Istituto Comprensivo Via Linneo

Piano per la sicurezza ICT

Il Piano per la sicurezza ICT di codesto Istituto si compone dei seguenti documenti:

N.	Documento	Note
1	Manuale di Gestione del Protocollo Contenente anche: - Piano di continuità operativa e di disaster recovery - Piano della sicurezza informatica	Aggiornato quando necessario Reperibile agli atti
2	Certificazione Sussistenza Misure Minime nel trattamento dei dati sensibili - Dlgs 196/2003	Aggiornata a cadenza annuale Reperibile agli atti
3	Piano per la sicurezza ICT Contenente anche: - Piano di gestione dei rischi	Il presente documento Aggiornato quando necessario Reperibile agli atti
4	Relazione semestrale dell'Amministratore di Sistema	Aggiornata a cadenza semestrale Reperibile agli atti
5	Roadmap operativa	Aggiornata quando necessario Reperibile agli atti
6	Inventario dispositivi presenti nella rete	Aggiornato quando necessario Reperibile agli atti
7	Certificazione Sicurezza Amministratore di rete (Punto 5.1.3)	Aggiornata quando necessario Reperibile agli atti

Sommario

1 Il piano di sicurezza informatica

1.1 Definizione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dall'Istituto per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi, comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati.

Il presente Piano descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto anche di quanto disposto dal D. Lgs 196/2003, "Codice in materia di protezione dei dati personali" e del relativo Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza". Sono elencate inoltre le strategie ed i controlli adottati per assicurare al Sistema Informativo dell'Istituto un adeguato livello di sicurezza.

1.2 Obiettivi

Scopo del presente documento è descrivere la strategia che l'Istituto intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

- Confidenzialità: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.
- Integrità: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).
- Disponibilità: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte degli utenti.
- Accountability (Tracciabilità): tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.
Il Piano per la sicurezza informatica si basa attualmente sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati e documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice dell'Istituto.

Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

1.3 Responsabilità (figure coinvolte)

L'Ente predispone il Piano per la sicurezza informatica ai sensi dell'art.12 del DPCM 13 novembre 2014. Tale piano risulta essere comprensivo del Manuale di Gestione del Protocollo Informatico e del Piano per la sicurezza informatica dei documenti di cui all'art. 4 del DPCM 3 dicembre 2013, relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, predisposto dal Responsabile della gestione documentale nel rispetto del D.Lgs 196/2003 e del relativo Allegato B, d'intesa con il Responsabile del trattamento dei dati personali.

2 Il sistema informativo dell'Istituto

2.1 Tipologia di servizi offerti

Il Sistema Informativo dell'Istituto è rivolto a soddisfare tutte le esigenze di carattere informativo-informatico, sia dal punto di vista delle esigenze "interne" cioè sostanzialmente provenienti dai servizi interni all'amministrazione stessa sia, quasi sempre indirettamente, provenienti dall'utenza esterna all'amministrazione.

Nell'uno e nell'altro caso l'esigenza può essere soddisfatta o da un sistema effettivamente interno, fisicamente residente presso i sistemi informativi dell'Istituto, oppure tramite un sistema esterno, reso disponibile da altri enti e all'Istituto stesso accessibile con le opportune modalità.

2.2 Servizio informativo

2.2.1 Organizzazione

Nel contesto del Sistema Informativo ogni dipendente dell'Istituto deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Nella seguente tabella riassuntiva sono presentate le possibili tipologie di utenza del sistema:

Tipo di utente	Compiti / Responsabilità	Note
Addetti Assistenza Informatica esterna	Attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …). Verifiche sull'attuazione delle politiche	Sala Alessandro
Dipendenti	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati	Si faccia riferimento al mansionario specifico
Responsabili	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati. Vigilanza sul comportamento di dipendenti e addetti esterni	Pepe Gianfranco
Amministratore di Rete	Verifica su attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …). Verifiche sull'attuazione delle politiche	Sala Alessandro
Amministratore di Sistema	Verifica su politiche di sicurezza informatiche, fisiche e sociali. Reporting e certificazione regolari sullo stato della struttura	Easyteam.org SRL Via Walter Tobagi 2 20067 Tribiano (MI) Sig.Bassi Ferdinando
Responsabile dei registri di Protocollo	Tenuta dei Registri di Protocollo e loro corretta conservazione a norma	Pepe Gianfranco
Responsabile del servizio archivistico	Verifica su utilizzo, gestione e sicurezza degli archivi dell'Istituto, sia fisici sia digitali	Pepe Gianfranco
Responsabile delle copie di sicurezza	Verifica sull'effettivo funzionamento degli strumenti automatici di salvataggio dei dati. Reporting di anomalie all'Amministratore di Rete	Sala Alessandro

2.2.2 Addetti

Nel contesto del Sistema Informativo ogni dipendente dell'Istituto è, in varia misura e con compiti diversi, corresponsabile del Sistema Informativo nel suo complesso. Per quanto concerne la gestione vera e propria della progettazione ed implementazione delle politiche di sicurezza informatica è stata incaricata una società esterna specializzata in tale settore la quale svolge anche attività di assistenza hardware e software.

2.3 Infrastruttura tecnologica

2.3.1 Generalità

L'Infrastruttura Tecnologica dell'Istituto può essere schematizzata come segue:

Tipologia di apparati	**Descrizione**
Apparati server interni	Indichiamo in questa categoria tutti gli ambienti server di proprietà dell'Istituto o comunque gestiti direttamente, sia fisici che virtuali; tutti gli apparati server interni sono dislocati presso ambienti dell'Istituto
Apparati server esterni	Indichiamo in questa categoria tutti gli ambienti server, sia fisici che virtuali, gestiti da società esterne o da Enti esterni (MIUR, etc), in virtù di contratti stipulati con l'Istituto
Apparati di rete	Indichiamo in questa categoria tutti gli apparati (router, switch, hub, …) che concorrono alla connettività fra le sedi dell'Istituto (connettività interna), da e verso Internet (connettività pubblica verso l'esterno)

Apparati Storage, di Backup e Sicurezza	Indichiamo in questa categoria tutti gli apparati che concorrono specificatamente alla sicurezza (storage per backup, apparati firewall)
Infrastruttura di comunicazione	Intendiamo con questo termine l'insieme delle cablature che realizzano, per ogni sede, la connettività LAN, nonché l'infrastruttura di comunicazione fra le sedi (WAN), da e verso Internet
Apparati client	In questa categoria raggruppiamo tutti gli apparati (PC, Portatili, …) utilizzati dall'utenza interna per l'utilizzo dalle sedi territoriali o in connettività mobile dei servizi dell'Istituto

2.3.2 Struttura fisica

Il sistema informatico dell'Ente è così costituito:

- Server "Microsoft Windows 2008/2012" con funzioni di domain controller, file server, DNS e DHCP; sul quale sono installati i software "SISSI in Rete", "Axios" utilizzati dall'Ente
- NAS di rete utilizzato come unità di storage per tutti i dati soggetti a backup
- Server "EasyWIFI" utilizzato per la gestione del servizio connettività WIFI; con funzione integrata di Captive Portal per il controllo degli accessi WIFI e di proxy per il controllo della navigazione in Internet degli utenti collegati in WIFI

La quasi totalità degli elaboratori del domino ha installato come sistema operativo "Microsoft Windows 7" o "Microsoft Windows 10". E' possibile che per alcuni elaboratori in punti non critici della rete il sistema operativo installato sia ancora "Microsoft Windows XP". È in fase di valutazione dell'Ente l'aggiornamento del sistema operativo degli elaboratori con "Microsoft Windows XP" verso un sistema ancora in supporto.

Tutti i servizi sono installati sull'unico server di dominio e vengono effettuati due backup:

- un backup giornaliero su unità NAS
- un backup settimanale in Cloud presso la server farm dell'azienda titolare dell'incarico di Amministratore di Sistema

2.3.3 Architettura applicativa

Nel presente paragrafo descriviamo i principali software applicativi ed utilità in uso presso l'Istituto esplicitandone le caratteristiche salienti.

Dal punto di vista della architettura applicativa possiamo distinguere le seguenti categorie:

- Software centralizzati: trattasi di applicativi in uso a livello di Istituto, installati in unica posizione, su server presso la sede, o in uno degli ambienti virtuali disponibili, oppure resi disponibili da enti esterni e usufruibili dall'Istituto via Web. Quasi sempre la architettura elaborativa è a 3 livelli, composta da un database server, da un application (e web) server con accesso dei client via Web tramite la Intranet di Istituto.
- Software stand-alone: in questa categoria intendiamo software installati localmente sulle postazioni di lavoro, essenzialmente ai fini della produttività personale.

2.3.4 Sistema di Conservazione

Per quanto concerne il sistema di conservazione si fa rimando a quanto dettagliato nel Manuale di Gestione del Protocollo Informatico.

3 Politiche organizzative della sicurezza

3.1 Generalità

La definizione e l'applicazione delle politiche di sicurezza all'interno dell'Istituto richiedono l'individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d'implementazione e ad altri elementi specifici dell'ambiente e del sistema informativo.

L'applicazione delle politiche di sicurezza all'interno dell'Istituto richiede, inoltre, la definizione di processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti. I processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza.

Attualmente, l'individuazione della politica di sicurezza determina il modello logico della sicurezza fissandone gli obiettivi. L'individuazione degli obiettivi di sicurezza si traduce in obiettivi del sistema informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento. Inoltre, la sicurezza viene considerata da tutto il personale, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

3.1.1 Backup

I dati, in qualunque modo elaborati dal sistema informatico dell'Ente, sono salvati nella memoria centrale del Server "Microsoft Windows 2008/2012". È stato attivato un sistema di duplicazione e memorizzazione dei dati informatici presenti sulle strutture hardware dell'Istituto in modalità remota (backup remoto). Tale servizio è stato realizzato e viene interamente gestito dalla società intestataria del contratto di assistenza tecnica e informatica, incaricata con atto scritto ad effettuare tali attività.

3.2 Sicurezza logica

3.2.1 Introduzione

La sicurezza logica si occupa della protezione dell'informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l'individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi, in modo tale da garantirne la fruibilità nel tempo, che deve essere nel contempo aperta a tutti gli operatori necessari, ma limitata alle funzioni ad essi attribuite in un determinato momento.

3.2.2 Sistema di autenticazione

La credenziale di autenticazione consiste in un codice per l'identificazione dell'Incaricato (utente), associato a una parola chiave riservata e conosciuta solamente dal medesimo. La parola chiave è composta da almeno otto caratteri (numeri e lettere) e non contiene riferimenti agevolmente riconducibili all'Incaricato, il quale provvederà a modificarla al primo utilizzo.

Le credenziali di autenticazione sono affidate al controllo del Server "Microsoft Windows 2008/2012" che garantisce l'applicazione delle politiche di protezione e sicurezza in forma centralizzata ed automatizzata. La politica di centralizzazione del sistema informativo si appoggia al sistema integrato di Microsoft Active Directory ("insieme di servizi di rete - account utente, account computer, cartelle condivise, stampanti, etc. - adottati dai sistemi operativi organizzati in modo da consentirne la condivisione da parte dei client") tramite apposita profilazione degli utenti (gestione dei profili di autorizzazione).

Ad integrare la protezione sul sistema informativo, i software dell'Ente e gli applicativi web sono dotati di apposite procedure di accesso tramite username ("nome con il quale l'utente viene riconosciuto da un computer, da un programma o da un server") e password ("sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica"). Lo username è un identificativo che, insieme alla password, rappresenta le credenziali per accedere alle risorse informatiche o ad un sistema.

3.2.3 Antivirus e similari

Il sistema informatico dell'Ente e i dati personali da esso custoditi sono protetti contro il rischio di intrusione e contro l'azione di programmi di cui all'Articolo 615-quinquies del Codice Penale ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"), mediante l'attivazione:

- software antivirus centralizzato per il Server "Microsoft Windows 2008/2012" e i singoli elaboratori e, per la posta elettronica e navigazione, mediante l'antivirus integrato nel Server di posta elettronica ("software atto a rilevare ed eliminare virus informatici o altri programmi dannosi");
- software antispyware installato sui singoli elaboratori ("programma il cui scopo è quello di cercare ed eliminare dal sistema, tramite un'apposita scansione, i software che raccolgono informazioni riguardanti l'attività on-line di un utente - siti visitati, acquisti eseguiti in rete etc. - senza il suo consenso per farne un uso illegittimo");
- software antispam integrato nel Server di posta elettronica ("software che individua messaggi di posta elettronica indesiderati generalmente commerciali e/o pubblicitari").

I sistemi operativi degli elaboratori e del Server "Microsoft Windows 2008/2012" sono periodicamente aggiornati automaticamente mediante Windows Update con le opportune patch di sicurezza ("programma o parte di programma che aggiorna e corregge un software"), ad eventuale eccezione degli elaboratori con sistema operativo "Windows XP" per i quali non sono più disponibili gli aggiornamenti. Regolarmente e costantemente i Responsabili aggiornano, vigilano e controllano.

Gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono stati correttamente installati. I programmi sono stati impostati in modo da scaricare e aggiornare automaticamente le loro funzionalità garantendone quindi sempre la massima efficacia di funzionamento.

Al fine di prevenire intrusioni dall'esterno è stato installato e configurato un firewall hardware e su ciascun elaboratore è stato attivato il firewall software integrato nel sistema operativo "Microsoft Windows". Periodicamente sono stati eseguiti e verranno effettuati, nei tempi previsti dalla normativa, gli aggiornamenti sui sistemi di protezione.

4 Documenti e Banche dati

4.1 Sistema di gestione informatica dei documenti

Il DPR 445/2000, all'art. 1, comma 1, lett. r) definisce il Sistema di Gestione Informatica dei Documenti come "l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti". Tale sistema è attivato dall'Istituto su tutte le postazioni di lavoro degli uffici afferenti all'AOO e le abilitazioni all'utilizzo delle sue funzionalità sono stabilite e aggiornate a cura dei Responsabili individuati all'interno dell'AOO (Responsabile della gestione documentale, Responsabile dei sistemi informativi).

Per quanto concerne i software attraverso i quali viene registrato e gestito il patrimonio documentale dell'ente si fa riferimento alle indicazioni contenute nel Manuale di Gestione del Protocollo Informatico, così come anche per i seguenti argomenti:

- Protocollo informatico;
- Formazione dei documenti;
- Formati adottati;
- Sottoscrizioni;
- Validazione temporale;
- Metadati;
- Trasmissione dei documenti;
- Conservazione.

5 Trattamento dei dati personali - Analisi e gestione dei rischi

Per quanto concerne le politiche inerenti il trattamento dei dati personali e l'analisi dei rischi incombenti sui dati ed i documenti si fa esplicito rimando al Documento Privacy sulle politiche di sicurezza adottato dall'Istituto.

5.1 Gestione dei rischi

Al fine di minimizzare i rischi di corruzione, perdita, alterazione, furto dei dati, l'Istituto adotta le seguenti politiche di sicurezza.

5.1.1 Configurazioni dei sistemi

I sistemi in utilizzo sulla rete sono installati in configurazioni standard con software di comprovata stabilità e sicurezza. Il personale dipendente dell'Istituto è informato sui rischi dovuti all'installazione e all'utilizzo di software non conformi alle politiche di sicurezza o quantomeno non sufficientemente testati. I tecnici che materialmente eseguono le installazioni dei sistemi provvedono a disattivare tutti i servizi non necessari e a chiudere le porte TCP/UDP non necessarie al corretto funzionamento degli applicativi.

5.1.2 Archivio immagini

I tecnici che materialmente provvedono alle installazioni dei sistemi provvedono a mantenere un archivio delle immagini di installazione delle postazioni, al fine di minimizzare i tempi di fermo in caso di guasto e allo scopo di garantire l'installazione di una configurazione standard e comune a tutti i sistemi.

L'archivio delle immagini di installazione può essere conservato internamente alla struttura dell'Istituto, oppure in outsourcing presso i datacenter della società titolare del contratto di assistenza tecnica e informatica.

5.1.3 Sicurezza

L'Amministratore di rete certifica di essere:

- abbonato a servizi offline/online in materia di sicurezza informatica e a servizi offline/online di alert in materia di cyberattacchi, sicurezza informatica, virus
- in possesso delle certificazioni che gli consentono di operare sui software applicativi in uso nella rete LAN senza invalidarne le garanzie dei produttori
- (*se dato in outsorcing*) in possesso di un datacenter ove conserva a norma di legge le immagini di installazione dei sistemi dell'Istituto