Ministero della Pubblica Istruzione

ISTITUTO COMPRENSIVO "SANDRO PERTINI"
Via Thomas Mann, 8-20162 Milano☏ 0288447715 - 🖷 0288447722
email: **MIIC8DF00R@ISTRUZIONE.IT** – PEC **MIIC8DF00R@PEC.ISTRUZIONE.it**
Cod.mecc. MIIC8DF00R C.F. 80124890155 Cod. Univoco Ufficio **UFTUDP**

Piano di sicurezza informatica

Sommario

Generalità

Scopo

Il presente documento contiene il piano di gestione dei rischi ICT dell'Istituto"E.Xxxxx" di Xxxxx (nel seguito Istituto) ai sensi dell'AgID Basic Security Control (ABSC) 4.8.1. delle Misure minime di sicurezza ICT per la Pubbliche Amministrazioni emesso dall'Agenzia per l'Italia Digitale (AgID) il 26 aprile 2016.

Storia delle modifiche

Ver.	Descrizione delle modifiche	Data emissione
1.0	Prima versione	11 marzo 2017

Riferimenti

ID	Estremi	Descrizione
[D1]	Direttiva 1 agosto 2015	Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015
[MM]	Misure minime	Misure minime di sicurezza ICT per le Pubbliche Amministrazioni del 26 aprile 2016

Acronimi

Acronimo	Descrizione
ABSC	AgID Basic Security Control(s)

Premessa

Le Misure minime di sicurezza ICT per le Pubbliche Amministrazioni prevedono la stesura di un piano di gestione dei rischi ICT per ciascuna Amministrazione, al fine di individuare i livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (ABSC 4.8.1). Il piano di gestione si basa su un monitoraggio della situazione esistente e individua gli interventi ritenuti idonei per l'adeguamento del sistema ICT al livello di protezione congruo con l'attività e le minacce cibernetiche che si possono ragionevolmente prefigurare per l'Istituto.

Il piano è elaborato in un momento di significativi cambiamenti sia sotto il profilo tecnologico che organizzativo. La rapida adozione delle misure riguardanti la digitalizzazione e dematerializzazione dell'azione amministrativa e i connessi obblighi di pubblicità e trasparenza richiedono un impiego particolarmente intenso dei sistemi ICT, che devono essere riprogettati in maniera da poter garantire un elevato standard di sicurezza, in un contesto di risorse economiche e strumentali particolarmente critico e in presenza di personale ancora non sufficientemente formato.

Sul lato didattico il Piano Nazionale Scuola Digitale stimola le istituzioni scolastiche ad individuare strategie e metodologie di insegnamento innovative, imperniate su un impiego diffuso delle tecnologie ICT, sia nella didattica disciplinare che nel potenziamento trasversale delle competenze digitali. Questo comporta l'installazione e la gestione

di nuovi dispositivi e un sostanziale ampliamento delle reti, per le quali è necessario prevedere adeguati sistemi di protezione.

Tenuto conto degli stringenti vincoli finanziari, strumentali e di risorse umane (totale assenza di figure in organico con uno specifico profilo tecnico informatico, non previsto per le scuole del primo ciclo d'istruzione), sulla base delle oggettive disponibilità dell'Amministrazione in linea generale l'obiettivo che ci si prefigge è il rispetto dell'implementazione delle ABSC al livello minimo.

L'analisi dei rischi segue la suddivisione presentata nel documento sulle Misure minime di sicurezza. Le prime tre classi riguardano la gestione aggiornata degli inventari dei dispositivi e dei software e la protezione della configurazione, la quarta classe l'analisi delle vulnerabilità, la quinta classe la gestione degli utenti, in particolare degli amministratori, la sesta classe le misure di protezione contro l'installazione di software malevolo, la settima classe la gestione delle copie di backup, la settima classe la protezione dei dati.

Il rischio è valutato come il prodotto dell'impatto del danno per la probabilità dell'evento. L'impatto è graduato su una scala da 1 a 4:

Valore	Livello	Definizione/criteri
1	Lieve	Il danno è totalmente reversibile; non si verificano perdita o esfiltrazione di informazioni
2	Medio	Il danno è totalmente reversibile; si verificano limitate perdite di dati comunque recuperabili ma non esfiltrazioni di informazioni
3	Grave	Il danno è solo parzialmente reversibile; si verificano perdite di dati non recuperabili o esfiltrazioni di informazioni
4	Gravissimo	Il danno è irreversibile; si verificano perdite di dati irrecuperabili o esfiltrazioni di informazioni critiche

La frequenza è valutata su una scala da 1 a 4:

Valore	Livello	Definizione/criteri
1	Improbabile	Eventi poco probabili e indipendenti; non sono noti episodi già verificatisi
2	Poco probabile	Il danno si verifica solo in presenza di circostanze particolari; sono noti solo rarissimi episodi già verificatisi
3	Probabile	La vulnerabilità del sistema ICT può provocare un danno anche se non in modo automatico o diretto; è già noto, all'interno dell'Istituto, qualche evento dannoso determinato dalla vulnerabilità del sistema ICT
4	Altamente probabile	Esiste una correlazione diretta fra la vulnerabilità del sistema ICT e il danno da essa causato; si sono già verificati danni per la stessa vulnerabilità rilevata in situazioni simili

Il presente documento è integrato nel più ampio quadro della definizione del sistema di gestione documentale dell'Istituto, di cui costituisce un allegato.

Analisi dei rischi e misure correttive

Classe 1 – Inventario dei dispositivi autorizzati e non autorizzati

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare
1.1.1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Utilizzo non autorizzato della connettività e delle risorse ICT dell'Istituto	**Verifica dello stato di aggiornamento del registro della rete attivato sull'antivirus cloud-based d'Istituto** (entro maggio 2017) **Ridefinizione dei compiti dei responsabili delle aule informatiche** (entro aprile 2017)
1.3.1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete	Utilizzo non autorizzato della connettività e delle risorse ICT dell'Istituto	**Aggiornamento tempestivo del registro della rete attivato sull'antivirus cloud-based d'Istituto** (misura immediata) **Ridefinizione dei compiti dei responsabili delle aule informatiche** (entro aprile 2017)
1.4.1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP	Utilizzo non autorizzato della connettività e delle risorse ICT dell'Istituto	**Aggiornamento tempestivo del registro della rete attivato sull'antivirus cloud-based d'Istituto** (misura immediata) **Verifica dei sistemi di log dei firewall e degli AP installati** (entro giugno 2017) **Ridefinizione dei compiti dei responsabili delle aule informatiche** (entro aprile 2017)

Soluzioni tecnologiche adottate

L'Istituto si è dotato in via sperimentale di un sistema antivirus e di monitoraggio della rete cloud-based che consente la gestione e il monitoraggio unificati dei dispositivi distribuiti nelle sei sedi dell'Istituto, registrando anche gli indirizzi IP.

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Utilizzo non autorizzato della connettività e delle risorse ICT dell'Istituto – Rete di segreteria	3	2	6
Utilizzo non autorizzato della connettività e delle risorse ICT dell'Istituto – Rete didattica	2	2	4

Osservazioni particolari

La metodologia BYOD sulle reti wireless della scuola richiede di soddisfare i Security Control ABSC 1.1.2 (Implementare ABSC 1.1.1 attraverso uno strumento automatico), 1.1.3 (Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie) ,1.2.1 (Implementare il "logging" delle operazioni del server DHCP), 1.2.2 (Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite), 1.4.2 (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).

L'implementazione di tali ABSC è particolarmente difficoltosa nell'Istituto, sia per la complessità di gestire sei reti in sei diversi plessi sia per l'esiguità delle risorse finanziarie e strumentali.

Al fine di mitigare il rischio si è pertanto proceduto con i seguenti passi:

1. Ai sensi dell'art. 515-bis della legge 28 dicembre 2015, n.208, le istituzioni scolastiche possono chiedere l'accesso alla rete del GARR, utilizzando la fibra e banda minima di 100 Mbs simmetrica per ciascuna sede, con un sostanziale salto di qualità rispetto alle attuali connessioni residenziali. Inoltre i protocolli di autenticazione (incluso EDUROAM) permettono di gestire in maniera coerente e unitaria l'accesso alla rete da ognuna delle sei sedi dell'Istituto. Si è pertanto proceduto a inviare domanda di adesione al GARR, che è stata tuttavia al momento respinta in quanto non è presente alcun punto di presenza GARR, né ente già collegato alla rete ad una distanza contenuta dalle scuole dell'Istituto (comunicazione del GARR nostro protocollo 359 del 19 gennaio 2017)
2. Si sta studiando una soluzione tecnica basata sull'utilizzo di un captive portal e autenticazione cloud-based sfuttando gli account @icxxxxx.it in dotazione all'istituto, previa quantificazione dei costi e della complessità tecnica.
3. Nelle more dell'implementazione di un sistema di autenticazione tracciabile della rete wireless, il rischio di utilizzo improprio delle risorse di connettività viene mitigato:
   a) attraverso misure gestionali (la connettività alla rete viene concessa esclusivamente al personale docente e ATA che ne faccia richiesta, previa comunicazione del MAC address dei dispositivi da autenticare); è vietato l'uso della connettività di rete ai terzi e agli studenti;

b) attraverso i sistemi di monitoraggio locali delle reti (firewall).

Non è presente al momento un sistema di conservazione dei log delle connessioni, criticità particolarmente seria per la quale è in corso un'interlocuzione con gli Enti locali al fine di individuare le appropriate misure tecniche.

Questo intervento ha carattere prioritario.

Classe 2 – Inventario dei software autorizzati e non autorizzati
Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare
2.1.1	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	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati	**Installazione di nuovi software consentita solo con privilegio di amministratore (una sola utenza)** (entro maggio 2017) **Omogeneizzazione dei software installati sulle macchine della rete di segreteria** (entro maggio 2017) **Ridefinizione dei compiti dei responsabili delle aule informatiche** (entro aprile 2017)
2.3.1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati	**Installazione di nuovi software consentita solo con privilegio di amministratore (una sola utenza)** (entro maggio 2017) **Monitoraggio dei sistemi con software antivirus** (misura immediata) **Ridefinizione dei compiti dei responsabili delle aule informatiche** (entro aprile 2017)

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete amministrativa	3	1	3

Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete didattica	2	1	2

Soluzioni tecnologiche adottate
L'Istituto si è dotato in via sperimentale di un sistema antivirus e di monitoraggio della rete cloud-based che consente la gestione e il monitoraggio unificati dei dispositivi distribuiti nelle sei sedi dell'Istituto, registrando anche le configurazioni dei SO in uso.

L'installazione di nuovi software è consentita solo all'unico utente con privilegio di amministratore.

Classe 3 – Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedure di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare
3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Aggiornamento automatico dei sistemi operativi**
3.2.1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione standard dei SO con applicazione automatica delle patch di sicurezza** **Aggiornamento costante del sito web alle ultime patch di sicurezza**
3.2.2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Applicazione della configurazione standard ai sistemi ripristinati**
3.3.1	Le immagini di installazione devono essere memorizzate off-line	Perdita delle immagini di installazione	**Inserimento della richiesta nei nuovi acquisti e generazione delle immagini di installazione per i sistemi della rete di segreteria**
3.4.1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi	Perdita e esfiltrazione di dati	**Connessione protetta già attiva per l'accesso al sito web** **Non sono al momento attive altre**

	di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri)		**connessioni remote**

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati – Rete amministrativa	3	1	3
Perdita delle immagini di installazione	3	2	6
Perdita e esfiltrazione di dati	4	1	4

Classe 4 – Valutazione e correzione continua delle vulnerabilità
Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare
4.1.1.	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 cone indicazioni delle vulnerabilità più critiche	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Scan dei sistemi con software automatici e l'antivirus cloud-based**
4.4.1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Aggiornamento automatico dell'antivirus e dei software di protezione di rete di sistema**
4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Aggiornamento automatico dei software del sistema operativo e degli applicativi** **Preferenza per sistemi cloud-based che garantiscono l'aggiornamento**

			all'ultima versione senza interventi manuali
4.5.2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Progettazione e configurazione del sistema di backup in modo che sia separato dalla rete e costantemente aggiornato** (entro maggio 2017)
4.7.1	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	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Verifica degli aggiornamenti Ridefinizione dei compiti dei responsabili delle aule informatiche** (entro maggio 2017)
4.8.1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia di apparati (e.g. server esposti, server interni, PdL, portatili, ecc.)	Mancata valutazione dei rischi	**Adozione del piano di gestione dei rischi** (entro maggio 2017)
4.8.2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche	Mancata valutazione dei rischi	**Implementare le patch per le vulnerabilità dei sistemi operativi e delle applicazioni prima sui server e poi sulle PdL**

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete amministrativa	3	1	3
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete didattica	2	1	2

Classe 5 – Uso appropriato dei privilegi di amministratore
Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare

5.1.1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi	Creazione di falle nella sicurezza ICT Perdita e violazione di dati	**Assegnazione dei privilegi di amministratore ad un solo utente**
5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Assegnazione dei privilegi di amministratore ad un solo utente** **Log degli accessi di amministratore** (entro maggio 2017)
5.2.1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Nomina amministratore di sistema**
5.3.1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative già in uso	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Assegnazione dei privilegi di amministratore ad un solo utente** (entro aprile 2017)
5.7.1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri)	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Aggiornamento della password per le utenze amministrative**
5.7.3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)	Aumento del rischio di accesso non autorizzato	**Adozione di un'adeguata policy delle password** (entro giugno 2017)
5.7.4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history)	Aumento del rischio di accesso non autorizzato	**Adozione di un'adeguata policy delle password** (entro giugno 2017)
5.10.1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali devono corrispondere credenziali diverse	Aumento del rischio di accesso non autorizzato	**Adozione di un'adeguata policy delle password** (entro giugno 2017)
5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona	Aumento del rischio di accesso non autorizzato	**Adozione di un'adeguata policy delle password** (entro giugno 2017)

5.10.3	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	Aumento del rischio di accesso non autorizzato	**Adozione di un'adeguata policy delle password** (entro giugno 2017)
5.11.1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza	Aumento del rischio di accesso non autorizzato	**Custodia delle password in luogo protetto a cura del DSGA**
5.11.2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private sino adeguatamente protette	Aumento del rischio di accesso non autorizzato	**Custodia dei certificati digitali in luogo protetto a cura del DSGA**

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete di segreteria	3	1	3
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete didattica	2	1	2

Classe 6 – Difese contro i malware
Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare
8.1.1	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	Creazione di falle nella sicurezza ICT Perdita e violazione di dati	**Impiego di un unico antivirus su tutti i sistemi connessi alla rete locale con funzionalità di aggiornamento automatico**

	mantenuti aggiornati in modo automatico		
8.1.2	Installare su tutti i dispositivi firewall ed IPS personali	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Installazione di firewall e IPS di sistema su ciascun dispositivo**
8.3.1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Definizione di una policy restrittiva degli accessi** (entro maggio 2017)
8.7.1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)
8.7.2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo e delle applicazioni Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)
8.7.3	Disattivare l'apertura automatica dei messaggi di posta elettronica	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo e delle applicazioni Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)
8.7.4	Disattivare l'anteprima automatica dei contenuti dei file	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo e delle applicazioni Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)
8.8.1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo e dell'antivirus Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)
8.9.1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo e dell'antivirus Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)

8.9.2	Filtrare il contenuto del traffico web	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo, del firewall e dell'antivirus Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)
8.9.3	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)	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Configurazione del sistema operativo e dell'antivirus Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete di segreteria	3	1	3
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita di dati – Rete didattica	2	1	2

Classe 7 – Copie di sicurezza
Procedure e strumenti necessari per produrre e mantenere copie di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare
10.1.1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema	Perdita di dati	**Adozione di un idoneo sistema di backup** (entro maggio 2017)
10.3.1	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	Perdita di dati Accesso non autorizzato ai dati	**Adozione di un idoneo sistema di backup in locale e in remoto Adozione di un'adeguata policy di disaster recovery** (entro maggio 2017)

10.3.4	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	Perdita di dati Accesso non autorizzato ai dati	**Adozione di un idoneo sistema di backup in locale e in remoto** **Adozione di un'adeguata policy di disaster recovery** (entro maggio 2017)

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Perdita di dati	4	2	8
Perdita di dati Accesso non autorizzato ai dati	4	2	8

Classe 8 – Protezione dei dati

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC_ID#	Descrizione	Rischi associati	Misure adottate o da adottare
13.1.1	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	Perdita di dati Accesso non autorizzato ai dati	**Cf. il manuale di gestione – sezione trattamento di dati riservati**
13.8.1	Bloccare il traffico da e verso url presenti in una blacklist	Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	**Verifica della configurazione dei firewall e del content filtering** **Istruzioni ai responsabili delle aule informatiche** (entro maggio 2017)

Rischi

Tipologia di rischio	Impatto	Frequenza	Rischio
Perdita di dati	4	2	8

Accesso non autorizzato ai dati			
Utilizzo improprio e non autorizzato dei sistemi ICT Perdita e violazione di dati	3	2	6