Istituto Comprensivo Rita Levi-Montalcini
Sedi di San Piero Patti, Montalbano Elicona, Librizzi, Basicò
Via Profeta, 27 – San Piero Patti (Me) Tel. e Fax segreteria 0941/661033 C. F. 94007180832
Sito web www.icsanpieropatti.gov.it ***e-mail*** meic878001@istruzione.it ***posta certificata***meic878001@pec.istruzione.it

Misure minime di sicurezza ICT per le pubbliche amministrazioni.

(Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015) - Circolare 18 aprile 2017, n. 2/2017 in sostituzione della circolare n. 1/2017 del 17 marzo 2017.

Introduzione

La Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015, in considerazione *dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi*, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della Pubblica Amministrazione, sollecita *tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici* a *dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici*.

.Il nuovo CAD contiene disposizioni importanti relative alla sicurezza digitale (art.51) sia sulla continuità operativa, sia sul *disaster recovery*.

I due termini sembrano molto simili, ma vi è una differenza sostanziale, in quanto la prima è riferita all'organizzazione nel suo insieme (e quindi comprende anche le risorse umane, logistiche, i rischi ambientali, ecc.), mentre la seconda è riferita all'infrastruttura tecnico/informatica.

Le Pubbliche Amministrazioni devono predisporre appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività.

Per Disaster Recovery si intende quindi l'insieme di misure tecnologiche e organizzative dirette a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi a fronte di gravi emergenze. I disastri informatici con ingenti perdite di dati nella maggioranza dei casi provocano quindi il fallimento dell'organizzazione, per cui investire in opportune strategie di recupero diventa una scelta quasi obbligatoria e il Piano di disaster recovery è il documento che esplicita tali misure.

Piano dei Sistemi

L' Istituto può rispondere in maniera efficiente ad una situazione di emergenza analizzando:

1. i possibili livelli di disastro
2. la criticità dei sistemi/applicazioni.

Per una corretta applicazione del piano, i sistemi devono essere classificati secondo le seguenti definizioni:

- Critici: Le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa.
- Vitali: Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi

critici, e queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

- Delicati: Queste funzioni possono essere svolte manualmente, per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.
- Non-critici: Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Le procedure applicative, il software di sistema ed i file che sono classificati e documentati come critici, devono essere ripristinati prioritariamente. La criticità di applicazioni, software di sistema e dati, deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere (per esempio il periodo degli esami o dell'emissione dei pagamenti al personale).
Un piano d'emergenza deve valutare le strategie di ripristino più opportune su: siti alternativi, metodi di back up, sostituzione dei ruoli e responsabilità dei gruppo degli operatori.
La prolungata indisponibilità del servizio elaborativo derivante in particolare situazione di disastro, e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo.
Il "disastro" per il nostro Istituto può avere molte facce e sfumature, ne può colpire parti diverse (gli edifici, le risorse umane, i sistemi informatici, la documentazione informatica..) e può causare una quantità di danni ingente.
Limitando il campo di analisi alle problematiche di natura informatica e quindi ai sistemi (computer, server, apparati di rete, linee...) che gestiscono i dati e le attività del nostro Istituto Comprensivo i punti su cui concentrare l'attenzione quando si deve redarre o ipotizzare un piano di analisi del rischio e disaster recovery, sono vari:
Integrità fisica dei sistemi informatici, che può essere messa a repentaglio da calamità naturali (alluvioni, terremoti, fulmini...), cause accidentali (incendi, allagamenti, crollo di un edificio, caduta di un rack o un computer) o cause esterne (furto, rivolte e devastazioni,);
- Integrità delle infrastrutture necessarie al funzionamento dei sistemi: elettricità, connettività di rete, eventualmente impianto di condizionamento.
- Integrità dei dati da azioni di cracking, errori umani, virus, guasti hardware ecc.

Le minacce possibili sono molte e disparate e l'analisi dei relativi rischi deve considerare la loro probabilità e il valore dei dati o dei beni da proteggere. E' ovvio che qualsiasi dispositivo e misura di disaster recovery non deve costare più di quanto valgano i beni stessi da proteggere.
Partiamo dal presupposto che nel concepire un piano di disaster recovery si devono considerare vari aspetti:
- Costo delle procedure di sicurezza e protezione;
- Efficacia di queste misure in riferimento a diversi tipi di rischio;
- Analisi dei rischi, delle loro probabilità e livello di pericolo;
- Valore dei dati e dei beni da preservare.
- Tempi di ripristino della normale funzionalità, o quantomeno della funzionalità minima indispensabile dei sistemi;
- Costi per il ripristino
- Impatto delle relazioni con l'utenza e con gli stackeolder e metodi per limitarne il danno d'immagine.

Possiamo illustrare alcune precauzioni e indicazioni di massima per prepararci ad un disastro e limitarne o prevenirne i danni.
Hanno campi di applicazione e costi diversi, ma riassumono la maggior parte delle procedure e accorgimenti comunemente previsti:
- Backup dei dati. E' la condizione minima indispensabile: tutti i dati importanti vanno backuppati. Il mezzo su cui viene mantenuto il backup dovrebbe essere custodito in un luogo ed edificio fisicamente distante, test di ripristino e di verifica dell'integrità dei dati va svolta regolarmente così come un analisi di quali dati vengono effettivamente copiati e se questi sono tutti i dati da copiare.
- Impianto elettrico a norma, che offra inoltre sufficiente protezione da fulmini, con gruppi di continuità che suppliscano a brevi interruzioni di elettricità ed eventualmente generatori per far fronte a prolungati black-out.

- Impianto anti incendio a norma, in grado possibilmente di individuare ed estinguere automaticamente principi di incendio, senza compromettere la funzionalità dei dispositivi elettronici stessi.
- Linee di backup o di emergenza, in grado di subentrare in caso di guasti di varia natura, tali per cui ha senso utilizzare per il backup linee di fornitori diversi che si attestino su centrali diverse.
- Piccoli accorgimenti di costo minimo e buon senso per proteggere fisicamente i sistemi informatici: tenere le macchine sollevate da terra per limitare i danni da allagamento; fissarle a supporti per evitare cadute accidentali o causate da lievi scosse telluriche; mantenerle in un posto riparato (da luoghi di passaggio o di lavoro fisico); sistemare i cavi vari (alimentazione, rete, video...) in modo tale da evitare che qualcuno rischi di inciamparci e via dicendo.
- Assicurazione sui dispositivi elettronici e i dati, che copra rischi di varia natura e che copra sia i costi dei danni che quelli di ripristino.

Tecniche di Disaster Recovery

Sistemi e dati considerati importanti vengono ridondati in un "sito secondario" o "sito di Disaster Recovery" per far sì che, in caso di disastro (terremoto, inondazione, incendio,attacco haker, ecc...) sia tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile attivare le attività sul sito secondario al più presto e con la minima perdita di dati possibile.

In particolare, i livelli di servizio sono usualmente definiti dai due parametri:

1. L'RTO (Recovery Time Objerctive)è il tempo di inattività massimo consentito prima del ripristino di sistemi, applicazioni e funzioni. È l'elemento base per sviluppare strategie di ripristino efficaci, nonché per determinare quando e in che modo applicarle in caso di situazioni di emergenza.
2. L'RPO (Recovery Point Objective) rappresenta il momento più recente al quale sistemi e dati devono essere ripristinati dopo un'interruzione delle attività e stabilisce la quantità massima di dati che un'azienda accetta di sacrificare a seguito di un errore.

Entrambi rappresentano un obiettivo concreto per una soluzione per la continuità e per il ripristino di emergenza. Per migliorarli, occorre aumentare gli investimenti a livello di processi e tecnologie di rete e di archiviazione.

Replica sincrona

La replica sincrona garantisce la specularità dei dati presenti sui due siti poiché considera ultimata una transazione solo se i dati sono stati scritti sia sulla postazione locale che su quella remota. In caso di evento disastroso sulla sede principale, le operazioni sul sito di Disaster Recovery possono essere riavviate molto rapidamente

Replica asincrona

Per far fronte al limite di distanza tra i due siti imposto da tecniche sincrone, si ricorre spesso alla tecnica di copia asincrona. In questo caso il sito che si occuperà della replica può trovarsi anche a distanze notevoli. In questo modo è possibile affrontare anche disastri con ripercussioni su larga scala (come ad esempio forti scosse sismiche) che altrimenti potrebbero coinvolgere entrambi i siti (se questi si trovano nelle vicinanze).

Tecnica mista

Per garantire la disponibilità dei servizi anche in caso di *disastro esteso* e al tempo stesso ridurre al minimo la perdita di dati vitali si può ricorrere ad una soluzione di tipo misto: effettuare una copia sincrona su un sito intermedio relativamente vicino al primario e una copia asincrona su un sito a grande distanza.

Backup, copia di sicurezza o copia di riserva

Si indica la conservazione di materiale fatta per prevenire la perdita totale dei dati archiviati nella memoria di massa dei computer (siano essi postazioni di lavoro o server).

L'attività di backup è un aspetto fondamentale della gestione di un computer in caso di guasti, manomissioni, furti, ecc., ci si assicura che esista una copia dei dati ed è quasi sempre impostata in maniera automatica e svolta normalmente con una periodicità stabilita (per esempio una volta alla settimana). Devono inoltre essere conservati in accordo con le politiche di sicurezza dell'Istituto, per esempio, ma non solo, per questioni legate alla privacy.

Funzionalità programmi di backup

Un programma di backup deve fornire alcune funzionalità indispensabili ovvero:

- Copia immagine di un disco rigido
- Copia selettiva di cartelle e singolii files
- Criteri di selezione per la ricerca dei contenuti salvati e per la scelta di quelli che devono essere oggetto di backup (per data, tipo di file, autore della modifica);
- Compressione dei contenuti per ridurre la memoria richiesta per la copia;
- Protezione dei dati copiati tramite password e crittografia.

Per il nostro Istituto una caratteristica importante del backup è che questa attività non vada a sovrapporsi con l'operatività quotidiana, caricando i sistemi informatici e rallentando i tempi di risposta agli utenti. Per questo motivo vari sistemi di backup vengono usati quando normalmente gli utenti non lavorano su quel programma o sulla rete lan.
Per aumentare la velocità del backup, solitamente vengono applicati uno o più delle seguenti pratiche:

- Backup differenziale
  il backup differenziale registra solo le differenze tra un file da copiare con quello già copiato ed è utile per file di grandi dimensioni e che necessitano di un backup completo e quotidiano, come i database.
- Compressione
  la compressione è ottenuta tramite compressione dei dati (come quelli usati dai programmi più famosi come Winzip) prima che vengano registrati sul supporto di backup.

La conservazione dei supporti di backup in posizioni fisicamente distinte e separate dai sistemi in uso è strettamente necessaria, per evitare che in caso di evento disastroso, le copie vadano perse insieme agli originali.
Il ripristino dei dati copiati con l'operazione di backup è normalmente detto restore ed è l'amministratore di sistema o gli utenti che hanno diritti di accesso analoghi che provvedono al ripristino dei file richiesti.
Importante il Backup Remoto che è un servizio di salvataggio dati che esegue copie di backup, attraverso la linea internet, verso appositi server collegati al web. Nella maggioranza dei casi si usa tramite un software apposito. (per noi quello di Archivist). Per ottenere un processo realmente efficace è necessario pianificare e effettuare dei test di disaster recovery prima che sorga l'effettiva necessità ed organizzare preventivamente un politica di bakup.

Sicurezza Informatica

Si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione dell'integrità logico-funzionale di un sitema informatico e dei dati in esso contenuti Tale protezione è ottenuta attraverso misure di carattere organizzativo e tecnologico tese ad assicurarne l'accesso solo ad utenti registrati (autenticazione) la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (permessi), l'oscuramento (cifratura) e la correttezza (integrità) dei dati scambiati in una comunicazione nonchè la protezione del sistema da attacchi di software pericolosi. La sicurezza informatica è un problema sempre più sentito in ambito tecnico-informatico per via della sempre più spinta informatizzazione della società e dei servizi in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione degli attaccanti o *hacker*. L'interesse per la sicurezza dei sistemi informatici è dunque cresciuto negli ultimi anni proporzionalmente alla loro diffusione ed al loro ruolo occupato nella collettività. Risulta evidente che per capire le strategie migliori di sicurezza informatica sia necessario entrare nella mentalità dell'attaccante per poterne prevedere ed ostacolarne le mosse.
Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, come la robustezza del software di base e applicativo oltre alla affidabilità dei computer e degli ambienti in cui essi sono collocati. Il nostro server infatti è collocato in un ambiente chiuso con porta blindata al fine di garantire la massima sicurezza anche perchè il sistema informatico deve essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia da eventi accidentali; inoltre deve impedire l'accesso abusivo ai dati.

Perdita dei dati

Le cause di probabile perdita di dati nei sistemi informatici possono essere molteplici, ma in genere le possiamo raggruppare in due eventi:

1. Eventi indesiderati;

Qui ci sono quelli per lo più inaspettati come gli attacchi Hacking che vengono fatti tramite la rete internet da parte di utenti chiamati appunto dalla società cracker che si intrufolano abusivamente all'interno del sistema riuscendo ad ottenere piena disponibilità della macchina per gestire risorse e dati senza avere i giusti requisiti richiesti ma tramite software costruiti da loro stessi. Invece l'accesso a sistemi da parte di utenti non autorizzati a differenza di un attacco cracker viene usata la macchina e non la rete.

2. Eventi accidentali ovvero causati accidentalmente dall'utente stesso, tipo: uso difforme dal consigliato di un qualche sistema, guasti imprevisti, ecc…

Di seguito sono descritte chiaramente alcune indicazioni atte a garantire la sicurezza e l'integrità dei dati:

1. "I computer, inclusi i server, risultano tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti;
2. il server è collegato ad un gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica.
3. L'integrità dei dati sul server amministrativo è garantita da una procedura di backup che avviene settimanalmente attraverso un'unità di backup rimovibile
4. Tutti i PC della rete amministrativa vengono protetti da password per impedire al personale non autorizzato l'accesso alla rete.
5. L'introduzione di password di BIOS all'accensione dei personal computer, di password dello screen-saver e di password per l'accesso in rete determina un soddisfacente livello di protezione dei dati contenuti nei PC.
6. L'introduzione delle password e di apposito software antivirus inibisce ad estranei l'uso dei personal computer, attraverso i quali si accede alla posta elettronica.
7. Per l'invio di messaggi e-mail a più destinatari, sono state fornite al personale istruzioni affinché quale destinatario venga sempre indicata la scuola con l'indirizzo e-mail in CCN i destinatari, in modo che non possano essere individuati gli indirizzi email degli altri destinatari attraverso la funzione di proprietà."

   Nel DPS si affermava che per garantire la sicurezza delle aree in cui i dati sono trattati elettronicamente, sono state introdotte sui personal computer password di BIOS e password di rete, trimestralmente cambiate. Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabili dei dipendenti e degli alunni) sono ubicate in modo tale che ciascun addetto possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee.

   Sono state impartite disposizioni affinché, in assenza del personale, le stanze rimangano chiuse e le chiavi siano custodite dal personale collaboratore scolastico in servizio addetto alla vigilanza che, al termine del servizio, provvederà al deposito delle chiavi nell'apposito contenitore.

<u>Analisi del rischio</u>

Dobbiamo procedere necessariamente alla valutazione di tutte le possibili minacce in termini di probabilità di occorrenza e relativo danno potendo così stimare il relativo rischio: in base a tale valore si decide se, come e quali contromisure di sicurezza adottare.

La protezione dagli attacchi informatici viene ottenuta agendo su più livelli: innanzitutto a livello fisico e materiale, ponendo server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi; anche se questo accorgimento fa parte della sicurezza normale e non della "sicurezza informatica" Il secondo livello è normalmente quello logico che prevede l'autenticazione e l'autorizzazione di un'entità che rappresenta l'utente nel sistema. Successivamente al processo di autenticazione, le operazioni effettuate dall'utente sono tracciate e questo processo di monitoraggio delle attività è detto audit.

Tipi di sicurezza:

1. Sicurezza passiva:

   sono le tecniche e gli strumenti di tipo *difensivo*, ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

2. *Sicurezza attiva*
   sono tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (riservatezza) sia dalla possibilità che un utente non autorizzato possa modificarli (integrità)

È evidente che la sicurezza passiva e quella attiva siano tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema.
Le possibili tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico, realizzando più barriere fra l'attaccante e l'obiettivo.
Le violazioni possono essere molteplici: vi possono essere tentativi non autorizzati di accesso a zone riservate, furto di identità digitale o di file riservati, utilizzo di risorse che l'utente non dovrebbe potere utilizzare ecc. L'uso della firma digitale di un documento informatico è uno strumento efficace per confermare la verifica del soggetto proprietario del documento stesso e garanzia di veridicità.

<u>I programmi</u>
Già nella fase di progettazione si deve raggiungere il compromesso più funzionale tra l'efficienza d'uso del programma in questione e la sua capacità di "sopravvivenza" ad attacchi esterni e ad errori più o meno critici. Una volta prodotto il software si procede alla verifica del suo comportamento, in modo tale da effettuare una ricerca estesa dei difetti presenti, per passare poi alla loro eventuale eliminazione. Per essere efficace un programma deve essere controllato nelle sue specifiche e deve essere privo di difetti nel codice. Vi sono anche errori di programma che non alterano i file di sistema come per es. gli spyware e quindi non sono nocivi per il sistema stesso.
Altri strumenti di protezione

- Antivirus
  consente di proteggere il proprio computer da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC per verificare la presenza di virus e per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus correttamente configurato a tale scopo.
- Antispyware
  software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato utilissimo per la rimozione di "file spia", gli spyware appunto, in grado di carpire informazioni riguardanti le attività on line dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.
- Firewall
  garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente.
- Firma digitale e crittografia
  la firma digitale, e l'utilizzo di certificati digitali e crittografia per identificare l'autorità di certificazione, un sito, un soggetto o un software. Nel nostro Istituto si procede all'archiviazione digitale dei documenti in formato p7m e si indica all'utente la modalità di verifica della firma del dirigente Scolastico tramite l'utilizzo del software infocert. Aprire un file p7m (se pdf) con Adobe reader è possibile ma non offre la garanzia di verifica dell'identità di appartenenza.
- Steganografia
  Ha l'obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli, mentre per la crittografia è non rendere accessibili i dati nascosti a chi non conosce la chiave. La crittanalisi è l'attacco alla crittografia, che mira ad estrarre i dati cifrati senza chiave. L'obiettivo della steganalisi non è quindi quello di estrarre i dati nascosti, ma semplicemente di dimostrarne l'esistenza.
- Sistema di autenticazione sofisticato

Altro sistema, più sofisticato, è quello del riconoscimento dell'utente tramite l'utilizzo dell'impronta digitale come forma di autenticazione che potrebbe essere uno strumento molto sicuro.

- Sicurezza della rete Internet
  Con la crescita a dismisura di internet e e del "www", le problematiche di sicurezza si sono estese anche ad essa e sul fronte tecnico le misure di protezione in rete si concretizzano nell'uso di opportuni protocolli di rete come per es.HTTPS che non fanno altro che applicare i metodi crittografici su uno o più livelli di architettura di rete modello ISO OSI.
- Safer Internet
  "Safer Internet" introdotto dal parlamento Europeo nel 2005, vuole promuovere l'uso sicuro di internet soprattutto per i bambini: una rete europea di 21 linee nazionali attraverso le quali gli utenti finali possono denunciare anonimamente la presenza di contenuti illegali su internet. È indispensabile che genitori e insegnanti seguano con costanza i ragazzi nella navigazione, fornendo loro gli strumenti critici necessari per un approccio consapevole alla rete.

Allegato n 2 alla Circolare 18 aprile 2017, n. 2/2017, sostituzione della circolare n. 1/2017 del 17 marzo 2017.

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	Realizzato un archivio delle risorse attive.
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 operazione 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'aggiornamento avverrà quando saranno aggiunte nuove risorse
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.	Realizzato, tali dati sono inseriti nell'archivio delle risorse attive di cui al punto 1.1.1
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse 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'installazione di software è interdetta a tutti gli utenti. Eventuali nuovi software sono installati dall'amministratore 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.	Periodicamente saranno realizzate dei controlli per verificare che non siano stati installati software non previsti nell'elenco di cui al punto 2.1.1.
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.	Nel caso in cui un dispositivo risulti compromesso sarà ripristinato alla configurazione standard
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.	Le postazioni non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Le postazioni non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari.
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.	Le postazioni non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Le operazioni di amministrazione da remoto sono impedite. In caso di necessità tutte le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessioni protetti e sicuri, disabilitate al termine dell'intervento.
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.	Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo dei dispositivo
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
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.	I software di ricerca delle vulnerabilità sono regolarmente aggiornati
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.	Le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni sono configurati per avvenire in automatico
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono presenti sistemi separati dalla rete. Nel caso fossero presenti sarà garantito l'aggiornamento anche ai dispositivi air-gapped.
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.	Nel caso fossero saranno riscontrati dei problemi questi saranno risolti attraverso l'installazione di patch o ripristinando il dispositivo.
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.).	Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione
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 pericolo è molto basso avendo già previsto che ogni dispositivo si aggiorni automaticamente applicando in tal modo anche le eventuali patch di sicurezza.
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.	Si sta procedendo a verificare che l'accesso ai dispositivi da parte degli utenti non avvenga con accessi amministrativi e ove lo fosse a convertire l'utenza in una non amministrativa

5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso amministrativo ai dispositivi sarà utilizzato solo per operazioni di manutenzione
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.	Ogni dispositivo avrà una sola utenza amministrativa
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.	Dopo l'installazione di un nuovo dispositivo sarà cambiata la password di default dell'utente amministratore
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).	Le password utilizzate per le utenze amministrative sono lunghe almeno 14 caratteri e non banali
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 vengano sostituite con sufficiente frequenza (password aging).	Le password per le utenze amministrative saranno periodicamente aggiornate
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Le password per le utenze amministrative non saranno riutilizzate 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.	
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.	Si assicura che c'è la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutte le utenze amministrative sono nominative e riconducibili ad una sola persona
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 anonime saranno utilizzate solo per situazioni di emergenza.
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 sono conservate in un luogo sicuro (cassaforte) accessibili solo al responsabile della struttura e al dsga
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano per l'accesso 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 dispositivi sono installati sistemi atti a rilevare la presenza e bloccare l’esecuzione di malware e sono aggiornati automaticamente
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Ogni dispositivo ha attivo un Firewall
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.	La rete didattica e “pubblica” poggia su una linea dati indipendente da quella degli uffici amministrativi.
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.	Disattivata l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Disattivata l’esecuzione automatica dei contenuti dinamici presenti nei file.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Disattivata l’apertura automatica dei messaggi di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Disattivata l’anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Al momento della connessione di supporti rimovibili sarà eseguita automaticamente una scansione anti-malware
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.	Filtrato il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, attraverso l’impiego di strumenti antispam
8	9	2	M	Filtrare il contenuto del traffico web.	Sarà installato un proxy server che garantisca il filtraggio del contenuto

					del traffico web .
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).	Bloccata nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa
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.	Molti dispositivi operano in con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto. Per gli altri il backup è effettuato almeno settimanalmente.
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.	Per i dispositivi che operano con applicativi che memorizzano i dati sul cloud non è necessario implementare tale punto. Per gli altri 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.	Per i dispositivi che operano con applicativi che memorizzano i dati sul cloud non è necessario implementare tale punto; per gli altri 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	L'analisi è in via di implementazione. Per i dispositivi che operano con applicativi che memorizzano i dati sul cloud (es.argo) è stata richiesta ai

					fornitori la dichiarazione relativa alle misure implementate.
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.	Bloccato il traffico da e verso url presenti nella blacklist implementata sul Firewall.
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 presente documento è firmato digitalmente dal dirigente scolastico, dott.ssa Clotilde Graziano, protocollato, marcato temporalmente e conservato agli atti dell'Istituto comprensivo Rita Levi-Montalcini.