ISTITUTO ISTRUZIONE SUPERIORE " ENRICO FERMI"
VIA COMO 435 - 97019 VITTORIA (RG)
Tel.: 0932 984360 - Fax: 0932 985895

TRATTAMENTO DEI DATI PERSONALI

MISURE DI SICUREZZA

LUOGO e DATA: VITTORIA, __ SETTEMBRE 2021

REVISIONE: N. 5 SETTEMBRE 2021

MOTIVAZIONE:

IL DATORE DI LAVORO

_____
(ROSARIA COSTANZO)

in collaborazione con

IL RESPONSABILE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE

_____
(GIUSEPPE TORNATORE)

per consultazione

IL RAPPRESENTANTE DEI LAVORATORI PER LA SICUREZZA

_____
(RAFFAELE INSACCO)

MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

Documento Programmatico sulla Sicurezza ai sensi del regolamento U.E. 679/16 e D.lgs 101/18

Premessa

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza, previsti regolamento U.E. 679/16 e D.lgs 101/18. Il piano prevede un'azione di formazione continua per tutti i dipendenti finalizzata a promuovere la cultura della sicurezza, indispensabile a garantire l'integrità e la riservatezza delle informazioni, siano esse conservate su supporti cartacei o informatici. In particolare tale piano persegue l'obiettivo di:

a) minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati sensibili;
b) minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni sensibili;
c) minimizzare la probabilità che i trattamenti dei dati sensibili siano modificati senza autorizzazione.

Il presente Documento Programmatico sulla Sicurezza delle Informazioni deve essere divulgato a tutti gli alunni e ai dipendenti della Scuola. Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Definizioni

DATO PERSONALE: qualunque informazione riferibile, anche indirettamente, a persona fisica, persona giuridica, ente o associazione.
DATO ANONIMO: il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.
DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati personali.
INTERESSATO: il soggetto al quale si riferiscono i dati personali.
RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali.
La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo
relativo alla sicurezza
RESPONSABILE DEL SISTEMA INFORMATIVO: il soggetto preposto dal titolare alla gestione della rete (amministratore di rete). La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali, deve inoltre conoscere le vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
TITOLARE: il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.
CREDENZIALI : le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente associato a una parola chiave riservata conosciuta solamente dal medesimo oppure di un dispositivo di

autenticazione in possesso ed uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave, oppure ad una caratteristica biometria dell'utente eventualmente associato a un codice identificativo o a una parola chiave.

Normativa di riferimento

regolamento U.E. 679/16 e D.lgs 101/18

Sedi

Il presente Documento Programmatico sulla Sicurezza delle Informazioni si applica all'IIS ENRICO FERMI DI VITTORIA

Titolare del trattamento

Il titolare del trattamento è l'istituto scolastico e la titolarità è esercitata dal Dirigente Scolastico, tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento e sicurezza.

Responsabili

Il **responsabile del trattamento dei dati personali e del sistema di rete**, ai fini della sicurezza, ha le seguenti responsabilità:
a) promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento Programmatico sulla Sicurezza dei Dati Personali;
b) informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;
c) promuovere lo svolgimento di un continuo programma di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza.
d) collaborare con il responsabile del sistema informativo.

Il **responsabile del sistema informativo (Responsabili di Laboratori, uno per laboratorio**) ha le seguenti responsabilità:
a) sovrintendere al funzionamento della rete del proprio Laboratorio, comprese le apparecchiature di protezione (firewall, filtri);
b) collaborare con il responsabile del trattamento dei dati personali;
c) monitorare lo stato dei sistemi informatici del laboratorio, con particolare attenzione alla sicurezza;
d) informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

Incaricati

Gli Incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:
a) svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del responsabile del trattamento dei dati;
b) non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
c) rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
d) informare il responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e non.

Il sistema informativo

Il Sistema Informativo d'istituto è costituito da cinque reti ciascuna protetta da Firewall, quindi non visibili l'una con l'altra. Per la connettività ad internet le cinque reti sono distribuite su due router con indirizzo pubblico diverso(ADSL alice Business).

Il nostro istituto è cablato mediante una rete WiFi esclusivamente per i docenti per fruire del servizio del registro elettronico, il sistema è sotto Proxy e l'accesso è mediante account.

Ogni aula del nostro istituto è dotata di una Lim con annesso un PC dove il docente potrà accedere solamente mediante il proprio account wifi.

Rete amministrativa

Tutti i posti di lavoro sono connessi in rete locale mediante uno switch e cablaggio Ethernet con protocollo TCP/IP statici. Sette personal computer sono riservati alla segreteria, uno al Direttore S.G.Amm.vi uno al vice preside e uno al dirigente scolastico. Il server si trova nella stanza del DSGA, con le apparecchiature di continuità. Tutti i computer sono dotati di indirizzo IP statico. La connettività internet avviene attraverso un firewall fisico di protezione con indirizzo IP statico in classe A.

Rete didattica

La rete didattica è costituita da 9 laboratori di informatica connessi in rete locale mediante switch e cablaggio Ethernet UTP RJ45 con protocollo TCP/IP staitoc e classe per ogni laboratorio. La connettività internet avviene attraverso un firewall con indirizzo IP statico in classe A.

INTERNET

Il collegamento ad INTERNET è controllato da due router ADSL 1 alice business con indirizzo pubblico 95.253.9.222 e ADSL2 con indirizzo pubblico 99.253.9.200.

Policy

Tutti gli utenti della rete devono rispettare le norme previste nel documento policy di utilizzo della rete.
La rete INTERNET della Scuola non può essere usata per:
-giocare in borsa
-visitare siti pornografici
-inserire nella "rete" dati sensibili e/o dati personali
-scaricare e diffondere programmi
-scaricare e diffondere file P2P (winmx, kazaa, ecc….)

Analisi del rischio

I rischi a cui sono sottoposti gli archivi presenti nella scuola si possono suddividere in rischi fisici e logici. Alla prima tipologia appartengono tutti gli archivi a supporto cartaceo e in parte quelli su supporto informatico. Alla seconda tipologia appartengono quelli che utilizzano elaboratori elettronici ed in specie quelli connessi in rete, sia locale che geografica.

Rischio fisico

Il furto o il danneggiamento degli archivi, la diffusione o distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre l'istituto IIS E. FERMI al rischio di violare regolamento U.E. 679/16 e D.lgs 101/18.

Archivi cartacei

Gli archivi cartacei sono conservati in armadi in locale chiuso a chiave ed appositamente predisposto e dotato di impianto antincendio, i rischi fisici a cui sono sottoposti sono i seguenti:
1) Accesso agli uffici e agli archivi di persone esterne alla Scuola;
2) Smarrimento per incuria da parte del personale;
3) Furto;
4) Visura e/o copiatura da parte di personale non autorizzato;
5) Perdita parziale o totale a causa di incendi o allagamenti;
6) Perdita parziale o totale per il degrado naturale del supporto (invecchiamento);
7) Atti di vandalismo.

Archivi informatici

Gli archivi informatizzati risiedono su elaboratori elettronici, i rischi fisici a cui sono soggetti sono i seguenti:

1) Distruzione fisica dell'elaboratore per eventi esterni allo stesso quali incendi, allagamenti, sbalzi di corrente;
2) Guasti hardware dell'elaboratore tali da impedire il recupero degli archivi che si trovano sugli hard disk;
3) Furto dell'elaboratore e/o dei supporti di backup dei dati;
4) Perdita di dati dovuta a imperizia del personale addetto;
5) Accesso agli elaboratori da parte di personale non autorizzato;
6) Interruzione dei servizi di connessione fisica alla rete (linee telefoniche, router, modem, switch, hub);
7) Atti di vandalismo.

Il nostro istituto ha stipulato un contratto con la società ARGO Software la quale ci fornisce il servizio di registro elettronico ma anche di mantenimento di tutti i dati personali dei nostri allievi.

Misure minime di sicurezza adottate

Le misure minime di sicurezza adottate dal nostro istituto si possono suddividere in due categorie:
1) destinate ai supporti cartacei;
2) destinate ai dati trattati in maniera informatica.

Archivi su supporto cartaceo

Le misure minime di sicurezza adottate per questo tipo di archivi sono così riassumibili.
a) Individuazione di tutti gli incaricati del trattamento delle informazioni.
b) Accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
c) Utilizzo di archivi con accesso selezionato;
d) Restituzione di atti e documenti al termine delle operazioni.

Norme per i dati sensibili e giudiziari

Utilizzo di armadi con controllo degli accessi agli archivi da parte del responsabile del trattamento dati.

Archivi su supporto informatico.

Le misure minime di sicurezza adottate per questo tipo di archivi si riferiscono a dati sensibili e non. Si ritiene che le misure adottate, molte delle quali in uso da anni, tendano a dare la massima copertura sui rischi a prescindere dalla tipologia dei dati.

Sicurezza fisica dei computer

L'accesso ai vari laboratori è consentito solo in presenza di docenti che si faranno carico del controllo del corretto utilizzo delle risorse informatiche.

Difesa da accessi non autorizzati da rete geografica

La connettività internet è garantita da firewall e software antivirus, per evitare l'accesso non autorizzato.

Codice identificativo degli utenti del sistema informativo

Tutti i pc dei laboratori sono dotati di account che verrà cambiato ad inizio di anno scolastico.

Le password di amministratore di ciascun laboratorio viene comunicato a inizio anno dal responsabile del laboratorio suddetto al DSGA conservato in busta chiusa nella cassaforte.

Le ID utente e le password per l'accesso al WIFI vengono gestite dal responsabile del trattamento dati.

Password

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente. Le regole di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati sensibili. Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo. Devono essere rispettate le seguenti regole per la definizione/gestione delle password:

1) la lunghezza minima della password è di 6 caratteri;

2) deve contenere almeno un carattere alfabetico ed uno numerico;

3) non deve contenere più di due caratteri identici consecutivi;

4) non deve essere simile alla password precedente;

5) non deve contenere l'user-id come parte della password;

6) deve essere cambiata all'inizio di ogni anno scolastico;

7) non deve essere comunicata ad altri utenti.

Il personale di Segreteria depositerà, in busta chiusa nella cassaforte, l' user id e la password del proprio PC.

Gli insegnanti sia per la password del registro elettronico sia per l'accesso al sistema wifi sono pienamente responsabili de i suddetti e hanno obbligo di salvaguardarli personalmente.

La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Salvataggio dei dati di backup

Il sistema di Backup viene effettuato da contratto con l'azienda che detiene i nostri dati personali.

Protezione da Virus informatici

Su tutti i Personal computer degli utenti e sui server è installato apposito software antivirus in grado di prevenire attacchi di virus informatici. Detto software controlla anche le caselle di posta elettronica ed i file di attacchi. L'utilizzo di software antivirus non è sufficiente da solo a garantire e prevenire attacchi di questo tipo.

Secondo l'esperienza comune, un virus è riconducibile a un codice eseguibile in grado di generare copie di se stesso e di introdursi in file di dati e nel codice di altri programmi.

L'introduzione di un virus può essere causata da un'operazione diretta quale il trasferimento di un file, la lettura di un e-mail, l'installazione di una applicazione da un supporto esterno (floppy, CD, zip) o attraverso internet o con un'azione indiretta tra cui l'apertura di un file in formato Word o Excel contenente un macro virus o la visualizzazione di una pagina Web contenente un applet o un componente Activex.

La raccomandazione è quella di lavorare, in particolare quando connessi ad internet (navigare, scaricare email ecc.), come utente generico, in questo modo eventuali danni provocati da virus saranno limitati ai file a cui l'utente ha il permesso di accesso; lavorare invece come utente privilegiato, ovvero come root, abbassa il livello di sicurezza intrinseca del sistema e permette, potenzialmente , ai virus di causare seri danni.

Formazione

Il buon funzionamento di un piano di sicurezza si realizza attraverso il coinvolgimento di tutto il personale della scuola creando la cultura necessaria a garantire e a preservare l'integrità e la riservatezza dell'intero patrimonio informativo, con particolare attenzione ai dati sensibili.

La formazione deve coinvolgere tutto il personale e si deve sviluppare attraverso le seguenti attività:

a) Seminari di illustrazione del presente piano (destinatari tutti);

b) Seminario sulla sicurezza destinato al personale di segreteria incaricato del trattamento dei dati

sensibili;

c) Destinazione di almeno il 40% del tempo di formazione nel settore informatica e sicurezza.

Incidente informatico

Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni. Tutti gli incaricati del trattamento dei dati sono pregati di avvisare tempestivamente i responsabili del sistema informativo e del trattamento nel caso in cui constatino le seguenti anomalie:

a) eccessivo uso degli user-id e password per l'accesso al wifi;

in questo caso si sospende l'account del docente si mette a conoscenza dell'accaduto e si provvede alla sostituzione della password

b) uso improprio della rete didattica a con ricaduta verso terzi

in questo caso si risale all'IP statico alla postazione quindi alla classe/allievo che era presente nel periodo contestato e si prendono provvedimenti dettati dal Dirigente scolastico

Aggiornamento del piano

Il presente piano è soggetto a revisione annua con scadenza entro il 31 dicembre di ogni anno; resta comunque valido fino a pubblicazione della successiva revisione. Il piano deve essere comunque aggiornato ogni qualvolta si verificano le seguenti condizioni:

a) modifiche all'assetto organizzativo della scuola ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;

b) danneggiamento o attacchi al patrimonio informativo dell'ente tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

Soggetti terzi

~~NetSense s.r.l. con sede legale in via Novaluce, 38 a Tremestieri Etneo (CT), partita IVA 04253850871~~