Assessment e Penetration Test.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	La rete "Pubblica" poggia su una linea dati indipendente da quelle degli uffici e dei laboratori
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.	L'infrastruttura Argo, oltre ad essersi dotata di un sistema di auditing interno finalizzato a rilevare eventuali criticità nel sistema di sicurezza dei dati, sfrutta anche il servizio di un'azienda esterna specializzata nel settore della sicurezza informatica i servizi di Vulnerability Assessment e Penetration Test.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	L'infrastruttura Argo è dotata di un sistema di auditing interno finalizzato a rilevare eventuali criticità nel sistema di sicurezza dei dati.
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.	

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.	Si, per le risorse interne
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Si, per le risorse interne
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Si, per le risorse interne
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Si, per le risorse interne
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Si, per le risorse interne
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.	Si, per le risorse interne
8	9	2	M	Filtrare il contenuto del traffico web.	Si, per le risorse interne
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).	Si, per le risorse interne
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
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.	

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.	Il backup del registro del protocollo è effettuato una volta al giorno sfruttando sistemi cloud offerti dell'infrastruttura esterna
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.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante	Per i servizi di gestione documentale, è stato implementato un

				ripristino di prova.	servizio di controllo di integrità dei file memorizzati come risorse esterne (Argo) che, con cadenza mensile, verifica gli hash dei file archiviati nel sistema
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.	Le copie sono cifrate
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.	Le copie vengono duplicate su dispositivi rimovibili

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	Tutti i dati sono protetti nello stesso modo. Per gli applicativi web Argo è possibile richiedere una copia di backup in locale dei dati residenti presso i server Argo. La procedura è totalmente automatizzata. Per motivi di sicurezza, la richiesta può essere inoltrata accedendo con le credenziali dell'amministratore dei servizi (supervisor), nella persona del DS o suo delegato. Una volta processata, i dati sono resi disponibili per il download per un periodo di tempo limitato. All'indirizzo mail comunicato in fase di richiesta, è inviata la password posta a protezione del file di backup.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	I dati sono trasmessi secondo il protocollo SSL, che garantisce il massimo livello di sicurezza a protezione delle trasmissioni telematiche.
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.	
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.	
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.	
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.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	La misura è implementata nel firewall delle risorse interne
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.	

IL DIRIGENTE SCOLASTICO
(Dott. Francesco G. NUZZACI)
**Documento firmato digitalmente
da Francesco G. Nuzzaci**