Isis Leopoldo II di Lorena

Grosseto

INDICE

PREMESSA

Ogni elemento contenuto in questo documento è stato elaborato, creato e predisposto in conformità alle nuove disposizioni in vigore al regolamento GDPR, ogni dato è stato misurato con il pieno rispetto della legittima realtà presente alla data di creazione del suddetto documento di comune accordo con il DATA CONTROLLER NOMEDATACONTROLLER e il DATA PROCESSOR (NOMEDATAPROCESSOR).

Le valutazioni, i rimedi e le condizioni che emergono sono connessi al principio della buona fede e della diligenza nell'attuare tutti i processi utili che vengono e verranno predisposti per renderne minima la probabilità di accadimento di eventi negativi.

La conservazione ed il trattamento del dato creato ed evidenziato nelle relazioni sottostanti determinano il PIA aziendale (Privacy Impact Assessment = censimento degli impatti privacy), in cui si vuole valutare la rischiosità complessiva, le azioni intraprese e da intraprendersi creando un documento che fotografa la situazione corrente.

Il nostro PIA nasce con un piano interno in cui viene stabilito in quale modo verrà mitigato il singolo rischio, coloro che sono incaricati di operare in tal senso e la gestione utile prevista per l'attività.

La mitigazione del Rischio, la privacy by design e gli strumenti di sicurezza utilizzati per il trattamento del dato personale vogliono diventare per l'Istituto un'importante base per l'approccio al Sistema Privacy.

Questo planning operativo è e sarà costantemente monitorato, avrà impatto sul Privacy Impact Assessment in cui andremo ad evidenziare i miglioramenti ottenuti e le eventuali ulteriori rischiosità subentrate nel corso dei periodi di esercizio.

In collaborazione con i nostri fornitori ci siamo dotati di un sistema informatico atto a censire, valutare, monitorare lo stato di rischio e implementando automaticamente il reporting necessario e le comunicazioni operative per le varie risorse.

Il nostro PIA è disegnato per raggiungere tre obiettivi:

- Garantire la conformità con le normative, e requisiti di politica legali applicabili per la privacy;
- Determinare i rischi e gli effetti che ne conseguono;
- Valutare le protezioni e eventuali processi alternativi per mitigare i potenziali rischi per la privacy.

Data Processor	Data Controller
NOMEDATAPROCESSOR	**NOMEDATACONTROLLER**

SISTEMI DI SICUREZZA PRESENTI IN ISTITUTO

Come noto la sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi. Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i data base, la trasmissione dati e l'elaborazione a distanza (informatica distribuita). In particolare non è da sottovalutare il rischio cui può andare incontro il trasferimento elettronico dei fondi tra banche oppure il trasferimento da uno Stato all'altro di intere basi di dati reso possibile dai moderni sistemi di trasmissione telematica.

Riguardo l'aspetto "sicurezza" connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati. Un bene può essere un'informazione, un servizio, una risorsa hardware o software e può avere diversi modi possibili di interazione con un soggetto (persona o processo). Se, ad esempio, il bene è un'informazione, ha senso considerare la lettura e la scrittura (intesa anche come modifica e cancellazione); se invece il bene è un servizio, l'interazione consiste nella fruizione delle funzioni offerte dal servizio stesso.

Nell'ottica del regolamento europeo n. 2016/679 (GDPR) questo concetto di sicurezza informatica ha assunto un significato più attuale alla luce anche dei sempre più numerosi attacchi ed incidenti di natura informatica che lasciano intuire una preoccupante tendenza alla crescita di tale fenomeno.

In particolare negli ultimi tempi si è assistito ad una rapida evoluzione della minaccia che possiamo definire "cibernetica" che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi: il primo è la quantità di

- risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati; il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo
- tale che questa possa procedere senza destare sospetti.

La combinazione di questi due fattori fa sì che, a prescindere dalle misure minime di sicurezza previste dal nostro codice in materia di protezione dei dati personali, (antivirus, firewall, difesa perimetrale, ecc.) bisogna fare particolare attenzione alle attività degli stessi utenti che devono rimanere sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

Ciò ovviamente comprende anche misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.

Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il Data Processor NOMEDATAPROCESSOR e il Data Controller NOMEDATACONTROLLER deve valutare anche il rischio informatico che può essere definito come il rischio di

danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

Nel GDPR un chiaro riferimento alle misure di sicurezza già si trova nell'art. 22 quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability).

A questo riguardo L'ISTITUTO in accordo con i propri consulenti IT ha delineato negli anni una protezione perimetrale che posa garantire standard adeguati di sicurezza e a tal proposito dichiara che il patrimonio aziendale relativo alla sicurezza è elencato qui sotto.

Antivirus Installati antivirus
commerciale

Firewall Installati firewall
software

Crittografia in Essere
nessuna crittografia

Dispositivi USB aziendali
dispositivo usb semplice

Cloud su webfarm certificati per quanto possibile

Protezione generica

Per quanto riguarda la parte delle risorse umane, L'istituto ha predisposto le seguenti misure per aumentare la consapevolezza dell'importanza dei dati:

- **consegna del mansionario**
- **formazione del personale**
- **nomina incaricato**
- **consegna delle policy**
- **autenticazione utenti**

Il Regolamento Generale sulla Protezione dei dati **si applicherà quindi sia ai dati detenuti in forma elettronica** (es. email e database) **che cartacea** (con poche eccezioni). Ciò significa che l'azienda è responsabile anche degli archivi cartacei che devono essere conservati in modo sicuro e, quando non più necessari, devono essere distrutti in sicurezza, grazie ad un distruggi documenti conforme alla nuova normativa. A questo proposito l'Istituto dichiara di aver predisposto la seguente protezione ambientale per il cartaceo:

- **armadi con chiave**
- **armadi blindati**
- **sistema di allarme**

La corretta conservazione di tutto l'apparato informatico rappresenta la prima difesa a protezione dei dati digitale. Una cattiva o non adeguata manutenzione dei sistemi informativi è spesso la causa di intrusioni e/o danneggiamenti con conseguente perdita di dati. A questo proposito l'Istituto dichiara di aver predisposto per tutte le apparecchiature informatiche la seguente policy:

- **Revisione annuale programmata di tutti i pc**
- **Manutenzione su caduta**
- **Riformattazione annuale e rebuilding dei pc nei laboratori degli studenti**
- **Visite periodica negli uffici**

L'Istituto dichiara di avere le seguenti sedi al cui interno sono presenti i seguenti uffici dove risiedono i dati sia digitali che cartacei.

SEDI E UFFICI

SEDE CENTRALE

- ,

UFFICIO DEL DIRIGENTE
UFFICIO DEL DSGA
UFFICIO PERSONALE
UFFICIO DEL PROTOCOLLO
UFFICIO DEI COLLABORATORI DEL DIRIGENTE
UFFICIO CONTABILITA' E BILANCIO
MAGAZZINO
AULE DOCENTI
UFFICIO VICEPRESIDE
UFFICIO AGENZIA FORMATIVA
UFFICIO DIRETTORE DI AZIENDA AGRARIA
PORTINERIA
UFFICIO ACCOGLIENZA AL PUBBLICO(RECEPTION)
UFFICIO ALUNNI

DATA PROCESSOR ESTERNI

vengono nominati tutti i data processor esterni all'istituto, le figure presenti hanno ricevuto la documentazione di informazione all'adeguamento al GDPR, hanno firmato ed accettato le lettere di incarico e i mansionari e le relative policy privacy

_____

L'ISTITUTO NON SI AVVALE dell'opera di data processor esterni.

DATA HANDLER

La **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile". Quindi anche se il GDPR non prevede la figura autonoma dell'incaricato, questo non vieta che se il titolare o il responsabile del trattamento, oltre a fare tutto quello che il regolamento espressamente prevede per "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile", vogliono anche fare (su base volontaria) una ulteriore responsabilizzazione di queste persone attraverso una specifica lettera di attribuzione di incarico e identificare queste persone utilizzando il termine "Incaricato" lo possono fare. Questa modalità operativa potrebbe anche essere considerata una buona prassi volta a poter ulteriormente sostenere la dimostrabilità della compliance al GDPR. Ma questa facoltà non deve essere intesa come un obbligo normativo come lo è invece per il Codice Privacy la nomina a incaricato prevista dall' art. 30, che al punto 2 prevede che la designazione dell'incaricato sia effettuata per iscritto e che nell'atto di nomina si debba individuare puntualmente l'ambito del trattamento consentito.

L'ISTITUTO in accordo con quanto affermato dal Garante per la protezione dei dati italiano ha deciso di nominare le figure dei data Handler, ovvero coloro che gestiscono e trattano il dato per nome dell'azienda. Di premette che ogni singolo individuo persona fisica o giuridica ha firmato e ricevuto le lettere di incarico, i mansionari e la policy privacy.
I dati relativi al personale vanno intesi alla data di redazione del presente documento e possono subire modifiche a fronte di trasferimenti e mobilità anche interna del personaledi personale
Pertanto se ne prevede una revisione periodica nei nomi e puntuale nel caso di accorpamento di mansioni

Altrettando dicasi per le competenze attribuite ancora da definire con direzione e DSGA

_____

Data handler DI MARTINO MARIA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler MASI PAOLA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler RAPINO VANIA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler VAGNOZZI PATRIZIA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler D'ELIA ROSANNA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler MILITO SILVANA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler MANFREDA MARINA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler SIMONI AMEDEO

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler BRAMERINI GUGLIELMO

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler BUGELLI LAURA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler VALENTINO ANGELO

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler PIANDELAGHI DANIELA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler FAVALI FABIO

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler GRAZIANO PATRIZIA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler CARLI MANUELA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler COMANDI ROBERTO

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler GIOVANNINI DANIELE

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler TESTA ELISABETTA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler CAMMARASANA SALVATORE

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler GAGGIOLI ROSSANA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

SITO WEB	SI		SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler COGNETTI GIULIA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA BILANCIO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
MAGAZZINOSI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AZIENDA AGRARIA	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler COLLABORATORI SCOLASTICI

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler DOCENTI

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA ALUNNI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PERSONALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA PROTOCOLLO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SEGRETERIA DIGITALE	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SITO WEB SI		SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

NOMINE INCARICATI

L' ISTITUTO per essere totalmente compliance alle direttive del nuovo regolamento europeo della privacy ha deciso di fare le seguenti nomine delle figure aziendali previste dalla normativa:

_____

Data controller

- GRAZIANO PATRIZIA

Data processor

- **CARLI MANUELA**

D.P.O.

- CAMNMARASANA SALVATORE

SISTEMI DI ELABORAZIONE

L'ISTITUTO identifica in questa sezione tutti i sistemi di elaborazione elettronici collegati e/o di proprietà dell'azienda, dichiarando che ogni strumento è conforme alla legge Europea e protetto con adeguati sistemi conformi alle direttive dettate dal GDPR.
I SISTEMI DI PROTEZIONE SONO DI SEGUITO DETTAGLIATI DAL DOCUMENTO PREVISTO DALL'AGID
Ricordiamo tra gli altri

- Profili differenziati utenti amministratori
- Antivirus e firewall attivi
- Backup quotidiano completo sulle aree LAN condivise

PC_DIRIGENTE_1

SEDE: SEDE CENTRALE
UFFICIO: UFFICIO DEL DIRIGENTE
AMBIENTE: Windows 10 Professional

DATA ACQUISTO: marzo 2018

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione apparecchiature SU CADUTA

PC_DSGA

SEDE: SEDE CENTRALE
UFFICIO: UFFICIO DEL DSGA
AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature SU CADUTA

PC_SERVER RETE LOCALE

SEDE: SEDE CENTRALE

UFFICIO: UFFICIO DEL DSGA
AMBIENTE: Windows 2003 server

DATA ACQUISTO: dicembre 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature SU CADUTA

PC_PERSONALE_1

SEDE: SEDE
UFFICIO: UFFICIO PERSONALE

AMBIENTE: Windows 10 Professional **DATA**
ACQUISTO: dicembre 2013

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_PERSONALE_1

SEDE: SEDE
UFFICIO: UFFICIO PERSONALE

AMBIENTE: Windows XP

DATA ACQUISTO: dicembre 2013

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_PERSONALE_2

SEDE: SEDE
UFFICIO: UFFICIO PERSONALE

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2015

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall

Manutenzione apparecchiature su caduta

PC_PERSONALE_3

SEDE: SEDE
UFFICIO: UFFICIO PERSONALE

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2015

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_ALUNNI_1

SEDE: SEDE
UFFICIO: UFFICIO ALUNNI

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_ALUNNI_2

SEDE: SEDE
UFFICIO: UFFICIO ALUNNI

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: APRILE 2018

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_ALUNNI3_1

SEDE: SEDE
UFFICIO: UFFICIO ALUNNI

AMBIENTE: Windows 7 Professional

DATA ACQUISTO: dicembre 2015

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_CONTABILITA'_1

SEDE: SEDE
UFFICIO: UFFICIO CONTABILITA'

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_CONTABILITA'_2

SEDE: SEDE
UFFICIO: UFFICIO CONTABILITA'

AMBIENTE: Windows 7 PROFESSIONAL

DATA ACQUISTO: dicembre 2015

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_CONTABILITA_3

SEDE: SEDE
UFFICIO: UFFICIO PERSONALE

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: MARZO 2018

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_PROTOCOLLO_1

SEDE: SEDE
UFFICIO: UFFICIO PROTOCOLLO

AMBIENTE: Windows XP Professional

DATA ACQUISTO: dicembre 2014

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_PROTOCOLLO_2

SEDE: SEDE
UFFICIO: UFFICIO PERSONALE

AMBIENTE: Windows 7 Professional

DATA ACQUISTO: dicembre 2015

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_COLLABORATORI ORARIO_1

SEDE: SEDE
UFFICIO: UFFICIO COLLABORATORI

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_COLLABORATORE DI SEDE_1

SEDE: SEDE
UFFICIO: UFFICIO COLLABORATORE DI SEDE

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: MARZO 2018

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_AULE DOCENTI_1 E 2

SEDE: SEDE
UFFICIO: AULE DOCENTI 6PC IDENTICI

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

PC_AULE DOCENTI_1

SEDE: VIA MEDA
UFFICIO: AULE DOCENTI 3PC IDENTICI

AMBIENTE: 2 Windows 10 Professional 1
WINDOWS 7

DATA ACQUISTO: dicembre 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

CENSIMENTO DA TERMINARE

PC_PERSONALE_1

SEDE: SEDE
UFFICIO: UFFICIO PERSONALE

AMBIENTE: Windows 10 Professional

DATA ACQUISTO: dicembre 2013

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Manutenzione periodica schedulata antivirus e firewall
Manutenzione apparecchiature su caduta

REGISTRO DEI TRATTAMENTI

L'Art. 30 del **Regolamento europeo in materia di protezione dei dati personali** nello specifico il par. 4 dell'art. 30, per il quale "su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo."

L'obbligo di documentazione della conformità della propria organizzazione alle prescrizioni della legge. Obbligo che grava anche sul responsabile, per i trattamenti che questi svolga per conto di un titolare.

L'autorità di controllo (Garante) è, d'altro canto, l'ente pubblico che ha titolo per richiedere la disponibilità del registro, al fine di esaminarlo.

L'obbligo di redazione e adozione del registro non è, tuttavia, generale. Il par. 5 dell'art. 30 specifica che esso non compete "alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."

L' ISTITUTO ha deciso tuttavia di attuare la redazione del registro come caldeggiato dal gruppo di lavoro Ex articolo 29 e dall'AGID ispirandosi alle seguenti ulteriori finalità:

- rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna; costituire lo strumento di pianificazione e controllo della politica della sicurezza di dati e banche
- di dati, tesa a garantire la loro integrità, riservatezza e disponibilità.

ALUNNI - GESTIONE ALUNNI E TUTORI

- **Queste le categorie interessati:** Scolari o studenti

- **Queste le categorie destinatari:** Istituti, scuole e università

- **I dati sono trattati in queste modalità:** Elettronica e cartacea

- **Le finalità del trattamento:**
  L' ISTITUTO, tramite il trattamento "AREA ALUNNI", tratta i sopraindicati dati per: **ADEMPIERE AGLI OBBLIGHI DI LEGGE SULLA ISTRUZIONE DEGLI ALUNNI**.

  Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **Il trattamento segue i seguenti criteri di liceità:**
  Interesse pubblico o esercizio di pubblici poteri, Obblighi di legge cui è soggetto il titolare.
  Per le seguenti motivazioni:
  Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "AREA ALUNNI" Vengono trattati dei minori:
  L' ISTITUTO, trattando dati di minori e siguramente minorenni tramite il trattamento "AREA ALUNNI", in osservanza dell'articolo 8 del GDPR si impegna a chiedere il consenso a chi ne esercita la patria potestà garantendo l'immediatezza nel comunicare eventuali modifiche al trattamento.

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "AREA ALUNNI" vengono trattati dati sanitari, biometrici e giudiziari per le seguenti motivazioni:
  Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

- **Durata del trattamento:**
  Il trattamento "AREA ALUNNI" ha durata indefinita:
  L' ISTITUTO dichiara il trattamento "AREA ALUNNI" con data indefinita in quanto continuerà a tenerlo in vita per poter proseguire la propria attività.
  Il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta raggiunte le finalità del presente trattamento, i dati verranno cancellati.

- **Profilazione:**

  Il trattamento non riguarda processi automatizzati o di profilazione

- **Trasferimento dei dati di questo trattamento:**

  I dati non vengono normalmente trasferiti in paesi extra UE

  Nel caso un ente faccia richiesta di tali dati (Puo accadere per studenti cittadini ucraini russi arabi sudamericani ecc) i dipendenti prima di rilasciare tali dati richiedono ina liberatoria su apposito modello tradotto in inglese

AREA BILANCIO - GESTIONE ANAGRAFICA FORNITORI E DIPENDENTI

- **Queste le categorie interessati:** Personale dipendente,Fornitori

- **Queste le categorie destinatari:**
  Consulenti e liberi professionisti in forma singola o associata,Istituti, scuole e università,Enti previdenziali ed assistenziali,Fornitori

- **I dati sono trattati in queste modalità:** Elettronica e cartacea

- **Le finalità del trattamento:**
  L' ISTITUTO, tramite il trattamento "AREA BILANCIO", tratta i sopraindicati dati per: **LA GESTIONE DEGLI INCASSI E DEL CICLO PASSIVO DAGLI ORDINI AL PAGAMENTO DELLE FATTURE E PAGAMENTO COMPENSI AD ESPERTI ESTERNI, PERSONALE INTERNO E VERSAMENTO RITENUTE FISCALI E PREVIDENZIALI AGLI ENTI PREPOSTI.**

  Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **Il trattamento segue i seguenti criteri di liceità:**
  Adempimento obblighi contrattuali, Obblighi di legge cui è soggetto il titolare, L'interessato ha espresso il consenso al trattamento.
  Per le seguenti motivazioni:

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "AREA BILANCIO" non vengono trattati dei minori

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "AREA BILANCIO" non vengono trattati dati sanitari, biometrici e giudiziari

- **Durata del trattamento:**
  Il trattamento "AREA BILANCIO" ha durata indefinita:
  L' ISTITUTO dichiara il trattamento "AREA BILANCIO" con data indefinita in quanto continuerà a tenerlo in vita per poter proseguire la propria attività.
  Il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta raggiunte le finalità del presente trattamento, i dati verranno cancellati.

- **Profilazione:**
  Il trattamento non riguarda processi automatizzati o di profilazione

- **Trasferimento dei dati di questo trattamento:**
  I dati non vengono trasferiti in paesi extra UE

PERSONALE - GESTIONE DATI ANAGRAFICI E FASCICOLO PERSONALE DEI DIPENDENTI

- **Queste le categorie interessati:** Personale dipendente,Insegnanti

- **Queste le categorie destinatari:** Istituti, scuole e università

- **I dati sono trattati in queste modalità:** Elettronica e cartacea

- **Le finalità del trattamento:**
  L' ISTITUTO ,tramite il trattamento "AREA PERSONALE", tratta i sopraindicati dati per: **LA GESTIONE DEGLI ATTI AMMINISTRATIVI DEL PERSONALE DIPENDENTE RIFERITI ALLA CARRIERA, ASSENZE ,FORMAZIONE ECC.**

  Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **Il trattamento segue i seguenti criteri di liceità:**
  Adempimento obblighi contrattuali, Obblighi di legge cui è soggetto il titolare, L'interessato ha espresso il consenso al trattamento. **Per le seguenti motivazioni:**
  Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "AREA PERSONALE" non vengono trattati dei minori

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "AREA PERSONALE" vengono trattati dati sanitari, biometrici e giudiziari per le seguenti motivazioni:
  Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

- **Durata del trattamento:**
  Il trattamento "AREA PERSONALE" ha durata indefinita:
  L' ISTITUTO dichiara il trattamento "AREA PERSONALE" con data indefinita in quanto continuerà a tenerlo in vita per poter proseguire la propria attività.
  Il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta raggiunte le finalità del presente trattamento, i dati verranno archiviati.

- **Profilazione:**
  Il trattamento non riguarda processi automatizzati o di profilazione

- **Trasferimento dei dati di questo trattamento:**
  I dati non vengono trasferiti in paesi extra UE

PROTOCOLLO/ SEGRETERIA DIGITALE - GESTIONE CORRISPONDENZA IN INGRESSO E USCITA

- **Queste le categorie interessati:**
  Personale dipendente,Lavoratori autonomi,Fornitori,Soggetti o organismi pubblici,Scolari o studenti,Insegnanti

- **Queste le categorie destinatari:**
  Enti locali,Consulenti e liberi professionisti in forma singola o associata,Società e imprese,Banche e istituti di credito,Organi istituzionali,Istituti, scuole e università,Enti previdenziali ed assistenziali,Altre amministrazioni pubbliche,Fornitori

- **I dati sono trattati in queste modalità:** Elettronica e cartacea

- **Le finalità del trattamento:**
  L' ISTITUTO, tramite il trattamento "AREA PROTOCOLLO/ SEGRETERIA DIGITALE", tratta i sopraindicati dati per:
  Gestione della corrispondenza in ingresso e uscita da posta Elettronica (peo), certificata (pec) e da posta cartacea, con smistamento presso gli uffici dell'Istituto

  Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **Il trattamento segue i seguenti criteri di liceità:**
  Interesse legittimo prevalente del titolare, Obblighi di legge cui è soggetto il titolare.
  Per le seguenti motivazioni:
  Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "AREA PROTOCOLLO/SEGRETERIA DIGITALE" non vengono trattati dei minori

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "AREA PROTOCOLLO/ SEGRETERIA DIGITALE" non vengono trattati dati sanitari, biometrici e giudiziari

- **Durata del trattamento:**
  Il trattamento "AREA PROTOCOLLO/SEGRETERIA DIGITALE" ha durata indefinita:
  L' ISTITUTO dichiara il trattamento "AREA PROTOCOLLO/ SEGRETERIA DIGITALE" con data indefinita in quanto continuerà a tenerlo in vita per poter proseguire la propria attività.
  Il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta raggiunte le finalità del presente trattamento, i dati verranno archiviati.

- **Profilazione:**

Il trattamento non riguarda processi automatizzati o di profilazione

- **Trasferimento dei dati di questo trattamento:**
  I dati non vengono trasferiti in paesi extra UE

RETRIBUZIONI - GESTIONE COMPENSI AL PERSONALE

- **Queste le categorie interessati:** Personale dipendente,Insegnanti

- **Queste le categorie destinatari:**
  Banche e istituti di credito,Istituti, scuole e università,Enti previdenziali ed assistenziali

- **I dati sono trattati in queste modalità:** Elettronica e cartacea

- **Le finalità del trattamento:**
  L' ISTITUTO, tramite il trattamento "AREA RETRIBUZIONI", tratta i sopraindicati dati per: **LA GESTIONE DEI COMPENSI ACCESSORI SPETTANTI AL PERSONALE DIPENDENTE NELL'AMBITO DELLE ATTIVITA' PREVISTE DAL PTOF, COMPETENZE MENSILI AL PERSONALE SUPPLENTE, VERSAMENTO RITENUTE PREVIDENZIALI E FISCALI AGLI ENTI INTERESSATI, DICHIARAZIONI CONTRIBUTIVE E FISCALI CORRELATE.**.

  Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **Il trattamento segue i seguenti criteri di liceità:**
  Adempimento obblighi contrattuali, Obblighi di legge cui è soggetto il titolare, L'interessato ha espresso il consenso al trattamento. **Per le seguenti motivazioni:**
  Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "AREA RETRIBUZIONI" non vengono trattati dei minori

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "AREA RETRIBUZIONI" non vengono trattati dati sanitari, biometrici e giudiziari

- **Durata del trattamento:**
  Il trattamento "AREA RETRIBUZIONI" ha durata indefinita:
  L' ISTITUTO dichiara il trattamento "AREA RETRIBUZIONI" con data indefinita in quanto continuerà a tenerlo in vita per poter proseguire la propria attività.
  Il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta raggiunte le finalità del presente trattamento, i dati verranno archiviati.

- **Profilazione:**
  Il trattamento non riguarda processi automatizzati o di profilazione

- **Trasferimento dei dati di questo trattamento:**

I dati non vengono trasferiti in paesi extra UE

BANCHE DATI

L'ISTITUTO identifica in questa sezione tutte le banche dati, i campi che le compongono e la tipologia di questi ultimi. Tali banche dati vengono utilizzate nei trattamenti secondo le direttive dettate dal GDPR.

Trattamento "AREA ALUNNI"

SIDI

ANAGRAFE ALUNNI (Personali)
CERTIFICATI DI MALATTIA (Personali) - DATI ANAGRAFICI ALUNNI (Personali) - DATI ANAGRAFICI TUTORI (Personali)

DATI ANAGRAFICI ALUNNI (Personali) - DATI ANAGRAFICI TUTORI (Personali) - DATI VALUTAZIONE ALUNNI (Personali)

Trattamento "AREA BILANCIO"

SIDI

ANAGRAFE DEL PERSONALE (Personali) - ANAGRAFE FORNITORI (Personali) - MODALITA DI PAGAMENTO (Personali)

Trattamento "AREA PERSONALE"

NOIPA sissi

ANAGRAFE PERSONALE GESTITO DAL MEF (Personali)

PER LA PA

DATI ANAGRAFICI PERS. DIP. PERMESSI LEGGE 104/92 (Personali) **SIDI**
ANAGRAFE DEL PERSONALE (Personali)

SISSI

CERTIFICATI DI MALATTIA (Personali) - DATI ANAGRAFICI DEL PERSONALE (Personali)

Trattamento "AREA PROTOCOLLO/SEGRETERIA DIGITALE"

ANAGRAFICO MITTENTI/DESTINATARI POSTA (Personali) - DATI ANAGRAFICI ALUNNI (Personali) - DATI ANAGRAFICI DEL PERSONALE (Personali) - DATI ANAGRAFICI TUTORI (Personali)

Trattamento "AREA RETRIBUZIONI"

DATI ANAGRAFICI PERSONALE NDR (Personali) - RETRIBUZIONI, SERVIZI AI FINI DEL TFR E FERIE (Personali)

NOIPA

ANAGRAFE PERSONALE GESTITO DAL MEF (Personali) - RETRIBUZIONI CORRISPOSTE DAL MEF (Personali)

SIDI

ANAGRAFE DEL PERSONALE (Personali)

SISSI

DATI ANAGRAFICI DEL PERSONALE (Personali) - MODALITA' DI PAGAMENTO (Personali)

PRIVACY IMPACT ASSESSMENT

L' ISTITUTO espone qui di seguito le valutazioni di impatto sulla privacy dei trattamenti sopra elencati.

PRIVACY IMPACT ASSESSMENT TRATTAMENTO **AREA ALUNNI**

L' ISTITUTO con sede in Grosseto, nell'ottica di assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

ISTITUTO effettua il seguente trattamento: **AREA ALUNNI** meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
tramite il trattamento "AREA ALUNNI", tratta i sopraindicati dati per: **ADEMPIERE AGLI OBBLIGHI DI LEGGE SULLA ISTRUZIONE DEGLI ALUNNI**.

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

Dopo attenta valutazione di comune accordo con il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR; ISTITUTO considera questo trattamento essenziale e indispensabile per il corretto perseguimento dell'oggetto sociale cosi come la sua proporzionalità e non eccedenza. A tale proposito è stato effettuato un ridimensionamento delle banche dati **SIDI, SISSI, SPAGGIARI,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

ISTITUTO per garantire una sempre maggiore libertà dei diritti e sicurezza dei dati agli interessati si sforza continuamente di trovare le migliori mitigazioni a tutti i rischi ai quali i dati in nostro possesso possono andare incontro.

in particolare segnaliamo di aver individuato i seguenti rischi:
Accessi esterni non autorizzati
Allagamento
Alterazione dolosa o colposa dati avvenuta internamente
Attacco Ransomware
Azione di virus informatici o di codici malefici
Carenza di consapevolezza, disattenzione o incuria
Comunicazione illegale dei dati e dei documenti
Copia abusiva

Degrado dei supporti e delle apparecchiature
Cortocircuito elettrico
Distruzione di apparecchiature o di supporti
Fenomeni meteorologici
Furto Apparecchiature
Incendio
Ingressi non autorizzati a locali/aree ad accesso ristretto
Malfunzionamento hardware o software
Mancanza di continuità di alimentazione elettrica
Mancata manutenzione del sistema informativo
Perdita credenziali
Polvere, corrosione o gelo
Possibile rottura dell'hard disk o altri componenti hardware/software
Accessi tramite dispositivi mobili non autorizzati
Errato utilizzo doloso o colposo del software
Mancata distruzione o restituzione dei supporti raggiunta la finalità

Dei sopraelencati rischi, in accordo con i consulenti IT abbiamo posto in essere le seguenti mitigazioni:**Firewall Software**
Antivirus commerciale
Manutenzione spot apparecchiature sistema di backup in cloude su supporti esterni remoti ai pc e ai server

Tali mitigazioni danno al trattamento **AREA ALUNNI** una compliance alla sicurezza del **85%**

La sua valutazione ci porta ad affermare che per importanza dei dati di questo trattamento e principio di proporzionalità il trattamento stesso ha una valutazione di impatto più che accettabile.
Tuttavia segnaliamo anche che sono stati individuate alcune criticità che possono mettere a rischio i dati anche se in misura minimale. A questo proposito segnaliamo:
Dispositivo USB semplice
Nessuna crittografia

Infine, per sensibilizzare tutti i dipendenti incaricati al trattamento ad una sempre maggiore attenzione alla protezione dei dati abbiamo realizzato e consegnato a ciascuno una privacy policy la cui visione è disponibile nella sezione privacy policy.
Il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR dichiarano di aver ottemperato a quanto richiesto dal GDPR in base al principio di proporzionalità, all'importanza e la quantità dei dati in loro possesso e ai fatturati aziendali

grosseto, li 18/05/2018

Il Data Controller NOMEDATACONTROLLER .....

Il Data Processor NOMEDATAPROCESSOR .....

BILANCIO

assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

L'ISTITUTO effettua il seguente trattamento: **AREA BILANCIO** meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L' ISTITUTO, tramite il trattamento "AREA BILANCIO", tratta i sopraindicati dati per: **LA GESTIONE DEGLI INCASSI E DEL CICLO PASSIVO DAGLI ORDINI AL PAGAMENTO DELLE FATTURE E PAGAMENTO COMPENSI AD ESPERTI ESTERNI, PERSONALE INTERNO E VERSAMENTO RITENUTE FISCALI E PREVIDENZIALI AGLI ENTI PREPOSTI.**

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

Dopo attenta valutazione di comune accordo con il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR; ISTITUTO considera questo trattamento essenziale e indispensabile per il corretto perseguimento dell'oggetto sociale cosi come la sua proporzionalità e non eccedenza. A tale proposito è stato effettuato un ridimensionamento delle banche dati **SIDI,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

ISTITUTO, per garantire una sempre maggiore libertà dei diritti e sicurezza dei dati agli interessati si sforza continuamente di trovare le migliori mitigazioni a tutti i rischi ai quali i dati in nostro possesso possono andare incontro.

in particolare segnaliamo di aver individuato i seguenti rischi:
Accessi esterni non autorizzati
Allagamento
Alterazione dolosa o colposa dati avvenuta internamente
Attacco Ransomware
Azione di virus informatici o di codici malefici
Carenza di consapevolezza, disattenzione o incuria
Comunicazione illegale dei dati e dei documenti
Copia abusiva
Degrado dei supporti e delle apparecchiature
Cortocircuito elettrico
Distruzione di apparecchiature o di supporti
Fenomeni meteorologici
Furto Apparecchiature
Incendio
Ingressi non autorizzati a locali/aree ad accesso ristretto
Malfunzionamento hardware o software

Mancanza di continuità di alimentazione elettrica
Mancata manutenzione del sistema informativo
Perdita credenziali
Polvere, corrosione o gelo
Possibile rottura dell'hard disk o altri componenti hardware/software
Accessi tramite dispositivi mobili non autorizzati
Errato utilizzo doloso o colposo del software
Mancata distruzione o restituzione dei supporti raggiunta la finalità

Dei sopraelencati rischi, in accordo con i consulenti IT abbiamo posto in essere le seguenti mitigazioni:**Firewall Software**
Antivirus commerciale gruppi
di continuità
Manutenzione spot apparecchiature sistema di
backup in cloud

Tali mitigazioni danno al trattamento **AREA BILANCIO** una compliance alla sicurezza del **53%**

La sua valutazione ci porta ad affermare che per importanza dei dati di questo trattamento e principio di proporzionalità il trattamento stesso ha una valutazione di impatto più che accettabile.
Tuttavia segnaliamo anche che sono stati individuate alcune criticità che possono mettere a rischio i dati anche se in misura minimale. A questo proposito segnaliamo:
Dispositivo USB semplice
Nessuna crittografia

Infine, per sensibilizzare tutti i dipendenti incaricati al trattamento ad una sempre maggiore attenzione alla protezione dei dati abbiamo realizzato e consegnato a ciascuno una privacy policy la cui visione è disponibile nella sezione privacy policy.
Il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR dichiarano di aver ottemperato a quanto richiesto dal GDPR in base al principio di proporzionalità, all'importanza e la quantità dei dati in loro possesso e ai fatturati aziendali

Grosseto, li 18/05/2018

Il Data Controller NOMEDATACONTROLLER .....

Il Data Processor NOMEDATAPROCESSOR .....

assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

ISTITUTO effettua il seguente trattamento: **AREA PERSONALE**
meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L' ISTITUTO, tramite il trattamento "AREA PERSONALE", tratta i sopraindicati dati per: **LA GESTIONE DEGLI ATTI AMMINISTRATIVI DEL PERSONALE DIPENDENTE RIFERITI ALLA CARRIERA, ASSENZE ,FORMAZIONE ECC.**

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

Dopo attenta valutazione di comune accordo con il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR; L'ISTITUTO considera questo trattamento essenziale e indispensabile per il corretto perseguimento dell'oggetto sociale cosi come la sua proporzionalità e non eccedenza. A tale proposito è stato effettuato un ridimensionamento delle banche dati **NOIPA, PERLAPA, SIDI, SISSI,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

ISTITUTO, per garantire una sempre maggiore libertà dei diritti e sicurezza dei dati agli interessati si sforza continuamente di trovare le migliori mitigazioni a tutti i rischi ai quali i dati in nostro possesso possono andare incontro.

in particolare segnaliamo di aver individuato i seguenti rischi:
Accessi esterni non autorizzati
Allagamento
Alterazione dolosa o colposa dati avvenuta internamente
Attacco Ransomware
Azione di virus informatici o di codici malefici
Carenza di consapevolezza, disattenzione o incuria
Comunicazione illegale dei dati e dei documenti
Copia abusiva
Degrado dei supporti e delle apparecchiature
Cortocircuito elettrico
Distruzione di apparecchiature o di supporti
Fenomeni meteorologici
Furto Apparecchiature

Incendio
Ingressi non autorizzati a locali/aree ad accesso ristretto
Malfunzionamento hardware o software
Mancanza di continuità di alimentazione elettrica
Mancata manutenzione del sistema informativo
Perdita credenziali
Polvere, corrosione o gelo
Possibile rottura dell'hard disk o altri componenti hardware/software
Accessi tramite dispositivi mobili non autorizzati
Errato utilizzo doloso o colposo del software
Mancata distruzione o restituzione dei supporti raggiunta la finalità

Dei sopraelencati rischi, in accordo con i consulenti IT abbiamo posto in essere le seguenti mitigazioni:**Firewall Software**
Antivirus commerciale gruppi
di continuità
Manutenzione spot apparecchiature sistema di
backup in cloud

Tali mitigazioni danno al trattamento **AREA PERSONALE** una compliance alla sicurezza del **69%**

La sua valutazione ci porta ad affermare che per importanza dei dati di questo trattamento e principio di proporzionalità il trattamento stesso ha una valutazione di impatto più che accettabile.
Tuttavia segnaliamo anche che sono stati individuate alcune criticità che possono mettere a rischio i dati anche se in misura minimale. A questo proposito segnaliamo:
Dispositivo USB semplice
Nessuna crittografia

Infine, per sensibilizzare tutti i dipendenti incaricati al trattamento ad una sempre maggiore attenzione alla protezione dei dati abbiamo realizzato e consegnato a ciascuno una privacy policy la cui visione è disponibile nella sezione privacy policy.
Il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR dichiarano di aver ottemperato a quanto richiesto dal GDPR in base al principio di proporzionalità, all'importanza e la quantità dei dati in loro possesso e ai fatturati aziendali

grosseto, li 15/06/2018

Il Data Controller NOMEDATACONTROLLER .....

Il Data Processor NOMEDATAPROCESSOR .....

PROTOCOLLO/SEGRETERIA DIGITALE

assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

ISTITUTO effettua il seguente trattamento: **AREA PROTOCOLLO/ SEGRETERIA DIGITALE** meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L' ISTITUTO, tramite il trattamento "AREA PROTOCOLLO/ SEGRETERIA DIGITALE", tratta i sopraindicati dati per:
Gestione della corrispondenza in ingresso e uscita da posta Elettronica (peo), certificata (pec) e da posta cartacea, con smistamento presso gli uffici dell'Istituto

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

Dopo attenta valutazione di comune accordo con il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR; L'ISTITUTO considera questo trattamento essenziale e indispensabile per il corretto perseguimento dell'oggetto sociale cosi come la sua proporzionalità e non eccedenza. A tale proposito è stato effettuato un ridimensionamento delle banche dati **SPAGGIARI,**
cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

L'ISTITUTO, per garantire una sempre maggiore libertà dei diritti e sicurezza dei dati agli interessati si sforza continuamente di trovare le migliori mitigazioni a tutti i rischi ai quali i dati in nostro possesso possono andare incontro.

in particolare segnaliamo di aver individuato i seguenti rischi:
Accessi esterni non autorizzati
Allagamento
Alterazione dolosa o colposa dati avvenuta internamente
Attacco Ransomware
Azione di virus informatici o di codici malefici
Carenza di consapevolezza, disattenzione o incuria
Comunicazione illegale dei dati e dei documenti
Copia abusiva
Degrado dei supporti e delle apparecchiature

Cortocircuito elettrico
Distruzione di apparecchiature o di supporti
Fenomeni meteorologici
Furto Apparecchiature
Incendio
Ingressi non autorizzati a locali/aree ad accesso ristretto
Malfunzionamento hardware o software
Mancanza di continuità di alimentazione elettrica
Mancata manutenzione del sistema informativo
Perdita credenziali
Polvere, corrosione o gelo
Possibile rottura dell'hard disk o altri componenti hardware/software
Accessi tramite dispositivi mobili non autorizzati
Errato utilizzo doloso o colposo del software
Mancata distruzione o restituzione dei supporti raggiunta la finalità

Dei sopraelencati rischi, in accordo con i consulenti IT abbiamo posto in essere le seguenti mitigazioni:**Firewall Software**
Antivirus commerciale gruppi
di continuità
Manutenzione spot apparecchiature sistema di
backup in cloud

Tali mitigazioni danno al trattamento **AREA PROTOCOLLO/ SEGRETERIA DIGITALE** una compliance alla sicurezza del **53%**

La sua valutazione ci porta ad affermare che per importanza dei dati di questo trattamento e principio di proporzionalità il trattamento stesso ha una valutazione di impatto più che accettabile.
Tuttavia segnaliamo anche che sono stati individuate alcune criticità che possono mettere a rischio i dati anche se in misura minimale. A questo proposito segnaliamo:
Dispositivo USB semplice
Nessuna crittografia

Infine, per sensibilizzare tutti i dipendenti incaricati al trattamento ad una sempre maggiore attenzione alla protezione dei dati abbiamo realizzato e consegnato a ciascuno una privacy policy la cui visione è disponibile nella sezione privacy policy.
Il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR dichiarano di aver ottemperato a quanto richiesto dal GDPR in base al principio di proporzionalità, all'importanza e la quantità dei dati in loro possesso e ai fatturati aziendali

Grosseto, li 18/06/2018

Il Data Controller NOMEDATACONTROLLER .....

Il Data Processor NOMEDATAPROCESSOR .....

PRIVACY IMPACT ASSESSMENT TRATTAMENTO **AREA RETRIBUZIONI**

L'ISTITUTO con sede in P.ZZA D. ALIGHIERI,19, nell'ottica di assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

l'ISTITUTO effettua il seguente trattamento: **AREA RETRIBUZIONI**
meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L' ISTITUTO, tramite il trattamento "AREA RETRIBUZIONI", tratta i sopraindicati dati per: **LA GESTIONE DEI COMPENSI ACCESSORI SPETTANTI AL PERSONALE DIPENDENTE NELL'AMBITO DELLE ATTIVITA' PREVISTE DAL PTOF, COMPETENZE MENSILI AL PERSONALE SUPPLENTE, VERSAMENTO RITENUTE PREVIDENZIALI E FISCALI AGLI ENTI INTERESSATI, DICHIARAZIONI CONTRIBUTIVE E FISCALI CORRELATE.**.

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

Obblighi di legge cui è soggetto l'Istituto; dati raccolti e trattati per legge

Dopo attenta valutazione di comune accordo con il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR; L'ISTITUTO considera questo trattamento essenziale e indispensabile per il corretto perseguimento dell'oggetto sociale cosi come la sua proporzionalità e non eccedenza. A tale proposito è stato effettuato un ridimensionamento delle banche dati **NOIPA, SIDI, SISSI,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

L'ISTITUTO, per garantire una sempre maggiore libertà dei diritti e sicurezza dei dati agli interessati si sforza continuamente di trovare le migliori mitigazioni a tutti i rischi ai quali i dati in nostro possesso possono andare incontro.

in particolare segnaliamo di aver individuato i seguenti rischi:
Accessi esterni non autorizzati
Allagamento
Alterazione dolosa o colposa dati avvenuta internamente
Attacco Ransomware
Azione di virus informatici o di codici malefici
Carenza di consapevolezza, disattenzione o incuria
Comunicazione illegale dei dati e dei documenti
Copia abusiva
Degrado dei supporti e delle apparecchiature
Cortocircuito elettrico
Distruzione di apparecchiature o di supporti

Fenomeni meteorologici
Furto Apparecchiature
Incendio
Ingressi non autorizzati a locali/aree ad accesso ristretto
Malfunzionamento hardware o software
Mancanza di continuità di alimentazione elettrica
Mancata manutenzione del sistema informativo
Perdita credenziali
Polvere, corrosione o gelo
Possibile rottura dell'hard disk o altri componenti hardware/software
Accessi tramite dispositivi mobili non autorizzati
Errato utilizzo doloso o colposo del software
Mancata distruzione o restituzione dei supporti raggiunta la finalità

Dei sopraelencati rischi, in accordo con i consulenti IT abbiamo posto in essere le seguenti mitigazioni:**Firewall Software**
Antivirus commerciale
Manutenzione spot apparecchiature
sistema di backup in cloud

Tali mitigazioni danno al trattamento **AREA RETRIBUZIONI** una compliance alla sicurezza del **68%**

La sua valutazione ci porta ad affermare che per importanza dei dati di questo trattamento e principio di proporzionalità il trattamento stesso ha una valutazione di impatto più che accettabile.
Tuttavia segnaliamo anche che sono stati individuate alcune criticità che possono mettere a rischio i dati anche se in misura minimale. A questo proposito segnaliamo:
Dispositivo USB semplice
Nessuna crittografia

Infine, per sensibilizzare tutti i dipendenti incaricati al trattamento ad una sempre maggiore attenzione alla protezione dei dati abbiamo realizzato e consegnato a ciascuno una privacy policy la cui visione è disponibile nella sezione privacy policy.
Il Data Controller NOMEDATACONTROLLERe il Data Processor NOMEDATAPROCESSOR dichiarano di aver ottemperato a quanto richiesto dal GDPR in base al principio di proporzionalità, all'importanza e la quantità dei dati in loro possesso e ai fatturati aziendali

PIA

PIA di dettaglio

Contesto

Panoramica

Si valuta il Trattamento dati in formato sia elettronico che cartaceo con particolare riguardo alle informazioni personali in questi contenuti

Si analizza altresì le pratiche trattate da i vari organi dell'azienda : contabilità,clienti, fornitori,dipendenti,Visitatori che a vario titolo possono venire a contatto con l'azienda il suo personale attraverso il sito web con particolare riguardo al rispetto delle norme del RE 676/2016

Responsabilità legate al trattamento

E' responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.
Per questo mette in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il regolamento emanato RE 676/1 6, compresa l'efficacia delle misure. Tali misure devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche,

Ci sono standard applicabili al trattamento?

Fermo restando che dati raccolti in modo diverso possono avere trattamenti diversi sia nella manipolazione che nell'utilizzo. Il titolare del trattamento definisce degli standard di default da applicare comunque a tutti i dati e si adopera perchè gli attori di tali trattamenti siano opportunamente formati. Tra gli standard si ricorda .

- protezione dei dati fin dalla progettazione
- riduzione al minimo il trattamento dei dati personali
- pseudonimizzare i dati personali il più presto possibile

- Protezione dei supporticartacei in luoghi a controllata accessibilità

consentire all'interessato di controllare il trattamento dei propri dati nel tempo per poter richiedere l'eventuale aggiornamento

Dati, processi e risorse di supporto

Dati trattati

I dati trattati che possono interessare i dettami definite nel regolamento privacy sono sostanzialmente di 4 tipi

1. Dati personali relativi ai clienti di utilizzati dalla contabillità per quanto riguarda fatturazione
    1. questi dati possono finire anche nei sistemi automatici di produzione ma è stato raccomandato ai produttori di software di utilizzare solo la ragione sociale in quasto in questo contesto altri dati sono superflui
    2. sul punto precedente sarà oggetto di verifica annuale
2. Dati personali relativi ai fornitori utilizzati esclusivamente dalla contabillità per quanto riguarda fatturazione passiva
3. Dati personali dei dipendenti Utilizzati esclusivamente dagli uffici amministrativi per quanto riguarda le retribuzioni gli adempimenti fiscali, e la gestione del personale

1. Su questo viene fatto corso di formazione al personale amministrativo su accorgimenti e precauzioni sia per quel che riguarda i dati conservati in via informatica che su quelli conservati in maniera cartacea.

2. Particolare attenzione viene posta su quei dati che anche indirettamente possono portare a considerazione sulla razza,orientamenti religiosi e politici (ad esempio lì'iscrizione ad un sindacato la nazionalità la foto per il Badge delle presenze In nessun caso sono mantenuti dati che possono condurre ad orientamenti religiosi,politici,di razza

4. Dati/immagini ripresi durante lo svolgimento del lavoro

    1. Queste immagini che documentano il lavoro svolto in azienda possono venir diffusi tramite sito web per pubblicitò dell'azienda stessa in tal senso i dipendenti sono informati e acconsentono alla diffusione fatto salvo il loro diritto a venire cancellati su richiesta e fatto salvo che mai saranno ripresi in atteggiamenti negativi e/o dannosi per la loro dignità personale

5. Dati immagini ripresi da telecamere esterne per motivi di sicurezza

6. Ciclo di vita del trattamento dei dati

7. Per i dati di cui al punto 1 2 3 il ciclo di vita dura quanto il rapporto con il cliente/fornitore/dipendente e l'azienda l'aggiornamento puo avvenire quotidianamente e in maniera imprevedibile (un dipendente può cambiare casa un fornitore puà modificare la ragione sociale così un cliente i dati sono comunque tenuti nel Sistema informativo aziendale Quali sono le risorse di supporto ai dati?

8. Per quel che riguarda tutti i dati amministrativi questi sono tenuti nel server Locale gestito con software e assistenza remota dalla ditta Teamsystem.

9. Per quel che riguarda i ppc che gestiscono i processi lavorativi ci si è affidati ad una ditta di grosseto ai quali è stato raccomandato e passato l'utilizzo dei soli dati di ragione sociale del cliente e nel caso di utilizzo di dati del dipendente che valida il lavoro solo la matricola / nominativo.

Principi Fondamentali

Proporzionalità, necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi

I Dati personali trattati al fine di poter svolgere la missione dell'azienda e si raccolgono esclusivamente a tale scopo o in caso diverso sotto ordine dell'autorità Pubblica (può verificarsi il caso di richiesta di dati vaccinali e/o siituazioni famiiare a fini statistici,)
Tali dati solo se richiesti da leggi saranno raccolti restituiti in forma di legge all'avente
titolo Valutazione : Da correggere

Quali sono le basi legali che rendono il trattamento legittimo

Occorre innanzitutto distinguere 2 casi

- dati vengono comunicati in forma automatica da altre entità che le hanno raccolte o INPS o ASL o Altre
- Dati che vengono acquisiti direttamente dagli interessati per presentazione dirtetta o Iscrizioni all'albo fornitori

Per i primi si Verifica che il fornitore dichiari di aver acquisito il consenso o che ci siano i presupposti di legge che consentano tale interscambio prima di accettarli.

- Naturalmente questo viene fatto una sola volta per tipologia (es se posso accettare i certificati medici dall'inps per un dipendente è chiaro che la procedura varrà anche per tutti gli altri)

Per i secondi Al primo contatto si acquisisce con firma il modello di consenso informato al trattamento dei dati e alla sua eventuale diffusione di parti specifiche nelle piattaforme Istituzionali

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati (minimizzazione dei dati)

I dati raccolti sono quelli minimi indispensabili per il funzionamento dell'Azienda

Ove possibile non vengono richiesti dati di cui l'azienda è già in possesso (es la profilazione riporta con se tutti i dati anagrafici di uno dipendente quindi una richiesta avviene sulla base del profilo e non scrivendo in chiaro su modelli i propri dati personali . Ciò limita la circolazione anche cartacea dei dati tra gli uffici)
Valutazione : Accettabile

I dati sono accurati e mantenuti aggiornati

La cura sulla qualità dei dati e mantenuta con costanza e meticolosità e questo deve essere attuato tramite due azioni principali

1. Ove possibile deve essere sempre offerta Il'interessato la possibilità di vedere i propri dati trattati al fine di poter richiedere eventuali correzioni se non poterle effettuare esso stesso.

2. Dall'incrocio delle banche dati trattati dall'azienda possono venire fuori disallineamenti che portano all'aggiornamento tempestivo dei dati nelle Basi Opportune /(es una difformità di residenza tra azienda asl e inps).

Valutazione : Accettabile

Durata della conservazione dei dati

Alcuni dati sono mantenuti in maniera perenne e in ogni caso quanti più possibili vengono digitalizzati e

- Restituiti su supporto digitale all'Azienda per una archiviazione storica in armadi protetti
- Tenuti in Databases o archiviazione remote all'ente sì da minimizzare l'effrazione
- Per i dati trasferiti su supporti digitali e conservati nell'Istituzione Scolastica è prevista una procedura di refresh globale.
- I dati salvati nei supporti nell'anno n contengono anche i dati degli anni <= n-l o I dati vengono tenuti in supporti separati leggibili nell'anno n questo per evitare ad esempio che la tecnologia li renda praticamente illeggibili (si pensi ai dati memorizzati sui nastri magnetici e tra poco stessa sorte subiranno i DVD rom)

ove non è possibile la digitalizzazione i dati sono mantenuti in apposite cartelle sistemate in armadi chiusi e non accessibili ai dipendenti se non autorizzati

Controlli per proteggere i diritti personali dei soggetti interessati

Come si ottiene il consenso dei soggetti interessati

Intanto si è previsto una serie di profili ad autorizzazioni associate che ogni attore dell'Azienda detiene .

In caso di non compilazione i I sistema blocca l'accesso ai dati utilizzando una politica restrittiva di tipo Dos (Deny of service)

Ove non possibile acquisizione elettronica si prevedono modelli specifici.

I soggetti interessati come esercitano i loro diritti di acceso alla portabilità dei dati?

I dipendenti hanno sempre la possibilità attraverso i loro profili di vedere i dati loro relativi se sono gestiti in formato elettronico qualora abbiano invece la necessità di accedere a degli atti tenuti in modo cartaceo devono comunque richiedere attraverso un documento preposto all'accesso ai dati in cui si impegnano alla non diffusione delle informazione che vedranno(sempre che abbiano diritto alla visura)
Per gli altri soggetti è prevista una richiesta attraverso un documento preposto all'accesso ai dati in cui si impegnano alla non diffusione delle informazione che vedranno(sempre che abbiano diritto alla visura)
Valutazione : Accettabile

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

con una mail di richiesta alla pec aziendale indirizzata al responsabile del trattamento dati per chiedere la cancellazione di parti del sito che lo riguardano purchè queste non ledano il diritto di altri che vogliano invece visualizzarle(un esempio Cancellare una foto di un gruppo di lavoro delle foto che altri vogliano vedere) in questo caso si può ottenere al massimo l'oscuramento del viso)
La richiesta verrà comunque tracciata e archiviata digitalmente.

i soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

con una mail di richiesta alla pec aziendale indirizzata al responsabile del trattamento
dati Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

I responsabili del trattamento dei dati ricevono e sottoscrivono una informativa ad hoc dove sono dettagliati i trattamenti dei dati loro assegnati.

Tale informativa è sottoposta a revisione annuale per accertarsi che nuove procedure non siano state introdotte e eventualmente le informative vengono mpodificate e nuovamente sottoscritte
Valutazione : Accettabile

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

Non sono previsti invio dati fuori dell'Unione europea

Rischi

Controlli esistenti o pianificati

Tracciabilità

Gli accessi ai dati sono di norma registrati in un db di journal che registra il profilo e la geolocalizzazione e le date dell'accesso nonche la pagina o l'azione web richiesta

La teamsystem proprietaria del software dovrebbe rilasciare un journal archiviabile di transazioni (In fase di attuazione) Per gli accessi wifi al sistema esiste una pwd WPA che è memorizzata sui singoli PC portatili e dispositivi mobili personali della direzione e solo una persona detiene questa password e comunque conservata in cassaforte in busta chiusa.

Lotta contro il malware

Sul server centrale esiste a sua volte un firewall e antivirus gestito dalla ditta TEAMSYSTEM Gestione

postazioniSu ogni pc esistono 2 profili uno di amministratore l'altro utente con minore autorità.

Su ogni pc è installato lo screensaver che entra in funzione dopo 5 minuti di inattività e richiede la password utente per riaccedere al sistema e entrare ad operare.
Tutti gli utenti non detengono la password di amministratore
Per maggiori dettagli sulle misure di sicurezza siveda il documento presentato il 31 / 1 2/2017 dell' AGID preparato dall'Azienda.

Sicurezza dei siti web

I dati sul web sono solo pagine di presentazione aziendale e quindi statici e a rara variazione.
L'accesso al sito è libero e non contiene pagine per l'acquisizione dati in
forma remota. E' comunque previsto un salvataggio di sistema periodico.

Backup

Il server locale che gestisce i dati effettua un backup incrementale gestito dalla teamsystem 2 volte al giorno. Il server è provvisto di un sistema di archiviazione raid mirroring quindi a fronte di una rottura di un hd i dati sono immediatamente disponibili sul disco mirror.
Ciononostante é stata comunque raccomandata una misura di backup ulteriore dei dati su 7 supporti esterni (Hd da 2 TB) uno per ogni giorno della settimana da montare la mattina e tenere in sede separata dal server per prevenire crash più drammatici di un guasto Hd (quali incendi o totale distruzione a fronte di ransomware dell'intero patrimonio di dati) Gestione dei terzi che accedono ai dati
Esistono persone che possono accedere ai dati aziendali e personali registrati in azienda tipicamente

- I fornitori di software (teamsystem)
- I consulenti che sovrintendono ai dati di comunicazione tra il server e i programmi di processo delle attività industriali

Per questi viene fatta firmare una dichiarazione di responsabilità alla non divulgazione dei dati cui venissero in possesso Controllo degli accessi fisici
I locali che contengono i dati sono tutti chiusi a chiave in caso di mancata presenza dell'operatore responsabile gli uffici sono protetti da allarme anti intrusione e la notte la zona oltre ad essere monitorata dall'esterno con telecamere e sistema di allarme è controllata da un guardiano che dorme in loco.
I visitatori se ammessi vengono sempre accompagnati da una persona dell'azienda
Se un cliente o fornitore non può essere ricevuto viene fatto accomodare in una zona di attesa in vista a 2 uffici amministrativi

Gestione del personale

A tutto il personale viene erogato all'assunzione un corso sulla privaci di 8 ore e nell'informativa si autocertifica di averlo fatto prima di iniziare il rapporto di lavoro.
Viene altresi dichiarato che i dati in possesso dell'azienda saranno mantenuti ai soli fini istituzionali anche al termine del rapporto di lavoro a disposizione dei soli organi di controllo e che non saranno comunque diffusi all'esterno se non previa autorizzazione dell'interessato.

Archiviazione

Le politiche di archiviazione dei dati sono dettagliate nella sezione Backup
Per ogni computerdegli amministrativi è conservata una copia del desktop sul server cosi da non perdere anche i dati memorizzati sulle postazioni locali

Sicurezza dei documenti cartacei

I documenti non digitalizzati contenenti dati personali sono comunque contenuti in cartelle conservate in armadi chiusi e non visibili al pubblico che non può neppure accedere allo spazio uffici (vedi sicurezza degli accessi) Manutenzione
Nel caso di un guasto ad una apparecchiatura che dovesse essere portato in riparazione fuori dall'azienda si prevede di

- Firmare l'hard disk con pennarello indelebile prima di consegnare l'oggetto guasto alla ditta deputata alla riparazione ▪ Rimuovere l'Hard disk contenente i dati se il guasto non è sull'HD
- Richiedere al fornitore impegno (con apposito modello)a non leggere i dati contenuti nell'HD qualora non sia rimovibile.
- Richiedere la restituzione dell'hd vecchio e firmato in caso di sostituzione del medesimo a fronte di guasto

- I fornitori di software
- I consulenti che sovrintendono ai dati di comunicazione tra il server e i programmi di processo delle attività industriali

Per questi viene fatta firmare una dichiarazione di responsabilità alla non divulgazione dei dati cui venissero in possesso Controllo degli accessi fisici
I locali che contengono i dati sono tutti chiusi a chiave in caso di mancata presenza dell'operatore responsabile gli uffici sono protetti da allarme anti intrusione e la notte la zona oltre ad essere monitorata dall'esterno con telecamere e sistema di allarme è controllata da un guardiano che dorme in loco.
I visitatori se ammessi vengono sempre accompagnati da una persona dell'azienda
Se un cliente o fornitore non può essere ricevuto viene fatto accomodare in una zona di attesa in vista a 2 uffici amministrativi

Gestione del personale

A tutto il personale viene erogato all'assunzione un corso sulla privaci di 8 ore e nell'informativa si autocertifica di averlo fatto prima di iniziare il rapporto di lavoro.
Viene altresi dichiarato che i dati in possesso dell'azienda saranno mantenuti ai soli fini istituzionali anche al termine del rapporto di lavoro a disposizione dei soli organi di controllo e che non saranno comunque diffusi all'esterno se non previa autorizzazione dell'interessato.

Archiviazione

Le politiche di archiviazione dei dati sono dettagliate nella sezione Backup
Per ogni computerdegli amministrativi è conservata una copia del desktop sul server cosi da non perdere anche i dati memorizzati sulle postazioni locali

Sicurezza dei documenti cartacei

I documenti non digitalizzati contenenti dati personali sono comunque contenuti in cartelle conservate in armadi chiusi e non visibili al pubblico che non può neppure accedere allo spazio uffici (vedi sicurezza degli accessi) Manutenzione
Nel caso di un guasto ad una apparecchiatura che dovesse essere portato in riparazione fuori dall'azienda si prevede di

- Firmare l'hard disk con pennarello indelebile prima di consegnare l'oggetto guasto alla ditta deputata alla riparazione ▪ Rimuovere l'Hard disk contenente i dati se il guasto non è sull'HD
- Richiedere al fornitore impegno (con apposito modello)a non leggere i dati contenuti nell'HD qualora non sia rimovibile.
- Richiedere la restituzione dell'hd vecchio e firmato in caso di sostituzione del medesimo a fronte di guasto

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

E' istituito un registro di data Breech dove riportare le eventuali effrazioni rilevate e le contromisure adottate da riportare al GDPO durante le visite periodiche o su chiamata a seconda del livello di pericolosityà rilevato.
Vigilanza sulla protezione dei dati
Sono previsti incontri periodici (almeno 1 1'anno) sulla verifica delle procedure di protezione dei dati e sulla attuazione delle misure indicate dal GPDRO

Contratto con il responsabile del trattamento

I dati personali comunicati a o gestiti da responsabili del trattamento Sono regolati da informativa dove si dichiara che:

Si Utilizzano esclusivamente responsabili del trattamento che offrono garanzie sufficienti ln quanto opportunamente formati

- Sono Adottare e documentate misure (audit di sicurezza, visite agli impianti, ecc.) che consentano di assicurare l'effettività delle garanzie offerte dal responsabile del trattamento in materia di protezione dei dati.
- Esistenza di procedure tali da garantire che i responsabili del trattamento non accedano ad altri dati diversi dai dati affidatigli
- - garanzie in materia di protezione della rete, tracciabilità (log, audit), gestione delle autorizzazioni, autenticazione,

ecc.

- Sono previste disposizioni relative a quanto segue:
- - gli obblighi dei responsabili in materia di riservatezza dei dati personali affidati
  - - requisiti minimi di autenticazione degli utenti o - clausole in materia di restituzione e/o distruzione dei dati allo scadere del contratto
- regole per la gestione e la notifica di eventuali incidenti. Queste ultime dovrebbero prevedere la comunicazione al titolare del trattamento qualora sia individuata una violazione di sicurezza o si verifichi un incidente di sicurezza, da effettuarsi con la massima celerità possibile qualora la violazione riguardi dati personali.

Riesaminare periodicamente la politica di sicurezza
interna , Monitorare gli sviluppi nel tempo.

Protezione contro fonti di rischio non umane

I dati grazie al backup esterni non tenuti nei locali aziendali sono al sicuro almeno quelli fino al giorno precedente qualsiasi evento possa accadere in azienda (incendio sabotaggi,furti del server e dei pc) Ciononostante l'azienda è dotata di allarmi anti effrazione e di anti incendio

Contratti di trattamento

Monitoraggio dell'attività della rete

Controllo degli accessi

Le postazioni sono tutte accedibili solo tramite autenticazione e per nquanto riguarda gli uffici che trattano dati personali viene fornita agli operatori una password forte di almeno 8 caratteri alfanumerici con almeno

un carattere speciale L'azienda utilizza un metodo di rotazione delle password che vengono cambiate ogni 1 80 giorni.
Le password sono conservate in cassaforte in formato anche cartaceeo lo stesso viene fatto per quanto riguarda i codici di attivazione dell'allarme e del sistema di videosorveglianza Vulnerabilità
Per quanto riguarda l'accesso ai dati cartacei questo viene minimizzato grazie all'utilizzo di documentazione scansionata presente nel server.
Benchè tutta la documentazione cartacea viene tenuta in armadi a chiave.

Accesso illegittimo ai dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare?

Discriminazione sociale nel caso di dati relativi ai dipendenti, Passaggio di dati relativi ai clienti ad altri concorrenti dell'azienda, Falsare una gara fornendo informazioni ad un partecipante per agevolarlo Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso ai dati non autorizzato, Accesso ai dati da parte del subfornitore software
Quali sono le fonti di rischio?
Mancata custodia delle password di accesso al sistema, Lasciare incustoditi i locali, Pratiche in vista sulla scrivania

Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati

Limitata

Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati

Limitata

Modifiche indesiderate dei dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare?

Diffusione di dati inesatti

Quali sono le principali minacce che possono portare al rischio?

Errate operazione da parte dei dipendenti Quali sono le fonti di rischio?
Sistemi software di contabilità e produzione

Quali dei controlli identificati contribuiscono a gestire il rischio?

undefined

Come stimeresti la gravità del rischio, in particolare riguardo l'impatto potenziale e i controlli pianificati?

Trascurabile

Come stimeresti la probabilità del rischio, specialmente riguardo minacce, fonti di rischio e controlli pianificati?

Trascurabile

Scomparsa di dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio dovesse realizzarsi?
Posto che i dati non possono essere persi in toto data la politica dei salvataggi l'unica sscomparsa possibile e la cancellazione di una dato per errore
Quali sono le minacce che potrebbero portare al rischio?
errore da parte dell'operatore
Quali sono le fonti di rischio?
Accidentale o voluta operazione da parte di un addetto
Quali dei controlli identificati contribuisce a gestire il rischio?

Grosseto li 18/06/2018

Generalità e obiettivi

Il DPI

Il documento di protezione AGID

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

ABSC_ID			Livello	Descrizione	Moda
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Su cloud, tramite applica che netware
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Programma ad hoc
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Zeroshell
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Zeroshell

1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Archiviazione periodica t
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Zeroshell
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Previsto in zerotruth
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Sì
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.	Sì, registriamo IP e indir non sei sotto DHCP altrin
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.	Sì, implementato dal sW
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.	Sì, quelli dei docenti e d autenticazione; gli altri r rete
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.	Sì
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Sì

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.	Nessun utente può installare softv nei pc della scuola non avendo i privilegi di admin che è l'unico che installa software sui pc tablet ecc tiene aggiornato l'elenco descritto punto 1.1.1
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	Non necessario perché solo admin installa il software e aggiorna l'ele di cui al punto 2.2.1
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).	Sì, v. punto 2.1.1
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Log sui sistemi per tentativi di accesso admin non autorizzati

2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Analisi registro hkey local machine periodico sulle macchine
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.	Sì, 1.1.1
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.	Sì, vedi 2.3.2
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.	No, macchine virtuali

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.	Sì, configurazioni minimali atte a garantire il funzionamento
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.	Sì, con antivirus e firewall attivate da admin su ogni macchina
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.	Per ogni tipologia di macchina backup della configurazione iniziale del sistema operativo e del software applicativo in dotazione.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Sì, vedi 3.1.3 per i server non esistono workstation
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Sì
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Sì
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Sì; una per ogni tipologia di macchine (es. per un laboratorio con 20 pc

					identici basta una sola immagine)
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	In cassaforte ignifuga in sede
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).	Sì, attraverso team viewer installato come dotazione di base in tutte le macchine con protocollo https
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.	Controllo tramite Antivirus
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.	Sì
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.	Solo admin può eseguire tali modifiche
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Sì
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Monitoring periodico trimestrale via team viewer
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Esistenza del punto di ripristino su ogni macchina ma direzione di migrazione dati utente su cloud quindi il ripristino avviene solo per il software di base e applicativo.

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.	Sì, tramite Antivirus
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Sì, tramite Antivirus
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.	Sì; da zeroshell e zerotruth
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Sì; da zeroshell e zerotruth
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Sì; da zeroshell e zerotruth
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.	Antivirus con aggiornamento all'avvio del pc
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.	Sì: da zeroshell e zerotruth
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Sì: da zeroshell e zerotruth
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	Antivirus con aggiornamento all'avvio del pc
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Tutte le macchine con windows 10 lo fanno automaticamente
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.	Sì: poche unita < 5 comunque dotate di AV
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.	Sì
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.	Sì
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.	Sì
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.).	Sì, ad es viene proibito (con disabilitazione dei device usb)l'uso delle penne di memoria privilegiando l'utilizzo del cloud sia per docenti che per studenti e ata

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.	Sì
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.	Sì: backup immediato dei dati su supporti esterni
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.	Sì: Dall'animatore digitale e team

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.	**Sì: su ogni pc esistono 2 profili con privilegi diversi (Group policy)**
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Sì
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Un solo utente amministratore
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Sì: log di sistema analizzato periodicamente
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Sì
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Sì; ma ce ne è una sola
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.	Sì
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Sì
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Nessuno può aggiungere utenze amministrative
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Sì
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Sì
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.	No, ma è allo studio un sistema biometrico poiché ogni pc è dotato di web cam si prevede lo studio del

					riconoscimento facciale e, per i pc più vecchi senza webcam, un dispositivo di riconoscimento tramite impronta digitale.
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).	Alla data la lunghezza minima è di 8 car ma si raccomanda 14
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Sì, l'amministratore usa password robuste
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	180 giorni per ogni password max
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Sì, history 3 password
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	No
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Sì
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.	Sì
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.	No
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Sì
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Sì
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.	Sì
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).	Sì
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Sì, in Cassaforte dal DSGA
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Sì

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.	Sì
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Sì
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Sì
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.	Sì
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.	Sì, via Team viewer
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	No
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Sì
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Sì, attraverso log che registra ip diversi da quelli statici dedicati alla scuola
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.	Si
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Sì
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.	Si
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Rimozione al primo suspicious
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Vedi 8.5.2
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Sì, disabilitate usb e dvd
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Sì per office e PDF
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Client di posta non installati sui pc le mail vengono filtrate ed inserite in un Data base per successive consultazioni
8	7	4	M	Disattivare 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.	Non si accettano supporti rimovibili
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.	Sì, installati nel mail server
8	9	2	M	Filtrare il contenuto del traffico web.	Sì, white e black list sul server firewall e proxy
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).	Sì
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Sì, antivirus sul server mail
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.	Sì

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.	Copie quotidiane automatiche su dispositivi diversi ogni giorno a riciclo settimanale
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.	Sì
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Vedi 10.1.1
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Sì, trimestralmente
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.	Le copie sono riposte ogni mattina in cassaforte dal dsga I dati su cloud sono in una webfarm remota alla scuola il backup e quotidiano e settimanale in periodi prefissati vengono off line e criptati
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.	Sono off line

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	Sì, l'accesso avviene se su cloud tramite protocollo Https
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Sì
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.	Sì, tramite Zeroshell
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.	No, perché i dati sensibili stanno criptati sul cloud
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.	Sì, disabilitate tutte le apparecchiature locali di supporti rimovibili
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.	Sì, accesso granted via mac login e password
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.	Sì, attraverso controller Huaweii
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Sì, Zerotruth
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Sì, Zerotruth
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Sì, Zerotruth
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.	Sì, Windows 10 lo fa nativo

Il registro delle attività

In questa sezione sono descritte come dai dettami Cad le attività previste che riguardano i dati personali trattati

Resta ovvio che tale registro è soggetto a variazione continua all'insorgere di nuovi trattamenti sia per motivi di legge che per necessita dell'istituto

Il formato scelto è una tabella excel che viene allegata e fa parte integrante del documento

Per visualizzarlo e/o modificarlo cliccare qui

Le azioni concordate

- Formazione ai dipendenti
  - Viene a tutti somministrato corso di 8 ore su piattaforma web
- Interventi software sulle macchine e sul sistema informativo informatico
  - Adeguamento agli standard Agid
  - Creazione di backup programmato periodico su hd usb esterno da conservare in luogo remoto ai dati
  - Trasportare su Cloud quanto più è possibile di attività di officedei vari PC
- Cartelli di avviso
  - Cartelli presso le aree esterne per videosorveglianza
  - Cartelli interni a ricordo per il personale interno
- Visite periodiche programmate
  - Annuale Concordato con la Dirigenzaper controllo aderenza eriepetto di quanto programmato
  - Revisione annuale del documento a fronte di cambiamenti sia normativi che organizzativi

I modelli per le informative

Sono forniti in allegato i seguenti modelli:

- Informativa ai dipendenti
- Informativa per i fornitori
- Informativa ai clienti

I modelli per l'acquisizione dei consensi

Sono forniti in allegato i seguenti modelli che saranno consegnati in doppia copia fatti firmare e archiviati:

- Acquisizione consenso dipendenti
- Acquisizione consenso per i fornitori
- Acquisizione consenso per clienti

I modelli per i gestori dati esterni

In allegato il modello da ricevere firmato dai gestori dati del sistema informativo

- Acquisizione consenso gestori esterni
-

Facsimile Dei Cartelli

Allegati

Metadati

Questi i campi da sostituire in tutto il documento

NOMEDATAPROCESSOR=nome di colui che controlla il processo dei dati

NOMEDATACONTROLLER=nome di colui che controlla l'immissione dei dati

http://www.forte.tum.de/kontakt/	MONACO GERMANIA
https://muenchen.phorms.de/en/secondary/secondary-school/experiences-with-phorms/	MONACO GERMANIA
https://www.obermenzinger.de/index.php/schulprofil/schulpreise	MONACO GERMANIA
http://www.lyc-artaud.ac-aix-marseille.fr/spip/spip.php?page=agenda	AGENDA MARSIGLIA FRANCIA