Ministero dell'Istruzione, dell'Università e della Ricerca
Istituto ComprensivodiMontecompatri
C.F. 92013790586 C.M. RMIC8AC002
"Paolo Borsellino"

REGOLAMENTO SULL'USO DI INTERNET E DELLA RETE DATI A DISPOSIZONE DEI DIPENDENTI PER L'ESERCIZIO DELLE FUNZIONI D'UFFICIO (POLICY DELLA SCUOLA)

INDICE

Premessa generale

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso delle tecnologie telematiche sia conformato al rispetto dei diritti fondamentali, nonché della dignità dell'interessato.

Occorre ulteriormente premettere che:

a) compete ai dirigenti scolastici (datori di lavoro) assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;

c) emerge l'esistenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinato ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

d) l'utilizzo di internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante l'elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controllo che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Regolamento per l'uso di Internet e della rete dati scolastica

Premesse particolari

Viste la legge 7 agosto 1990 n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto* di accesso ai documenti amministrativi" e la Legge 11 febbraio 2005 "*Modifiche ed integrazioni alla legge 7/8/90 n. 41 concernenti norme generali sull'azione amministrativa";*

Visto il DLgs 19/03/96 "*modifiche e integrazioni al DLgs n. 626/1994 controlli operati tramite sistemi aziendali";*

Visto il DPR del 28/12/2000 n. 445 "*Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*

Visto il DLgs del 30/06/2003 n. 196 "*Codice in materia di protezione di dati personali" e sue s.m.i.;*

Visto il DM del 7 dicembre 2006, n. 305 "*Regolamento recante identificazione dei dati sensibili e giudiziari"*

Vista la deliberazione del CNIPA 19/12/2004 n. 11 "*Regole tecniche dei documenti digitali*";

Visto il DLgs 7 marzo 2005 n. 82 "*Codice dell'Amministrazione Digitale*";

Visto il SO n. 93 aggiornato dal DLgs 159 del 4/4/2006 recante "*Disposizioni integrative e correttive al DLgs 7/3/2005 n. 82*

Vista la legge 20 maggio 1970 n. 300 "*Statuto dei Lavoratori*";

Vista la Direttiva del Consiglio dei Ministri n. 2/2009 del 26/05/2009;

Ritenuto opportuno richiamare gli artt. 2086, 2087 e 2014 del Codice Civile;

Considerato che l'I.C "P. Borsellino", tra i vari strumenti di lavoro, ha messo a disposizione dei dipendenti accessi ad Internet, servizi rete dati e strumenti per lo svolgimento delle mansioni e compiti loro affidati;

Richiamato il principio generale che l'utilizzo delle risorse TIC che la scuola mette a disposizione dei dipendenti deve sempre ispirarsi a criteri di diligenza e correttezza e normalmente adottati nell'ambito dei rapporti di lavoro;

Rilevato che l'Autorità Garante per la Privacy, con delibera n. 13 del 1.3.2007 (pubblicato in G.U. del 10.3.2007 n. 58) ha inteso precisare che è opportuno da parte dei Datori di Lavoro, adottare un disciplinare interno redatto in modo chiaro, senza formule generiche ed adeguatamente pubblicizzato verso i singoli dipendenti interessati, anche ai fini dell'esercizio del potere disciplinare;

Ritenuto che l'adozione del regolamento consente di escludere l'applicabilità della normativa penale a tutela della corrispondenza elettronica poiché, essendo considerata strumento di lavoro, non può essere considerata corrispondenza privata;

Considerato, inoltre, che, se correttamente applicato e fatto rispettare, il regolamento può risultare uno efficace strumento della Policy scolastica anche al fine di limitare il rischio di insorgenza di responsabilità amministrativa della Scuola;

Ritenuto, pertanto dover adottare apposito regolamento per l'utilizzo di Internet e della Posta Elettronica in cui è tra l'altro, precisato che gli stessi sono strumenti aziendali e come tali soggetti anche a controlli secondo i principi ed i criteri di cui ai commi 5, 6 e 7 del citato Provvedimento del Garante e della normativa in tema di Protezione dei dati personali DLgs 196/2003 n. 196 e del DM 35 del 7 dicembre 2006;

Tenuto conto che il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori, interni od sterni, della scuola, agli esperti esterni, ai collaboratori a progetto ed a quelli durante il periodo di stage, a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Art. 1 – Definizioni

a) L'Istituzione Scolastica si identifica con l'Istituto Comprensivo "Paolo Borsellino";

b) "Utenti":

- l'insieme dei soggetti interni (personale amministrativo, docenti, collaboratori scolastici, esperti esterni, soggetti in stage, ecc.), che indipendentemente dal rapporto di lavoro intrattenuto con l'amministrazione scolastica, utilizzano, nella loro attività lavorativa, connessioni ad Internet e rete dati dell'Istituzione Scolastica;
- le ditte che effettuano attività di manutenzione, gli eventuali altri soggetti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle convenzioni stesse nel rispetto del presente regolamento.

Art. 2 – Finalità

Il presente regolamento disciplina le modalità di accesso e di uso della Rete informatica, telematica e dei servizi che, tramite la Rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto Scolastico per dare il supporto informatico, documentario, alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

Art. 3 – Ambito di applicazione

La Rete dell'Istituto Scolastico è costituita dall'insieme delle risorse informatiche, cioè

- dalle componenti hardware/software e dagli apparati elettronici collegati alla Rete informatica dell'Istituto;
- dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Art. 4 – Principi fondamentali

Sono tenuti all'osservanza del presente disciplinare tecnico i "Responsabili del Trattamento" dei dati personali e gli "Incaricati del Trattamento" ai sensi del DLgs 196/2003, nonché i Responsabili e gli Incaricati del Trattamento "esterni" all'Istituzione Scolastica.

La navigazione in Internet e il sistema dei di comunicazione, informazione e trasmissione di dati nonché i dati che vengono inviati e ricevuti con tale sistema sono di esclusiva proprietà dell'Istituzione Scolastica.
Tutte le attività svolte mediante la navigazione in Internet sono finalizzate al conseguimento dei fini istituzionali dell'Istituzione Scolastica stessa.
La connessione ad Internet e l'utilizzo delle infrastrutture sono fruibili con continuità.
Gli utenti hanno l'obbligo di non cedere ad altri le proprie credenziali di cui sono gli unici responsabili e, eventualmente, di sostituirle periodicamente nel rispetto del D. Lgs. 196/2003 con le modalità ed i tempi in esso riportati.
I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi del Codice *Privacy*:

a) il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai dipendenti;
c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, osservando il principio di *pertinenza e non eccedenza*. Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "*mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza";*
d) il principio di *indispensabilità* nel caso in cui ricorra il trattamento di dati sensibili.

Art. 5 – Compiti dell'Amministratore di Sistema

L'abilitazione per la connessione ad Internet ed alla rete scolastica verranno gestiti dall'Amministratore di Sistema o da altra figura tecnicamente competente a cui sono assegnate la responsabilità del corretto funzionamento degli strumenti elettronici, del monitoraggio costante dei livelli dei sistemi al fine di garantire la massima efficienza, della storicizzazione dei processi, della realizzazione e conservazione delle copie di backup, nonché di assicurare l'assistenza tecnica e formativa degli utenti.

Art. 6 – Accesso ad Internet e uso della rete scolastica

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete internet dai Personal Computer, espone la Scuola rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine alla Scuola medesima.

L'utilizzo delle risorse informatiche e telematiche della Scuola devono sempre inspirarsi al principio delle diligenza e della correttezza, pertanto, l'Istituzione Scolastica ha adottato il presente Regolamento per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Internet è una rete mondiale di computer che contiene milioni di pagine di informazioni; parte di queste possono avere contenuti offensivi o illegali, con cui si può entrare accidentalmente in contatto attraverso interrogazioni a motori di ricerca effettuate per scopi "innocui".

Pertanto la Scuola non si ritiene responsabile per il materiale acceduto o scaricato da internet da parte degli utenti e cerca di minimizzare i rischi connessi all'uso di internet mediante l'applicazione di quanto contenuto nel presente regolamento, cui gli utenti sono obbligati ad attenersi.

L'uso di Internet nelle numerose funzionalità è consentito esclusivamente per gli scopi attinenti alle proprie mansioni.

Per non limitare le attività tipicamente aziendali, non è definito a priori un elenco di siti autorizzati; è tuttavia permesso l'utilizzo di adeguati strumenti di filtraggio, mediante i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività lavorative.
Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.
Viene altresì proibita la possibilità di caricare/scaricare (upload/download) a/da Internet file musicali, video o software che non siano attinenti alla propria mansione, scambio di materiale protetto da copyright come anche l'utilizzo della connessione ad Internet per motivi strettamente personali, in quanto ciò si configura come danno patrimoniale cagionato all'Amministrazione consistente nel mancato svolgimento della prestazione lavorativa durante il periodo di connessione.
Viene tassativamente vietato l'utilizzo delle risorse strumentali della Scuola per la memorizzazione di materiale privato, personale o non attinente alla specifica attività lavorativa.
Relativamente all'utilizzo dei singoli PC affidati agli utenti, si precisa che l'assegnazione delle risorse non ne comporta la privatezza, in quanto trattasi di strumenti di esclusiva proprietà Istituzionale e quindi i file memorizzati non sono né tutelati né garantiti dall'Istituto Scolastico per qualsiasi causa.
Infine, il dipendente preposto all'utilizzo di internet nonché della rete dati è tenuto, comunque, ad osservare il segreto d'Ufficio ai sensi dell'art. 15 del DPR 10.01.1957, n. 3

Art. 7 – Memorizzazione file di log durante la navigazione internet

Al fine di verificare la funzionalità, la sicurezza del sistema e il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, generano registri delle attività, nello specifico *log file*, (così come si creano anche i file temporanei e i *cookie*) contenente le informazioni relative ai siti che i singoli PC hanno visitato. Tale registro memorizza l'indirizzo fisico delle prestazioni di lavoro e non i riferimenti dell'utente garantendo in tal modo il suo anonimato.

L'accesso a questi dati è effettuato dal Dirigente Scolastico o da un suo fiduciario autorizzato.
I sistemi software sono programmati e configurati in modo da cancellare periodicamente i dati relativi agli accessi ad internet e al traffico telematico.
L'eventuale prolungamento e/o conservazione dei file può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

Art. 8 – Controlli

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'I.C. "Paolo Borsellino" effettuerà con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi, al fine di verificare l'effettivo adempimento delle prestazioni lavorative e, occorrendo, anche il corretto e legittimo utilizzo degli strumenti di lavoro:

1. analisi aggregata del traffico di rete riferita agli uffici di segreterie, ai laboratori, ai dispositivi LAN-WLAN e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);
2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo alla osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
3. in caso di successivo permanere di una situazioni non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro.

Con la stessa gradualità verranno effettuati controlli sull'utilizzo degli strumenti scolastici per scopi personali (memorizzazione di documenti personali, scambio di materiale protetto da copyright, ecc.) attraverso le fasi:

1. analisi aggregata dei dati memorizzati sul server a livello degli uffici di segreterie, su strumenti PC di laboratorio, di classe, rilevazione della tipologia di utilizzo (file audio, file video, immagini software non autorizzato) e relativa pertinenza con l'attività lavorativa;

2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni

impartite; il richiamo alla osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;

3. in caso di successivo permanere di una situazioni non conforme, è possibile procedere con una analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

Art. 9 – Assistenza tecnica da remoto

In relazione alle eventuali attività di manutenzione da remoto ai PC degli uffici connessi ad internet, il personale tecnico autorizzato dalla Istituzione Scolastica potrà utilizzare specifici software. Tali programmi verranno utilizzati per assistere l'utente durante la normale attività informatica ovvero di svolgere manutenzione su applicazioni e su hardware. L'attività di assistenza e manutenzione avverrà previa autorizzazione telefonica da parte dell'utente interessato. La configurazione del software da utilizzare per gli interventi da remoto, prevedranno un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al PC.

Potrà essere fornita, su richiesta, una informativa sul software utilizzato, nonché le modalità del suo utilizzo per tutti gli utenti interessati.

Art. 10 – Provvedimenti disciplinari

Qualora, a seguito di controlli effettuati nel rispetto dei suddetti articoli del presente regolamento, si rilevino delle anomalie sull'utilizzo degli strumenti informatici che possano essere configurate quali attività non conformi, il Dirigente Scolastico, effettuate le verifiche del caso, procederà ad irrogare sanzioni che possono andare sino alla sospensione delle mansioni per un periodo di tempo sino a 6 mesi.

Per anomalie più gravi riscontrate l'I.C. "Paolo Borsellino" provvederà a segnalare l'abuso all'Autorità competente.

Art. 11 – Soluzioni che garantiscono la continuità lavorativa.

Ciascun dipendente può utilizzare, nelle specifiche funzionalità, gli strumenti della Scuola per garantire efficienza e continuità lavorativa.

Art. 12 – Informativa ai sensi dell'art. 13 del D. Lgs. 196/2003

L'I.C. "Paolo Borsellino" in persona del Dirigente Scolastico è Titolare del Trattamento dei dati personali relativo all'utilizzo di strumenti elettronici da parte degli utenti.

Finalità del trattamento è la verifica del corretto utilizzo della rete dati (LAN e WLAN) e della rete Internet durante il rapporto di lavoro.

Modalità del trattamento dei dati è quella stabilita esclusivamente con strumenti informatici da parte di tutti gli utenti ed operatori.

Comunicazione dei dati. Il trattamento di verifica è effettuato con gradualità per aree aggregate per cui i dati non verranno comunicati con riferimento al singolo utente. La comunicazione, nel caso in cui si accerti un uso indebito della singola postazione sarà data al Dirigente Scolastico per la valutazione del caso sotto il profilo disciplinare.

I diritti dell'interessato sono garantiti in quanto lo stesso potrà farli valere invocando l'art. 7 del DLgs 196/2003 facendo pervenire richiesta scritta dei diritti che vuole difendere direttamente al Dirigente Scolastico o al responsabile del trattamento dei dati.

Art. 13 – Modalità di uso personale dei dispositivi.

Non sono previste modalità di uso personale di mezzi informatici della scuola.

Art. 14 – Prescrizioni interne

Per quanto riguarda le misure di sicurezza si rimanda al Codice Disciplinare adottato dall'Istituto Scolastico ed aggiornato periodicamente.

ALLEGATO 1 - Modulo implementazione Misure Minime con suggerimenti

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	**1**	**1**	**M**	**Implementare un inventario delle risorse attive correlato a quello ABSC 1.4**	L'inventario è riportato in allegato al presente documento conservato presso Ufficio di Presidenza I.C. Paolo Borsellino Via G. felici, 14 Montecompatri, ed elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio.
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.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	
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.**	L'elenco di cui alla misura 1.1.1 è aggiornato. L'aggiornamento dell'elenco è a carico degli Amministratori di Sistema.
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.**	L'inventario è riportato in allegato al presente documento conservato presso Ufficio di Presidenza I.C. Paolo Borsellino Via G. felici, 14 Montecompatri, ed elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio
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.	
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.	
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'elenco è riportato in allegato al presente documento è conservato presso l'Ufficio di Presidenza dell'Istituto Comprensivo P. Borsellino Via G. Felici, 14 Montecompatri. L'aggiornamento dell'elenco dei software è a carico degli Amministratori di Sistema. Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori di Sistema, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco. Le abilitazioni all'installazione del software sono stati concessi solamente agli amministratori di sistema (vedi 5.1.1)
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.**	Gli Amministratori di Sistema eseguono ogni anno la verifica del software installato su ciascun dispositivo e comparano il risultato con l'elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell'elenco viene segnalato agli Amministratori di Sistema, che provvedono affinché venga rimosso o, se valutato necessario, a che venga inserito nell'elenco.
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.	
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.**	Gli Amministratori di Sistema hanno definito e documentato le configurazioni sicure standard per ciascun sistema operativo utilizzato. Sono utilizzate copie immagine conservate come descritto al punto 3.3.1 e 3.3.2
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.	
3	**2**	**1**	**M**	**Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.**	Vedi 3.1.1.
3	**2**	**2**	**M**	**Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.**	Sono state date disposizioni agli amministratori di sistema in tale senso.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	**3**	**1**	**M**	**Le immagini d'installazione devono essere memorizzate offline.**	Sono state date disposizioni agli amministratori di sistema di salvare le immagini d'installazione sul supporto rimovibile
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Il supporto removibile è conservato presso la cassaforte dell'ufficio di presidenza.
3	**4**	**1**	**M**	**Eseguire tutte le operazioni di amministrazione remota di**	Per attività di gestione effettuate da reti esterne alla rete della

				server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	scuola vengono utilizzate connessioni VPN o comunque criptate.
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.	
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.	
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.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
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.	

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.**	Sono state date disposizioni agli Amministratori di Sistema di effettuare una scansione su tutta la rete.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità	*Una volta attuata la misura 4.1.1, si suggerisce caldamente di eseguire anche la misura 4.1.2:*

				dell'infrastruttura.	Sono state date disposizioni agli Amministratori di Sistema di effettuare annualmente una scansione su tutta la rete.
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).	
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.**	E’ in corso l’adozione di una strumento informatico adeguato.
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	
4	**5**	**1**	**M**	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	L’applicazione delle patch di vulnerabilità è schedulata dagli Amministratori di Sistema Qualora l’applicazione automatica delle patch non abbia avuto successo o provochi gravi problemi al funzionamento dei sistemi, gli Amministratori di Sistema valutano e motivano a quale livello di patching occorra fermarsi.
4	**5**	**2**	**M**	**Assicurare l'aggiornamento dei sistemi separati dalla rete, in**	Sono state date disposizioni agli Amministratori di Sistema di

				particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	controllare ed aggiornare manualmente periodicamente i sistemi non raggiungibili via rete. Sono state date disposizioni ai possessori di smartphone, tablet o notebook di proprietà dell'ente di accettare gli aggiornamenti proposti automaticamente dal sistema.
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.**	Sono state date disposizioni agli Amministratori di Sistema di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie, gli Amministratori di Sistema documentano il caso, le eventuali contromisure o la motivazione della mancata risoluzioni su apposito registro/rapportino conservato presso l'Istituto.
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.).**	E' stato redatto il DPP (*Documento Programmatico in materia di Privacy)* per la gestione del rischio informatico in generale.
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.**	Sono state date disposizioni agli Amministratori di Sistema
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 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 amministrazione sono assegnati al soggetto al quale l'apparato è dato in dotazione dato che devono avere la possibilità di accettare in autonomia gli aggiornamenti di sicurezza. (Allegato 5) Axios- I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD). Il sistema Axios Cloud consente le medesime funzionalità.
5	**1**	**2**	**M**	**Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.**	E' attivato il log di sistema per registrare gli accessi come amministratore su server. Axios - I prodotti Axios registrano in automatico ogni accesso effettuato al sistema. Il sistema Axios Cloud possiede un log puntuale di tutte le operazioni effettuate e consente l'accesso allo stesso a qualsiasi richiesta proveniente dall'utente o dalle autorità preposte
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.**	I documenti di nomina degli amministratori di sistema sono consegnati agli stessi e una copia è conservata presso l'ufficio di presidenza (vedi 5.11.1). Axios-Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso. Axios Cloud consente in ogni istante, da parte dell'amministratore di sistema, di verificare lo status delle utente.
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**	Agli amministratori di sistema sono state impartite adeguate

				credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	istruzioni al riguardo.
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.	
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).**	Il sistema di autenticazione per tutti gli utenti obbliga all'utilizzo di password di autenticazioni "forti": **almeno 6 caratteri + 1 numero + una maiuscola** Axios – Axios consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite: 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 In Axios Cloud verranno a breve implementate le stesse funzioni
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	**7**	**3**	**M**	**Assicurare che le credenziali delle utenze amministrative**	Il sistema di autenticazione è configurato per obbligare tutti gli

				vengano sostituite con sufficiente frequenza (password aging)	utenti al cambio password ogni 30 gg. Axios - Vedi parametri indicati nel punto 5.7.1.M
5	**7**	**4**	**M**	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**	Il sistema di autenticazione è configurato per impedire il riutilizzo delle ultime 2 password per tutti gli utenti Axios – Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza. In Axios Cloud sarà a breve implementata le medesima funzione
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
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.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo. Axios-La gestione degli amministratori rispetto alle normali utenze viene fatta, in Axios, tramite la gestione dei livelli (1-9 9=amministratore) e le tipologie di accesso per ogni utente/funzione (5.1.1M)
5	**10**	**2**	**M**	**Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo. Axios-In Axios, ad ogni utenze, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi Anche in Axios Cloud le utenze di accesso sono legate a precise anagrafiche presenti nel 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**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo, creato utente **adminscuola** per le funzioni di amministrazione del dominio

				debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
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 amministrative non personali sono elencate su un documento conservato presso l'Ufficio di Presidenza Axios-Per quanto concerne i prodotti Axios tali credenziali sono gestite all'interno della base dati, l'accesso alla stessa è consentito solo tramite i programmi Axios e quindi secondo le regole di sicurezza enunciate in questo documento. Anche per Axios Cloud vale lo stesso principio con l'aggiunta che la base dati non è in alcun modo accessibile a nessuno se non tramite programmi Axios e quindi secondo le regole indicate nel presente documento.
5	**11**	**2**	**M**	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

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 PC, portatili e server è installato un antivirus con aggiornamento automatico.
8	**1**	**2**	**M**	**Installare su tutti i dispositivi firewall ed IPS personali.**	Su tutti i PC, portatili e server Windows è attivato il firewall di Windows. Sui server Linux è installato iptables
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.	
8	**3**	**1**	**M**	**Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.**	Nel disciplinare dei dipendenti è stata data disposizione di limitare l'uso di dispositivi esterni a quelli necessari per le attività didattiche.
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.	
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.	
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.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**2**	**M**	**Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**3**	**M**	**Disattivare l'apertura automatica dei messaggi di posta elettronica.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**4**	**M**	**Disattivare l'anteprima automatica dei contenuti dei file.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**8**	**1**	**M**	**Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
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.**	L'istituto utilizza un servizio di posta elettronica esterno, che include il filtraggio richiesto. (SEGRETERIA DIGITALE)

8	**9**	**2**	**M**	**Filtrare il contenuto del traffico web.**	Sono state date disposizioni agli amministratori di sistema di configurare i SERVER all'utilizzo dei DNS di OPEN DNS FREE e di conseguenza tutte le postazioni di lavoro.
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).**	Sono state date disposizioni agli amministratori di sistema di configurare il software antivirus delle postazioni di lavoro in tal senso.
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.**	Le copie di sicurezza sono effettuare quotidianamente Axios-Il programma Axios prevede un sistema automatico e non presidiato di copie del proprio DB presente localmente sul server della scuola. Il sistema prevede inoltre l'invio automatico a tre indirizzi mail e/o a tre numeri di cellulare, di un messaggio sull'esito dell'esecuzione delle copie. Il sistema di backup Axios prevede anche la possibilità di effettuare un backup non solo della base dati ma anche di una specifica cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle. Axios Cloud effettua - Backup del logo delle transazioni ogni 30 minuti - Backup completo ogni giorno alle 2.00 circa - Retention dei backup 8/10 gg
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 ripristino di prova.	

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.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup. Tramite Cobian Backup installato sul server con password BackUp1! Cadenza giornaliera, settimanale su NAS di rete e dispositivo esterno rimovibile Axios-Il backup effettuato da Axios è un file ZIP criptato che può essere ripristinato solo dalla scuola che lo ha generato. Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Axios. Axios Cloud consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transazioni Axios Cloud sono cifrate e protette da protocollo HTTPS
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.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup. Più specificatamente le copie di backup vengono copiate su supposto esterno off line e conservato in cassaforte ufficio presidenza Axios- è possibile effettuare una copia su un disco esterno e poi isolare quest'ultimo dal sistema semplicemente scollegando il cavo dal server. I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery

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 dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL). L'Istituto ha rilevato i seguenti ambiti di riservatezza che richiedono crittografia dei dati che è stata realizzata crittografando il volume che contiene le relative cartelle: sul Server: D:\Documenti Comuni D:\Documenti Personali.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi	

				che contengono informazioni rilevanti	
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.**	Vedi misura 8.9.2
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.	