SCUOLE ANNESSE EDUCANDATO STATALE SS ANNUNZIATA - AOO - PR. U. N. 0012502 DEL 31/12/2022 - A.18

SCUOLE ANNESSE
Educandato Statale SS. Annunziata
Piazzale del Poggio Imperiale, 1 - 50125 Firenze - Tel. 055 226171 - C.F. 80020090488
e-mail: five010004@istruzione.it – pec: five010004@pec.istruzione.it - sito web: www.ssannunziatascuole.edu.it

SCUOLE ANNESSE ALL'EDUCANDATO SS. ANNUNZIATA

PIANO DI CONTINUITA'

OPERATIVA E DI

DISASTER RECOVERY

PIANO DI CONTINUITA' OPERATIVA

1. FINALITA' E AMBITO DI APPLICAZIONE

Il CAD sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la Digitalizzazione dei servizi. Da tale indicazione consegue, per la Pubblica Amministrazione (nel prosieguo PA), anche l'obbligo di assicurare la continuità dei processi che presiedono alla erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese.

Ne consegue che la continuità dei servizi informatici rappresenta un impegno inderogabile per la PA che deve operare in modo da limitare al massimo gli effetti negativi di possibili fermi prolungati dei servizi ICT. A titolo esemplificativo, la compromissione della continuità di un sistema informatico, può essere conseguenza di:

- errori/malfunzionamenti dei processi (il processo organizzativo che usa il servizio ICT non ha funzionato come avrebbe dovuto per errori materiali, errori nell'applicazione di norme ovvero per il verificarsi di circostanze non adeguatamente previste dalle stesse);
- malfunzionamento dei sistemi, delle applicazioni e delle infrastrutture;
- attacchi o eventi naturali di tipo accidentale;
- disastri.

Il Piano di Continuità Operativa racchiude tutte le informazioni relative alla gestione di eventi straordinari che compromettano l'ordinaria attività lavorativa dell'Ente. Tutti i dipendenti possiedano adeguate competenze e conoscono le procedure per affrontare la condizione di disastro e/o emergenza in modo che possano continuare a fornire i servizi principali, ovvero i servizi classificati con alta priorità di recupero in caso di evento disastroso. Tale documento è finalizzato a illustrare le modalità tecnico/organizzative a cui l'Ente deve attenersi per garantire l'operatività dei propri uffici e servizi, rispettando un predeterminato periodo di tempo, a seguito di disastro o grave evento dannoso.

Nella redazione del Piano di Continuità Operativa l'Ente ha cercato di analizzare e ridurre le cause di rischio e ha opportunamente adeguato il proprio sistema informativo cercando di elevare i livelli di sicurezza informatica, secondo le possibilità e le risorse disponibili.

Il Piano in oggetto racchiude quindi tutte le informazioni legate all'organizzazione logistica dell'Ente, dalla dichiarazione dell'emergenza al rientro alla normalità, alle metodologie per il riconoscimento di una situazione di crisi e poter far fronte alla stessa. Tale Piano include i processi di gestione della crisi e del disaster recovery ovvero le procedure riferite alle modalità di ripristino delle funzionalità dei sistemi informatici per permettere una prosecuzione nell'erogazione dei servizi.

Il Piano di Continuità Operativa rappresenta quindi un processo globale che consente all'Amministrazione di aumentare e migliorare, nel corso dei successivi esercizi, la capacità di risposta all'emergenza degli addetti alla gestione e del sistema informatico. Il PCO, che prevede al suo interno anche una sezione appositamente dedicata del Piano di Disaster Recovery, affronta gli aspetti di definizione dei possibili disastri e degli scenari di rischio, individua i processi critici e le figure coinvolte, interne ed esterne all'Ente, di riferimento in caso di gravi problemi.

La redazione del Piano in oggetto consente all'Ente di assicurare il ripristino della normale attività lavorativa, in caso di processi critici, e quindi di poter affrontare una situazione di emergenza con la consapevolezza di prendere le giuste scelte in caso di crisi, dettate da una preventiva analisi dei servizi e delle condizioni di rischio. Questa analisi permette di stabilire quali siano le procedure alternative da attuare in caso di disastro per garantire l'operatività dell'Amministrazione, riducendo al minimo i tempi di interruzione dei servizi erogati e garantendo, attraverso i test periodici, l'efficacia delle procedure di ripristino.

Per garantire quest'ultima condizione risulta fondamentale un continuo e corretto controllo delle procedure di ripristino con predefiniti test che garantiscano un puntuale aggiornamento del Piano di

Continuità Operativa e del Piano di Disaster Recovery. I servizi erogati sono classificati in base all'impatto che avrebbe una loro interruzione e sono suddivisi in quattro categorie: critici, vitali, delicati, non critici.

Servizi critici: quelli per cui risulta molto bassa la tolleranza in caso di interruzione degli stessi; tali servizi vengono svolti con applicazioni informatiche per cui non è possibile sostituire mezzi e strumenti per erogare il servizio con una metodologia differente ovvero tramite supporti cartacei.

Servizi vitali: quelli erogati con l'ausilio delle applicazioni e delle infrastrutture informatiche, possono essere sostituiti anche con metodi differenti (supporti cartacei) solo per brevi periodi; per questi servizi la tolleranza

dell'interruzione degli stessi, rispetto a quelli critici, risulta superiore.

Servizi delicati: quelli erogati con l'ausilio delle applicazioni e delle infrastrutture informatiche, ma possono essere sostituiti con metodi manuali anche per lunghi periodi di tempo; per questi servizi risulta comunque difficoltosa l'erogazione attraverso procedure manuali.

Servizi non critici: quelli per cui l'erogazione può rimanere interrotta anche per un lungo periodo di tempo.

Prima di stimare una condizione limite o di disastro l'Ente provvede a valutare i servizi erogati e classificarli in modo che, nell'arco temporale in cui viene dichiarata l'emergenza, possa provvedere a fronteggiare i disservizi dati all'utenza e provvedere al ripristino.

Il Piano di Continuità Operativa valuta la criticità dei servizi, dei software di sistema e dei software gestionali utilizzati per fronteggiare l'emergenza e provvedere alla valutazione delle strategie di ripristino: sito alternativo, metodologie per il backup, apparecchiature per il backup, ruoli e responsabilità delle figure coinvolte.

Particolare attenzione viene data all'interno del PCO alla definizione degli scenari di disastro/emergenza in quanto il mancato riconoscimento immediato della gravità di un problema potrebbe portare ad un ritardo irrecuperabile nella dichiarazione di emergenza.

La struttura informatica ha il compito di rilevare il tipo di danno lamentato dal/dagli utenti ed eseguire opportuna diagnosi in merito, elaborata sulla base di elementi quali:

- ampiezza del danno informatico, o del blocco.
- gravità informatica del danno o del blocco
- eventuale possibilità di ripristino o impossibilità nei tempi prescritti

Deve quindi comunicare al responsabile della Continuità Operativa tali valutazioni, in modo tale da permettere a quest'ultimo:

1. La formulazione di richiesta di "restore" di dati e/o procedure

oppure

2. La formalizzazione della dichiarazione di "Disastro", per accedere alle procedure di "Disaster Recovery"

Di fondamentale importanza, quindi, per le figure coinvolte avere un documento che permetta loro di riconoscere le varie situazioni di emergenza che possono presentarsi. Le figure direttamente coinvolte nella Continuità Operativa dovranno sempre essere aggiornate in merito agli scenari di rischio e alle tipologie di problemi che potrebbero verificarsi soprattutto nella gestione del sistema informatico comunale.

Tutto questo lega il Piano di Continuità Operativa alla necessità fondamentale della pubblica amministrazione di custodire copie dei dati trattati e di poter definire tempi certi per il ripristino dei servizi erogati.

Per far fronte a situazioni di disastro e/o emergenza l'Ente si è adoperato per adottare una soluzione tecnologica che consenta di custodire copie dei dati, delle procedure applicative e dei data base in siti alternativi alla sede consortile.

L'indisponibilità prolungata di un servizio, in conseguenza all'indisponibilità dei servizi informatici dell'Ente, in particolari situazioni di disastro, rende necessario garantire un sito secondario di appoggio nel quale trasferire dipendenti e risorse in modo che si possa ripristinare il sistema informatico e garantire una prosecuzione nell'erogazione dei servizi.

L'Ente ha provveduto alla valutazione e alla stima degli elementi di rischio presenti, in modo da organizzare e reagire in caso di emergenza. Verranno di seguito elencati i rischi valutati, ovvero per i quali l'Amministrazione stima il rischio, e definisce politiche e processi all'interno del PCO per affrontarli.
L'ente infatti deve sempre tendere ad un continuo aggiornamento di hardware e software per cercare di ridurre comunque al minimo il livello di rischio e le criticità che potrebbero portare a condizioni di emergenza. Di pari passo dovranno essere adeguate le apparecchiature destinate al disaster recovery e al salvataggio dei dati e dei data base dell'Ente. I servizi critici dell'Ente hanno priorità di ripristino elevata, pertanto in caso di interruzione degli stessi sarà necessario ristabilire procedure applicative, software di sistema, file e documenti.

L'ambito di applicazione del Piano di Continuità Operativa risulta essere costituito da tutti i servizi erogati dall'Ente, per cui si vanno a coprire in un'unica soluzione tecnologica tutte le categorie di servizi e/o classi di servizi.

Tabella servizi:

SERVIZIO	SISTEMA(I) DI	LOCALIZZAZIONE	LDS (orario
Albo pretorio E Amministrazione trasparente	Software Nettuno	Direttamente dislocato presso il sito web	24 ore giornaliere
Atti amministrativi	Software Argo	Programma installato sul server e su Cloud	8 ore giornaliere
Gestione del bilancio	Software Argo	Programma installato su Cloud	24 ore giornaliere
Gestione del personale	Software Argo	Programma installato su Cloud	8 ore giornaliere
Registro Elettronico	Software Nettuno	Programma installato su Cloud	8 ore giornaliere
Protocollo	Software Nettuno	Programma installato su Cloud	8 ore giornaliere
Ufficio Magazzino	Software Nettuno	Programma installato su Cloud	8 ore giornaliere

Sede primaria del servizio: Piazzale del Poggio Imperiale 1 - FIRENZE

Tabella servizi esterni in hosting:

Classe di Servizi	Servizio	Descrizione Servizio	Fornitore
1	Sito Internet	Servizi Web con dati vari compresa trasparenza. Il provider sarà tenuto a provvedere al Disaster Recovery, in quanto I DNS Internet ed altri parametrici tipici vengono da lui gestiti	REGISTER
2	Posta Elettronica	La posta Elettronica utilizzata dai dipendenti viene visualizzata sia tramite Outlook che attraverso un qualsiasi browser Internet, per cui i dipendenti hanno ricevuto opportune istruzioni per il corretto utilizzo sia in condizioni operative normali che "straordinarie".	MICROSOFT

TABELLA ORGANIZZATIVA:

RESPONSABILE ENTE: Dirigente Scolastico

RESPONSABILE AREA AMMINISTRATIVA

1- Respons. Proced. Ammvo contabile

1 - Secondo responsabile del procedimento

9- *esecutori amministrativi*

1.1 Servizi da recuperare con priorità di recupero

L'ambito di applicazione del Piano di Continuità Operativa racchiude tutti i servizi erogati dall'Ente, di prioritario ripristino attraverso l'attuazione del cloud backup.

La soluzione tecnologica scelta da parte dell'Amministrazione risulta essere la medesima per tutti i servizi erogati, indifferentemente dall'indice complessivo di criticità o dalla classe, e risulta di livello tier 2.
La soluzione è quella del cloud backup dove vengono trasferite delle copie di sicurezza dei propri dati in cloud, al fine di garantire la conservazione dei dati vitali a fronte a qualsiasi evenienza disastrosa. Tramite un'unica console di gestione centralizzata è possibile automatizzare la protezione globale e i criteri di conservazione, mentre un accesso sicuro, self service aumenta la disponibilità delle informazioni e diminuisce i tempi necessari all'accesso dei dati.

La soluzione della soluzione di Continuità Operativa adottata dalla scuola è quella del Cloud Argo e Cloud Nettuno

Il suddetto sistema di Backup viene gestito da apposito software in maniera automatica.

Responsabile della Continuità Operativa

Il Responsabile della Continuità Operativa nella scuola è l'assistente amministrativo Carmela Ferrante

1.2 Tempi entro i quali i servizi devono essere recuperati (RTO)

L'RTO, acronimo inglese di Recovery Time Objective, rappresenta il tempo massimo che deve essere necessario per il ripristino dei servizi ovvero tempo massimo entro il quale deve essere ripristinato il sistema informativo con il quale si provvede all'erogazione dei servizi.

Servizio RTO:

Software Amministrativi	4 ore
Registro Elettronico	4 ore
Sito Web e posta elettronica	4 ore
Servizio tecnico	3 giorni

1.3 Livelli di recupero necessario per ogni servizio (RPO)

L'RPO, acronimo inglese di Recovery Point Objective, rappresenta la massima perdita di dati tollerata, risulta quindi essere il dato che descrive la differenza tra il momento in cui il dato viene prodotto e la sua messa in sicurezza attraverso opportune procedure di backup e/o copia sul sito di DR.

Servizio RPO: settimanale

1.4 Condizioni limite che portano all'invocazione del piano

Le condizioni per le quali è necessario ricorrere alla continuità operativa sono:

- Inagibilità della sede primaria, ovvero della sede di produzione dei dati e di erogazione dei servizi in condizioni di normale svolgimento dell'attività istituzionale, individuata nella sede operativa
- Indisponibilità o assenza prolungata della corrente elettrica che superi i tempi massimi di tolleranza di mancanza di erogazione del servizio ovvero i tempi individuati come RTO.
- Assenza prolungata di corrente nel sito primario.
- Indisponibilità o assenza prolungata della rete per il trasferimento dei dati (internet).
- Indisponibilità o assenza prolungata della rete per la telefonia fissa.

Ogni dipendente che riscontri un problema e/o un disservizio che impedisca il normale svolgimento dell'attività lavorativa, sia esso logistico o informatico, deve darne conoscenza al Responsabile della propria Area/Settore.

Il Responsabile dell'Area/Settore interessato valuterà la situazione sottopostagli dal dipendente; nel caso in cui il problema non sia risolvibile con gli ordinari mezzi di intervento ovvero provochi l'interruzione di altri servizi deve darne conoscenza al Responsabile della Continuità Operativa.

Nei casi sopra citati la categoria del disastro potrebbe considerarsi "Grave" o "Disastroso", pertanto rimane a discrezione del Responsabile della Continuità Operativa la valutazione del caso. Ogni Responsabile/Referente di Area o di Settore è tenuto ad utilizzare la "Tabella di classificazione degli incidenti" per determinare il grado di severità dell'incidente ed eventualmente notificare al Responsabile della Continuità operativa o suo delegato l'evento incidentale se ritenuto di categoria "Grave" o "Disastroso", come meglio descritto nella seguente tabella relativa alla classificazione degli incidenti con i livelli di disastro.

Nel seguito viene riportato il Diagramma di Flusso che schematizza le decisioni da prendere in base alla valutazione delle condizioni dello stabile ove c'è la sede operativa, sito di produzione dei dati, e della gravità di perdita dei dati o di perdita dei sistemi informatici, in cui sono residenti i dati, che permettono il normale svolgimento dell'attività lavorativa.

Ogni Responsabile/Referente di Area è tenuto ad utilizzare la seguente tabella per determinare il grado di severità dell'incidente ed eventualmente notificare al Responsabile della Continuità operativa o suo delegato l'evento incidentale se ritenuto di categoria "Grave" o "Disastroso", come meglio descritto nella seguente tabella relativa alla classificazione degli incidenti con i livelli di disastro.

		Interruzione	dei Servizi più	

3	GRAVE	importanti/critici che potrebbero compromettere la continuità operativa dell'Ente o che creano un disservizio che coinvolge un numero elevato di Persone/Servizi. Valutazione dell'incidente in termini di mezzi di intervento in quanto potrebbe non essere risolvibile velocemente e potrebbe essere necessaria l'attivazione di risorse elevate e/o non valutabili	A discrezione del responsabile della Continuità Operativa
4	DISASTROSO	Incidente che causa l'interruzione dei servizi per un periodo superiore a 3 GIORNI	Comitato di Crisi

2. **Ruoli e responsabilità**

In questa sezione vengono elencate le figure facenti parte del Comitato di Gestione Crisi, cui competono le responsabilità nel processo decisionale durante l'emergenza. Tali decisioni saranno successivamente documentate in apposita relazione nel momento in cui sarà conclusa l'emergenza, e controfirmate da tutti i soggetti partecipanti al sopra menzionato Comitato di Gestione Crisi. La relazione dovrà recare tutte le informazioni relative all'attivazione del processo di continuità operativa, alla dichiarazione di rientro dall'emergenza, compito spettante al Comitato di Gestione Crisi, che dovrà riunirsi per valutare l'emergenza e prendere le necessarie decisioni per provvedere al rientro dall'emergenza. Il Comitato di Gestione Crisi della scuola servizi ecologia e ambiente è composto dalle seguenti figure:

NOME E COGNOME	RUOLO	POSTA ELETTRONICA
Prof. Mario Di Carlo	Dirigente Scolastico	dirigentescolastico@ssannuziatascuole.edu.it
Assistente amministrativo Carmina Ferrante	Responsabile della continuità operativa	personale@ssannuziatascuole.edu.it
Dott.ssa Elisabetta Nicolaci	Affidamento incarichi, supporto, organizzazione generale, gestione affidamento incarichi	dsga@ssannunziatascuole.edu.it
Dott. Corrado Faletti	DPO	direttore@controllerprivacy.it

Il **Comitato di Gestione Crisi** è pertanto composto dalle sopra elencate figure che rappresentano i componenti del Comitato di Gestione Crisi dell'ente, ai sensi e per gli effetti dell'articolo 50 – bis del D. Lgs. n. 82/2005 per lo svolgimento delle seguenti attività:

- Definizione, approvazione e aggiornamento del Piano di Continuità Operativa;
- Valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi;
- Avvio delle attività di recupero e controllo del loro svolgimento;
- Rapporti con l'esterno e comunicazioni ai dipendenti;
- Attivazione del processo di rientro che deve essere attuato da specifici gruppi operativi, ma deve essere continuamente monitorato dal Comitato, per assicurare la verifica dello stato di avanzamento complessivo e risolvere i casi dubbi. Infatti, per loro natura, le operazioni di rientro, per quanto dettagliate, possono presentare imprevisti o azioni che coinvolgono altre persone ed hanno impatto su molteplici attività. In tutti questi casi il Comitato deve acquisire tutti gli elementi utili a condurre alla soluzione del problema;
- Avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
- Dichiarazione di rientro;
- Gestione di tutte le situazioni non contemplate;
- Gestione dei rapporti interni e risoluzione dei conflitti di competenza;
- Promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità.

Il **Comitato di Gestione Crisi** è l'organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività delle risorse coinvolte. È l'organo di direzione strategica dell'intera struttura in occasione dell'apertura della crisi e, inoltre, ha la responsabilità di garanzia e controllo sull'intero progetto. Le figure minime necessarie per la costituzione del Comitato di gestione della crisi sono rappresentate da:

- Un ruolo di vertice con poteri decisionali e di indirizzo in materia organizzativa ed economica, ovvero il responsabile ex art. 17 del CAD, coincidente con la figura del Segretario Generale e, in caso di sua assenza, del Responsabile della Continuità Operativa;
- Il Responsabile della "Continuità Operativa" dell'ente;
- Il Responsabile dell'Unità locale di sicurezza prevista dal DPCM 01.04.2008 (Responsabile Area Tecnica);
- I referenti tecnici (anche presso i fornitori di servizi ICT) di volta in volta necessari alla gestione della crisi;
- Il responsabile della logistica (Responsabile continuità operativa);
- Il responsabile della safety dell'ente (datore di lavoro - Dirigente Scolastico);
- Il responsabile delle applicazioni (Responsabile della Continuità Operativa).

In condizioni di **incidente disastroso**, il Comitato assume il controllo di tutte le operazioni e assume le responsabilità sulle decisioni per affrontare l'emergenza, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.

In condizioni di **incidente grave**, il Responsabile del Comitato di Crisi può decidere di lasciare il coordinamento delle operazioni al Responsabile di Area coinvolto, oppure al Comitato di Crisi stesso. Per svolgere i propri compiti, il Comitato attiva le altre figure identificate come risorse dell'Unità Locale di Sicurezza, che fa in modo che il Comitato possa disporre di strumenti e competenze per affrontare ogni sua decisione.

Il Comitato deve essere supportato nelle seguenti aree:

- Area logistica, per garantire supporto negli eventuali spostamenti;
- Area tecnologica, per garantire il funzionamento e l'accesso a tutte le infrastrutture informatiche e di telecomunicazioni predisposte;

- Area informazioni, per aggiornare il Comitato relativamente alle notizie provenienti dai canali pubblici di comunicazione;

- Area comunicazioni di processo, per provvedere alla raccolta di tutta la documentazione dai vari gruppi di lavoro.

Può essere necessario assicurare al Comitato un supporto anche sulle aree:

- Comunicazioni, ad esempio tramite valutazione delle strategie di comunicazione verso cittadini, organizzazioni e dipendenti e dei canali da utilizzare per ciascun tipo di comunicato;
- Finanza, ad esempio con definizione di tutte le iniziative di carattere finanziario necessarie ad assicurare risorse tempestive;
- Risorse umane e rapporti sindacali, ad esempio definizione di comportamenti e formulazione di messaggi specifici volti a rassicurare i dipendenti, sensibilizzare quelli coinvolti nelle operazioni di ripristino, dirimere ogni possibile motivo di disagio che possa ridurre l'efficacia dell'organizzazione;
- Sicurezza informatica, con l'esame di tutti gli aspetti di sicurezza, in particolare per quanto riguarda la verifica del grado di sicurezza offerto dalle configurazioni adottate per l'emergenza e la protezione dei dati, o tramite il riesame delle soluzioni adottate per il ripristino dei sistemi e per il rientro alla normalità;
- Area legale, per eventuali azioni nei confronti del fornitore della soluzione di CO (es. per il mancato rispetto dei tempi di RTO/RPO).

Le date delle riunioni del Comitato saranno decise di volta in volta in relazione alle esigenze. Si precisa inoltre che la validità delle soluzioni e delle azioni presenti nel Piano di Continuità Operativa e nel Piano di Disaster Recovery saranno valutate periodicamente e ne verrà dato atto nei verbali delle riunioni del Comitato di Gestione Crisi.

Il **Responsabile della Continuità Operativa (RCO)**, ha il compito di contattare tutte le figure del Comitato di Gestione Crisi per le riunioni periodiche e provvedere agli aggiornamenti dei piani. Provvede inoltre ad avvisare le figure del Comitato di Gestione Crisi prima della data fissata tramite posta elettronica.

In caso di dichiarazione disastro/emergenza il RCO provvede a contattare tutte le figure facenti parte del Comitato di Gestione Crisi.

In caso di dichiarazione di disastro/emergenza il RCO provvede inoltre a redigere una relazione che illustri le fasi e l'evoluzione dell'emergenza che, una volta rientrata, dovrà essere inviata all'Agenzia per l'Italia Digitale.

3. MODALITA' DI ATTIVAZIONE, GESTIONE E MANUTENZIONE del PCO

La dichiarazione dello stato di crisi e l'attivazione del presente Piano di CO è obbligo del Responsabile della Continuità Operativa, che assicura anche la gestione delle fasi successive di recovery descritte nei capitoli successivi.

Le modalità per cui si deve attivare il piano di continuità operativa e il sistema con cui deve essere attivato sono regolamentate in questa sezione. Nello specifico vengono di seguito elencati i casi limite in cui deve essere attivato il piano in modo che i dipendenti e le figure facenti parte del Comitato di Gestione Crisi sappiano valutare immediatamente il livello del disservizio. Risulta molto importante rendersi conto del livello di disastro in quanto il tempo perso per effettuare un tale tipo di valutazione non è recuperabile. Infatti il lasso di tempo per prendere una decisione in merito al livello di disastro deve essere ricompreso all'interno del tempo di ripristino del servizio.

Fatte queste premesse risulta molto importante la valutazione della gravità dell'evento in modo da attuare subito il piano per arginare l'emergenza.

A tal proposito tutti i dipendenti dell'Amministrazione, le figure del Comitato di Gestione Crisi, gli Amministratori, gli amministratori del sistema informatico e i fornitori con cui l'Ente ha stipulato contratti di assistenza hardware e software, devono avere copia del PCO e del PDR.

Il piano include:

- **Modalità di mobilitazione delle persone interessate;**
- **Punti di ritrovo;**

- **Circostanze in cui l'organizzazione ritiene che l'attivazione del PCO non sia necessaria;**
- **Modalità di gestione, manutenzione, verifica e test del PCO;**
- **Piano di Disaster Recovery;**
- **Modalità di rientro dall'emergenza.**

I suelencati punti vengono sviluppati nei prossimi paragrafi.

3.1 Modalità di mobilitazione delle persone interessate

I componenti del Comitato di Gestione Crisi e le altre figure interessate nell'attivazione del Piano di Continuità Operativa e di Disaster Recovery, interni ed esterni all'Amministrazione, devono essere contattati attraverso almeno uno dei mezzi di comunicazione come sopra indicato.

TABELLA CON RUOLI E RESPONSABILITA' DEL TEAM DI RIPRISTINO DELLA CO

3.2 Punti di ritrovo

Il punto di ritrovo principale è la sede operativa della scuola Piazzale del Poggio Imperiale 1 – Firenze

Nel caso in cui non sia possibile operare presso il sito primario di produzione dei dati, il Comitato di Gestione Crisi dichiarerà lo spostamento del personale e delle infrastrutture trasportabili, e darà dettaglio delle modalità di spostamento a seconda della gravità dei casi di disastro oppure prevvederà l'utilizzo dello smart working su indicazione del Dirigente Scolastico.

3.3 Circostanze in cui l'organizzazione ritiene che l'attivazione del PCO non sia necessaria

Nei casi in cui l'interruzione momentanea di un servizio non comporti perdite di dati (vedi Tabella di classificazione degli incidenti) non sarà necessario attivare il Piano di Continuità Operativa. Al contrario, come meglio specificato nella tabella descrittiva sulla classificazione degli incidenti, in tutti quei casi in cui venga riscontrata una perdita di dati da parte di una qualsiasi delle strutture dell'Amministrazione, è necessario invocare immediatamente il Piano di Continuità Operativa per non perdere tempo utile necessario al ripristino del sistema informativo. La rapidità nell'attivazione dei Piani risulta di particolare importanza poiché consente all'Ente di rimanere all'interno dei parametri di tolleranza per la riattivazione dei servizi minimi.

3.4 Modalità di gestione, manutenzione, verifica e test del PCO e del PDR

Il PCO e il PDR saranno aggiornati periodicamente secondo la normativa vigente e sottoposti ad approvazione da parte del Comitato di Gestione Crisi nel corso delle riunioni periodiche indetta dal Responsabile della Continuità Operativa. Il Piano di Continuità Operativa dovrà essere aggiornato almeno una volta ogni due anni e dovrà essere vagliato ed approvato dal Comitato di Gestione Crisi. Sulla base dei dati raccolti durante i test il Comitato di Gestione Crisi valuta la conformità del Piano di CO e in base a questo ne dichiara l'accettazione, preoccupandosi di mettere agli atti tale decisione e di notificarlo a tutte le figure interessate nelle procedure di CO e di DR.

Il Piano di Disaster Recovery dovrà essere aggiornato in relazione alle esigenze.

I responsabili del coordinamento delle operazioni per il disaster recovery dei processi e dei sistemi sono tenuti a:

- Relazionare periodicamente il Responsabile della CO sullo stato delle operazioni di ripristino dello specifico servizio in oggetto;
- Tenere traccia scritta di tutte le principali decisioni e azioni intraprese in accordo o in deroga ai piani predisposti;

- Tenere traccia di tutte le spese/acquisti richiesti all'organizzazione o sostenute direttamente;

- Il Responsabile della CO aggiorna periodicamente il Responsabile del Comitato di Gestione Crisi sullo stato complessivo delle operazioni di recovery e ripristino del servizio.

- Il Responsabile del CO/DR è tenuto a verificare l'aggiornamento periodico dei piani e degli allegati, la formazione del personale citato nei documenti, test ed esercitazioni.

- Il Responsabile ICT/l'Amministratore di Sistema è tenuto a segnalare preventivamente al Responsabile di Area/Servizio ogni cambiamento tecnologico che possa rendere inapplicabile il presente documento, variazioni rilevanti nelle criticità dei processi gestiti, e in particolare nel RTO, in modo da modificare congruentemente strategia, piani e soluzioni di tecnologiche qui contenute.

- L'Amministratore di Sistema provvede come primo passo al controllo dello stato del sistema informatico dell'Ente, valutando la situazione e gli eventuali danni delle apparecchiature, dei sistemi o di perdita dei dati trattati, e successivamente si occupa del ripristino del sistema in modo che siano mantenuti i livelli minimi di sicurezza nei dati trattati.

Qualsiasi modifica apportata al Piano di Continuità Operativa e/o al Piano di Disaster Recovery costituisce revisione del Piano stesso e pertanto deve essere messa agli atti.

Le copia del Piano di Continuità Operativa e del Piano di Disaster Recovery della scuola servizi ecologia e ambiente saranno depositate presso gli uffici oltre che salvate in maniera digitale sul sito stesso

Il Responsabile della Continuità Operativa provvede inoltre a dare copie dei piani alle figure facenti parte del Comitato di Gestione Crisi, al Segretario e al legale rappresentante.

Le versioni aggiornate dei piani dovranno anch'esse essere trasmesse alle medesime figure secondo i metodi prestabiliti nell'apposita sezione dedicata del piano nella quale sono stati inseriti tutti i riferimenti necessari.

Ciascuna versione del Piano dovrà avere un numero identificativo della data e della versione del piano.

3.5 Piano di Disaster Recovery (PDR)

Il PDR è contenuto all'interno del presente Piano di Continuità operativa**.**

3.6 Modalità di rientro dall'emergenza

Il ritorno allo svolgimento della normale attività lavorativa è la situazione tale per cui non risulta ulteriormente necessario prolungare la continuità operativa e ne consegue il rientro dall'emergenza. Il rientro dall'emergenza è nelle facoltà del Comitato di Gestione Crisi che si riunisce per la valutazione del disastro, per la dichiarazione dell'emergenza, per prendere le decisioni durante tutto l'arco temporale dell'emergenza e al termine della stessa per decidere sul rientro, dopo aver valutato le condizioni di ripristino del sistema informativo comunale e aver ripreso l'erogazione dei servizi.

La dichiarazione di rientro dall'emergenza sarà fatta nel momento in cui l'erogazione dei servizi ai cittadini abbia raggiunto livelli tali da garantire l'accesso a dati e strutture che consentano il normale svolgimento dell'attività lavorativa. Per normale svolgimento dell'attività lavorativa si intende il totale accesso alle strutture, ai dati e al sistema informatico che non pregiudichi l'erogazione dei servizi ovvero si possa ritornare alle attività come venivano svolte precedentemente alla dichiarazione di disastro e/o emergenza. Il Comitato di Gestione Crisi provvederà ad informare i Responsabili delle Aree coinvolte sul momento di rientro alla sede abituale e/o ad una diversa sede in caso di indisponibilità di quella principale.

PIANO DI DISASTER RECOVERY

In merito alla soluzione di Disaster Recovery, la scuola al momento utilizza programmi residenti. La prospettiva di fusione dei Consorzi di rifiuti in Piemonte al momento rende non opportune scelte di cambio radicali di software (legge regionale 1/2018).

1. INTRODUZIONE

Il sistema informativo di un amministrazione scolastica rappresenta il punto cardine per l'attività lavorativa dell'Amministrazione e l'erogazione dei servizi ai cittadini. Il sistema informativo è a sua volta basato su un sistema informatico che, in caso di problema, causerebbe l'interruzione di svariati servizi, causando disservizio agli utenti e di conseguenza ai dipendenti dell'Amministrazione. I danni derivanti da tali interruzioni sono valutabili però anche in funzione del tempo di ripristino dei servizi e di tutto il sistema informatico. Il corretto utilizzo e funzionamento del sistema informatico dell'Ente rappresentano inoltre la base per garantire integrità, disponibilità e riservatezza dei dati trattati, secondo quanto prescritto dal D. Lgs. 196/2003. Il Piano di Disaster Recovery è l'insieme delle informazioni legate alle azioni, ai sistemi e ai dati con i quali l'Amministrazione provvede al ripristino delle funzionalità tecnologiche e organizzative della propria struttura.

La predisposizione di un Piano di Disaster Recovery non garantisce all'Ente la continuità dei processi aziendali in caso di disastro in quanto il documento racchiude le informazioni della sola funzionalità del sistema informatico, mentre gli aspetti legati alla gestione delle risorse e all'organizzazione vengono inquadrati all'interno del Piano di Continuità Operativa, di cui il Piano di Disaster Recovery è una parte integrante.

1.1 Finalità e contenuti del Piano di Disaster Recovery

Il Piano di Disaster Recovery, parte integrante del Piano di Continuità Operativa dell'Ente, viene descritto in questa sezione appositamente rubricata ed ha la funzione di spiegare nel dettaglio le fasi necessarie per il ripristino delle risorse hardware e software utilizzate per l'erogazione dei servizi da parte dei dipendenti dell'Amministrazione.

Nel piano di DR vengono dettagliate le procedure operative necessarie per effettuare una corretta valutazione della situazione di emergenza/disastro che non consenta la normale erogazione dei servizi ai cittadini e alle imprese da parte dell'Ente. Nel presente documento vengono inoltre descritte le varie fasi per provvedere al ripristino del sistema informativo primario, ovvero del recupero dei dati e la riconfigurazione delle procedure per arginare e rientrare dallo stato di emergenza dichiarato. Vengono inoltre esposte nel piano di DR le procedure per l'attivazione del sito di DR nel caso non sia accessibile e utilizzabile il sito primario.

L'Ente ha inoltre provveduto all'analisi delle minacce possibili e dei relativi rischi che possono derivare sia da una non corretta gestione dell'infrastruttura informatica, sia dall'integrità delle apparecchiature elettroniche ed informatiche. La sicurezza e l'integrità dei dati, in termini di protezione degli stessi da varie tipologie di cause, esterne ed interne all'Ente, ha permesso di raggiungere livelli di sicurezza che permettano una drastica diminuzione delle probabilità di rischio.

L'integrità fisica dei sistemi informatici, dettagliata nei paragrafi successivi, può infatti essere intaccata o distrutta da calamità naturali (alluvioni, terremoti, fulmini, etc.), da cause accidentali (incidenti, allagamenti, distruzione dell'edificio, distruzione di personal computer, server o altri elaboratori elettronici in cui siano custoditi i dati trattati), da cause esterne (sommosse, rivolte, devastazioni, atti vandalici, eventi socio-politici).

Per assicurare l'integrità fisica dei sistemi informatici si possono inoltre adottare alcuni accorgimenti di minimo costo per proteggere fisicamente i sistemi informatici come ad esempio la collocazione degli elaboratori elettronici non a diretto contatto con il piano di calpestio per evitare o limitare i danni in caso di allagamento oppure al riparo da luoghi di passaggio per evitare rotture accidentali dovute a caduta.

L'integrità fisica delle infrastrutture, dettagliata nei paragrafi successivi, necessaria per il funzionamento dei sistemi e per poter consentire una normale attività lavorativa ai dipendenti dell'Ente, deve essere assicurata dalla continua presenza dell'elettricità nello stabile e della connessione di rete.

Deve inoltre essere prevista la disponibilità di Dispositivi UPS (Gruppi di Continuità), di linee di backup o di emergenza, in grado di subentrare in caso di guasti di varia natura, da attivare con fornitori diversi, se possibile, e nella possibilità tecnica che si attestino su centrali diverse.

Per l'integrità fisica delle infrastrutture è necessario che gli stabili utilizzati risultino, sotto il profilo prevenzionistico, essere conformi alle vigenti disposizioni in materia di igiene e sicurezza sul lavoro (D. Lgs. 81/2008) e di prevenzione incendi (DPR 157/2011 – D.M. 10/03/98).

L'integrità dei dati, indispensabile nell'attività lavorativa di un'amministrazione scolastica, deve sempre essere garantita e potrebbe essere compromessa da semplici errori umani del personale, da guasti dell'hardware, da furto di dati o di credenziali di accesso al sistema, da azioni di hacking.

Per limitare almeno la perdita dei dati o l'alterazione degli stessi è necessario predisporre minimi livelli di sicurezza e garantire un corretto e costante backup dei dati trattati, come nel seguito meglio dettagliato nel paragrafo rubricato "Politiche di sicurezza e salvaguardia dei dati".

La condizione minima e indispensabile per evitare la perdita dei dati trattati è l'esecuzione di corrette copie di backup, conservate e custodite opportunamente, con altresì salvataggio in cloud.

In alternativa, poiché la scuola non possiede sedi alternative è tollerabile la custodia dei supporti di Backup all'interno di cassaforte ubicata all'esterno dell'ente, supporti di cui deve essere garantita la rotazione con cadenza di norma quindicinale/trisettimanale.

L'Ente, dopo l'analisi delle varie tipologie di dati trattati e della spesa da sostenere, ha provveduto a configurare e implementare una soluzione tecnologica di tipo "Cloud", con la quale vengono sincronizzati i dati entro le 24 ore rispetto alla produzione degli stessi.

Tale soluzione può essere garantita in quanto il volume dei dati giornalmente modificati, risulta congruente con la velocità delle linee possedute dalle Scuole Annesse all'Educandato SS. Annunziata, per una trasmissione giornaliera.

Nel momento in cui vi sarà una produzione di dati superiore, verranno richieste ai provider specifiche di linea adeguate.

2. DESCRIZIONE DELLA SOLUZIONE DI DISASTER RECOVERY

Questa sezione viene dedicata alla descrizione della soluzione di disaster recovery adottata dall'Ente per assicurare la continuità di funzionamento del sistema informatico a fronte di eventi dannosi che comportino un'indisponibilità del servizio oltre la soglia di tolleranza.

La scelta di istituire il sito di su "Cloud", è stata dettata dalle condizioni operative che permettevano di sfruttare una soluzione con rapporto costi/benefici ottimali.

In sintesi, il processo decisionale ha tenuto in conto dei seguenti elementi:

- Volume medio-basso di dati da mantenere sul Cloud.
- Variazione giornaliera dei dati che permette la trasmissione attraverso le n.3 linee ADSL ++ tutt'ora nelle possibilità dell'Ente di cui una dedicata esclusivamente all'attività amministrativa.

in caso di avaria di uno qualsiasi dei componenti della catena di rete che va dal/dai computer client ad Internet, verrebbe a mancare la connettività necessaria per l'utilizzo delle risorse elaborative disponibili sul sito di DR. Questa è sicuramente una "criticità" conosciuta e ovvia data dalle soluzioni "basate su internet", ma è risolvibile in quanto ormai le potenzialità di collegamento sono su fibra ottica.

E' attivo inoltre un contratto di assistenza tecnica sistemistica, con Leonardo Tec (che ha anche fornito il Server) che garantisce la presenza dei propri tecnici strutturati entro 4 ore dalla richiesta di intervento.

In questa soluzione definitiva, l'attivazione del sito di DR consisterà quindi nell'unica azione di accesso in internet di qualsiasi computer, Tablet in modalità "Desktop Remoto".

3. OBIETTIVI DEL PIANO DI DISASTER RECOVERY (PIANO DI DR)

Obiettivo principale del piano di DR deve essere quello di pianificare tutte le attività di gestione e manutenzione della soluzione di DR in caso di normale svolgimento dell'attività lavorativa e di assicurare in condizioni di emergenza l'attuazione delle corrette procedure per il ripristino del sistema e il rientro dall'emergenza, con conseguente ripresa dell'erogazione dei servizi.

Il Piano di Disaster Recovery rappresenta l'insieme delle misure tecnologiche e organizzative necessarie per poter provvedere al ripristino del sistema informatico e dei dati dell'Ente in modo da riattivare l'erogazione dei servizi secondo quanto predisposto dall'Amministrazione in termini di salvaguardia dei dati e disposizione di elaboratori elettronici nella sede secondaria.

Nel caso in cui l'Ente non abbia a disposizione elaboratori elettronici pronti all'utilizzo nell'eventualità di un'emergenza, ci dovrà essere un fornitore esterno con cui l'Ente ha predisposto apposito contratto, che garantisce tempi di intervento ben definiti e prestabiliti, renderà disponibili personal computer e altre apparecchiature necessarie per permettere una riattivazione dei servizi.

Si ricorda inoltre che i servizi in Hosting, Albo Pretorio online, il Sito Web istituzionale e la posta elettronica, sono gestiti da più operatori, per cui risiedono presso i Data Center delle aziende fornitrici dei servizi, e garantiscono tempi di ripristino immediati dei servizi presenti nelle loro piattaforme in quanto vengono riversati anche su altri data center di backup, provvedendo loro stessi ai propri piani di DR.

4. INFORMAZIONI RELATIVE AL PIANO DI DR

Informazioni Statiche e Informazioni Dinamiche

Informazioni Statiche: informazioni che rimarranno costanti e non saranno oggetto di frequente revisione.

Rientrano in questa sezione tutte le informazioni strutturali relative agli stabili che ospitano sia l'ente sia la sede secondaria, qualora individuata, saranno inoltre elencati i dati sulla struttura organizzativa e gestionale dell'Amministrazione.

Gli argomenti di seguito trattati fanno parte delle informazioni statiche della sede di produzione dei dati, per cui non si dovrebbero avere aggiornamenti nel corso dei prossimi esercizi e per le quali si rimanda agli appositi paragrafi successivi in cui saranno dettagliate.

Si precisa che il sito primario risulta, sotto il profilo prevenzionistico, essere conforme alle vigenti disposizioni in materia di igiene e sicurezza sul lavoro (D. Lgs. 81/2008) e di prevenzione incendi (DPR 157/2011 – D.M. 10/03/98).

Alimentazione Elettrica. La sede degli uffici è dotata di impianto elettrico cablato a norma di legge.

I server di rete, gli apparati di rete e i personal computer sono protetti da gruppi di continuità UPS sui server atti a garantire la necessaria protezione delle apparecchiature informatiche dagli sbalzi e dall'interruzione della corrente elettrica di rete, fornendo il tempo necessario al corretto spegnimento dei sistemi informatici ad essi collegati.

Sistemi antincendio. La sede degli uffici è provvista di estintori portatili

Sistemi antintrusione. Risulta attivo un sistema antintrusione, dotato di allarme sonoro e combinatore telefonico, con sensori volumetrici.

Aree di emergenza. Non sono presenti locali attrezzati in caso di parziale inagibilità degli uffici, ma grazie all'interoperabilità delle postazioni di lavoro è possibile riallocare i dipendenti negli uffici ancora agibili.

Accesso alle banche dati e internet. L'Ente è dotato di sistema di autenticazione informatica al proprio sistema informativo, come previsto dal D. Lgs. 196/2003 e succ., automatizzato tramite funzionalità Active Directory di Windows oltre a software antivirus, presente su tutti i client, firewall su hardware dedicato con Antivirus. Gli edifici sono dotati di cablaggio di rete strutturato su cavi in rame UTP di categoria 5E.

Informazioni Dinamiche: informazioni relative al piano di DR che necessitano di un regolare e costante aggiornamento per provvedere al corretto mantenimento dello stesso piano relativamente ai cambiamenti che possono essere attuati nell'organizzazione tecnico-operativa dell'Ente.

Gli argomenti di seguito trattati fanno parte delle informazioni dinamiche per cui l'Ente potrebbe provvedere all'aggiornamento nel corso dei prossimi esercizi e per le quali si rimanda agli appositi paragrafi successivi in cui saranno dettagliate.

Backup. Le procedure di custodia dei dati trattati dall'ente prevedono l'impiego di soluzioni che contemplano sia il Backup locale secondo la normativa sulla privacy (già descritto precedentemente), sia la replica, sulle macchine virtuali del sito DR, dei dati e programmi presenti sulle unità elaborative del Server, garantendo così disponibilità dei dati e funzionalità del sito di DR.

Sistemi di protezione dati sugli elaboratori centrali. Sui sistemi informatici dell'Ente identificati come critici, sono presenti i seguenti sistemi di protezione:

- Server Dati: Doppio Hard Disk in configurazione Mirroring (RAID 1).

Nell'eventualità di evento disastroso che interessi unicamente l'unità elaborativa Server, sarà necessario commutare l'attività lavorativa sul sito di DR, continuando al lavorare tramite Desktop Remoto.

Contratti di assistenza tecnica. Sono attivi i contratti di assistenza software per le procedure gestionali informatizzate dell'Ente fornite da – TCP Technology s.r.l.- ARGO SOFTWARE – NETTUNO SOFTWARE in relazione alle specifiche competenze

5. CLAUSOLE E DIRETTIVE APPLICABILI

Norme e riferimenti di standard a cui deve fare riferimento il Piano di DR:

come da sito AGID

6. PERIMETRO DI RIFERIMENTO DEL PIANO

6.1 Descrizione del sistema informativo primario e dei servizi critici che la soluzione di DR deve garantire

Gli Uffici sono ospitati in un unico edificio in Piazzale del Poggio Imperiale 1 - Firenze

L'Ente possiede una propria struttura informatica, internamente agli edifici sulla rete locale LAN, strutturata secondo il sistema informativo basato sul modello **Client/Server**.

SCHEMA DELLA STRUTTURA INFORMATICA

Server Dati ed Applicazioni: Windows Server 2008 - 2019

Switch: D-Link

Firewall: Ubiquiti Edgerouter Firewell ER6

6.3 Fattori critici e di rischio, descrizione dei casi di disastro/indisponibilità prolungata che si intendono affrontare con la soluzione di DR

6.3.1 Fattori critici e di rischio: elenco dei possibili rischi

In questa sezione vengono dettagliati i rischi possibili e probabili a cui possono essere sottoposte le infrastrutture, fisiche e tecnologiche dell'Ente, e i dati trattati.

Per i dati trattati devono essere garantite le qualità fondamentali che, per espressa previsione normativa, dati personali oggetto di trattamento debbono sempre possedere e cioè:

a) la **disponibilità,** che assicura che l'accesso ai dati sia disponibile quando necessario. Per garantire questa "qualità" è necessario che l'accesso alle informazioni o alle risorse informatiche sia negato senza autorizzazione;

b) l'**integrità,** che garantisce della accuratezza e della completezza dei dati e delle informazioni custodite e contenute all'interno degli elaboratori ovvero sui supporti magnetici o ottici utilizzati per il salvataggio dei dati.

Per garantire questa "qualità" si rende necessario codificare ed adottare delle corrette procedure per il backup dei dati e nel contempo evitare che le informazioni correttamente salvate possano formare oggetto di modifica o di accesso senza autorizzazione;

c) la **riservatezza,** che garantisce che i dati e le informazioni siano conosciute ed accessibili solo ed esclusivamente al personale autorizzato. Il rispetto della citata "qualità" si ottiene negando l'accesso alle informazioni a tutti i soggetti, interni ovvero esterni all'Amministrazione, che non siano legittimati al trattamento ed alla conoscenza degli stessi dati da una espressa previsione normativa oppure da necessità legate all' espletamento di funzioni istituzionali.

Per garantire il rispetto di queste qualità è necessario conoscere ed analizzare le minacce che potrebbero incidere sulle stesse.

Per un soggetto Pubblico come questo, i danni che possono essere provocati alle Banche Dati che contengono informazioni personali, sensibili o giudiziarie, si possono distinguere in due macro – categorie:

- **DANNI RICOLLEGABILI AD ATTIVITÀ UMANE**
- **DANNI DERIVANTI DA EVENTI NATURALI, INCIDENTI, GUASTI MECCANICI.**

I danni che una persona, autorizzata/legittimata o meno al trattamento può apportare, volutamente inconsciamente, alle banche dati si possono classificare nelle seguenti ipotesi:

- Accesso non autorizzato ad informazioni;
- Modifica non controllata del contenuto delle Banche Dati con conseguente perdita delle caratteristiche di **correttezza, completezza e congruità logica** dei dati stessi;
- Distruzione di Banche Dati;
- Copia non autorizzata dei dati contenuti nelle Banche Dati;
- Malfunzionamento del Servizio;
- Interruzione del Servizio;
- Inserimento nelle pagine web di frasi o immagini non in linea con i fini Istituzionali propri dell'Ente;
- Inserimento nelle pagine web di informazioni non corrette, false o fuorvianti;
- Utilizzo, mediante impersonamento informatico, di macchine ed indirizzi dell'Amministrazione per il compimento di attività illecite.

Come si è detto, esistono però altri fattori di rischio non legati ad attività umane ma derivanti da eventi naturali, incidenti, avarie, guasti meccanici, che possono comunque determinare malfunzionamenti o, nei casi più gravi, interruzione di servizi, di cui è necessario tenere conto nella presente analisi.

ANALISI DI DETTAGLIO DEGLI EVENTI CHE POSSONO GENERARE DANNI E CHE COMPORTANO QUINDI RISCHI PER LA SICUREZZA DEI DATI PERSONALI TRATTATI

Gli eventi in grado di determinare dei danni e, conseguentemente, in grado di rappresentare un rischio per la sicurezza dei dati personali trattati dall'Ente, possono essere ricondotti a 3 MACRO-CATEGORIE:

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO

B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI

C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

Il dettaglio delle minacce e dei rischi propri di ciascuna categoria di EVENTI appare essere il seguente:

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO

A.1 Accesso non autorizzato ai dati personali trattati mediante impersonamento informatico

La concreta possibilità che si verifichi un'ipotesi di accesso non autorizzato a dati personali trattati su supporto informatico mediante il c.d. "impersonamento informatico" si può avere nelle seguenti situazioni:

1.I. distrazione ovvero negligenza di un Incaricato del trattamento dei dati il quale, per esempio, lascia incustodita la propria postazione di lavoro collegata ovvero non custodisce diligentemente le proprie credenziali di autenticazione.

1.II. scambio delle Password tra gli Incaricati.

1.III. carenza nel sistema e nelle procedure di attribuzione e gestione dei profili di autenticazione e di autorizzazione degli utenti.

Nelle ipotesi di accesso non autorizzato ai dati personali trattati dall'Ente mediante impersonamento informatico, un soggetto non autorizzato (interno ovvero esterno all'Amministrazione stessa), può accedere ai dati, con le credenziali di autenticazione attribuite all'incaricato legittimato all'accesso sostituendosi in tutto e per tutto al soggetto titolare delle stesse.

Secondo quanto espressamente previsto dal D. Lgs. 196/03, ogni dipendente individuato quale Incaricato del trattamento dei dati deve poter accedere **esclusivamente** a quelle informazioni che risultino essere necessarie, pertinenti e non eccedenti per svolgere correttamente il proprio lavoro e porre in essere l'attività istituzionale propria dell'Ufficio.

E' dunque necessario verificare e assicurare che l'accesso ai dati personali, sensibili e giudiziari sia rigorosamente controllato e avvenga esclusivamente ad opera dei soggetti espressamente autorizzati. L'accesso non autorizzato ai dati personali trattati dall'Ente espone agli ulteriori rischi di modifica non autorizzata, di danneggiamento, di mancanza di congruità, di perdita e di esportazione illegittima dei dati stessi.

In riferimento al punto (III.) La scuola, come già espresso, ha preso tutte le misure di sicurezza creando un Dominio Active Directory con una struttura di password complessa (lettere e numeri) e gruppi di utenza per l'abilitazione alle singole aree informatiche di competenza.

A.2 Insufficiente conoscenza del sistema informatico o dell'applicazione

In alcuni casi, il dipendente individuato quale Incaricato del trattamento dei dati, può involontariamente compiere azioni che comportano un danno semplicemente perché non è perfettamente a conoscenza delle conseguenze del suo operato a causa di una mediocre conoscenza del sistema, dello strumento informatico ovvero dell'applicazione.

Il danno che può essere provocato varia a seconda del comportamento posto in essere e può determinare:

i. Un blocco momentaneo della stazione di lavoro

ii. Un blocco che può coinvolgere anche altri utenti della Rete

iii. L'inserimento, la modifica o la cancellazione (e dunque la perdita) non voluta di informazioni e dati

iv. L'invio di dati personali, sensibili o giudiziari a soggetti non autorizzati

v. La visione di dati personali, sensibili o giudiziari a soggetti non autorizzati

In merito a tale ipotesi la scuola aveva già impartito in passato le opportune istruzioni, che con il presente vengono confermate.

A.3 Insufficiente conoscenza dei rischi e delle misure di sicurezza

Si osserva talvolta negli Incaricati del trattamento dei dati, una sorta di superficialità di comportamento con riferimento alle problematiche relative alla sicurezza informatica. Superficialità dovuta, in genere, ad una non puntuale conoscenza dei gravi rischi che possono determinarsi quale conseguenza di una condotta non improntata al rispetto delle norme tecniche dettate dal D. Lgs. 196/03.

I comportamenti più ricorrenti che si possono ascrivere a questa categoria sono:

i. La diffusione nell'ambito dell'Ufficio, tra colleghi, della componente riservata della credenziale di autenticazione o PASSWORD

ii. La negligente custodia delle credenziali di autenticazione da parte del singolo Incaricato del trattamento

iii. La circostanza che venga lasciata la propria stazione di lavoro accesa e collegata quando ci si assenta per qualsivoglia ragione dall'Ufficio

iv. La circostanza che vengano lasciate, liberamente fruibili, stampe e tabulati contenenti dati personali, sensibili o giudiziari.

Il danno che può essere determinato nelle ipotesi considerate è quello di accesso non autorizzato ai dati personali trattati, di modifica dei dati, di esportazione illegittima degli stessi e, nei casi più gravi, di distruzione.

In merito a tale comportamento la scuola aggiornerà i Documenti sulla Privacy, oltre ad informare i dipendenti circa le normative comportamentali obbligatorie per gli incaricati al trattamento dei dati.

A.4 Distrazione e Negligenza

La distrazione e la negligenza possono essere di tipo "fisico" ovvero "logico".

La distrazione/negligenza di tipo fisico, in genere, comporta direttamente danni alla strumentazione ed alle attrezzature e, in alcuni casi, indirettamente e conseguentemente danni ai dati (si rovescia la bottiglia dell'acqua sull'unità centrale, si urta la postazione di lavoro facendola cadere e danneggiandola).

La distrazione/negligenza di tipo logico invece, determina in genere esclusivamente danni ai dati trattati (durante la sessione di lavoro l'Incaricato del trattamento viene distratto da una telefonata e dimentica di salvare il documento su cui stava lavorando ovvero preme inavvertitamente dei tasti che provocano l'esecuzione di un comando non voluto).

Il danno che tale evento può determinare sui dati personali oggetto di trattamento è quello di alterazione, corruzione, cancellazione e, nei casi più gravi, perdita dei dati stessi.

A.5 Atto doloso

E' senza dubbio il più grave e pericoloso degli eventi dannosi legati al fattore umano in grado di determinare un danno ai dati personali in quanto presuppone una precisa volontà indirizzata alla manomissione ovvero alla distruzione delle strumentazioni o dei dati trattati.

Potrebbe verificarsi che, con comportamento consapevole, derivante potenzialmente da vari fattori (risentimento verso l'Ente ovvero perseguimento di fini personali), gli Incaricati del trattamento compiano operazioni illecite sulle Banche Dati assegnate.

B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI

B.1 Azione di Virus Informatici ovvero di programmi suscettibili di recare danno

Ci si riferisce all'azione di virus informatici programmati per cancellare i dati a cui gli interessati hanno accesso o comunque per danneggiarli, ovvero per causare la paralisi dei servizi erogati mediante gli strumenti informatici.

L'azione di questi agenti dannosi è generalmente innescata dallo scaricamento di programmi eseguibili di varia natura che vengono diffusi per posta elettronica sotto forma di allegati, oppure provengono da siti che, ingannando l'utente, lo inducono a salvare questi file sulla propria postazione di lavoro.

In merito a tale minaccia la scuola ha impostato:

- Sistema Antivirus professionale
- Filtro Antispam implementato sulla gestione email

B.2 Spamming o tecniche di sabotaggio

Ci si riferisce ad azioni di sabotaggio compiute da terzi tramite programmi che, sfruttando difetti del software utilizzato per la gestione della posta elettronica o di altri servizi informatici, saturano il servizio di richieste fino alla paralisi parziale o totale dello stesso. Questa azione determina l'indisponibilità temporanea dei dati gestiti dal servizio che forma oggetto di attacco.

In merito a tale minaccia la scuola ha impostato un Filtro Antispam implementato direttamente sulla consolle di gestione delle email.

B.3 Obsolescenza degli strumenti Hardware

L'obsolescenza delle attrezzature, che nel campo informatico è particolarmente rapida, oltre a rappresentare un fattore di rischio "attivo", può impedire l'attivazione e l'implementazione di misure di sicurezza fisiche o logiche che si rendano opportune per eliminare o ridurre alcuni rischi.

L'esempio che può essere fatto è quello che si riferisce alla impossibilità tecnica di installare su un vecchio elaboratore un sistema di cifratura dei dati che richiede processori di una certa potenza e sufficiente memoria.

In merito a tale obsolescenza, la scuola opera in stretta sinergia con l'Amministratore di sistema per l'aggiornamento informatico.

B.4 Malfunzionamento/indisponibilità degli strumenti Hardware

Come tutte le macchine, anche le strumentazioni informatiche sono soggette ad avarie che possono renderle inutilizzabili per periodi più o meno lunghi.

A seconda del tipo di guasto si può avere solo il blocco dell'attività della postazione di lavoro oppure anche il danneggiamento o la perdita dei dati (si pensi al caso di avaria che interessi l'hard disk).

In tale evenienza, la scuola ha stipulato dei contratti di assistenza ad intervento con aziende in grado di offrire i tempi di intervento e "depannage" adeguati al piano di CO.

B.5 Malfunzionamento Software e obsolescenza derivante da mancato aggiornamento

Ci si riferisce alla possibilità, insita in ogni software, di rivelare difetti di funzionamento inizialmente non presenti o non evidenti. Tale possibilità esiste sempre in quanto ogni software dipende da altri prodotti software (primo fra tutti il sistema operativo) e hardware (le apparecchiature di rete) che possono dover essere sostituiti o aggiornati nel tempo con altri di caratteristiche differenti. Il risultato di tale evento può essere l'indisponibilità temporanea o addirittura permanente di dati nel caso più grave, in cui cioè non sia più possibile ristabilire la situazione originaria.

Anche per tale evento sono stati stipulati opportuni contratti di Aggiornamento/manutenzione Software con le aziende produttrici o intermediarie.

B.6 Accessi esterni non autorizzati

Ci si riferisce al caso in cui vi siano intrusioni via rete, avvenute senza furto di credenziali di autenticazione ma semplicemente mediante lo sfruttamento di difetti del software, per effettuare accessi non autorizzati ai dati.

Il Firewall centralizzato di alta affidabilità oltre ad impedire accessi dall'esterno ne traccia anche i tentativi.

B.7 Intercettazione di informazioni in rete

Ci si intende riferire ad un'operazione volontaria che si basa sull'analisi e sul filtraggio dei pacchetti dati in transito sulla rete, generalmente con l'ausilio di software apposito. Il rischio è di accesso non autorizzato ai dati.

Per tale minaccia, la scuola ha scelto di utilizzare il WiFi solo per l'accesso ad internet dei device mobile, ma non per l'accesso alla rete informatica in modo da non mettere a repentaglio l'integrità dei dati da potenziali minacce. Inoltre i Cavi di rete transitano all'interno di muri e canaline di difficile accesso per un collegamento non autorizzato.

C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

C.1 Ingressi non autorizzati ad aree/locali ad accesso ristretto

Ci si riferisce alla concreta possibilità che soggetti non legittimati all'accesso possano materialmente accedere all'interno dei locali e degli Uffici in cui sono posizionati gli apparati e gli elaboratori informatici ospitanti i dati personali che formano oggetto di trattamento. In casi di questo tipo, il danno che può derivare non è solo quello, di per sé già molto grave, di accesso di soggetto non legittimato alle banche dati trattate dagli Uffici in quanto, si possono verificare anche ipotesi di modifica non autorizzata, di distruzione e conseguente perdita, di esportazione illegittima delle Banche Dati oggetto dell'evento dannoso considerato.

In relazione a tale possibilità la scuola ha provveduto alla protezione dei locali con apposite serrature le cui chiavi di accesso sono consegnate solo al personale dipendente e al Dirigente Scolastico della scuola ovvero ad amministratori individuati

C.2 Sottrazione/Furto di strumenti contenenti dati personali

Ci si riferisce all'ipotesi di furto di una postazione di lavoro (workstation) ovvero di un Server con conseguente perdita di tutti i dati ospitati nello strumento informatico oggetto di sottrazione. Nell'ipotesi considerata, il danno che si determina è sia quello legato al fatto che un soggetto non legittimato abbia accesso alle banche dati ospitate all'interno dello strumento informatico, che quello legato al fatto che l'Ente perda la disponibilità delle stesse.

In relazione a tale possibilità la scuola ha provveduto alla protezione dei locali con apposite serrature le cui chiavi di accesso sono consegnate solo al personale dipendente e al Dirigente Scolastico della scuola ovvero ad amministratori individuati. E' inoltre stato installato allarme anti intrusione.

C.3 Guasto a sistemi complementari (Impianto elettrico, climatizzazione)

Ci si riferisce a tutti quegli eventi che riguardando sistemi ed impianti esterni ma complementari agli strumenti informatici, vanno ad impattare sugli stessi inficiandone la funzionalità. Il tipico esempio di guasto a sistema complementare è quello che riguarda l'impianto elettrico ovvero l'impianto di climatizzazione.

Il rischio correlato a tale tipologia di evento è quello di danneggiamento dei dati e di indisponibilità temporanea, ovvero nei casi più gravi, permanente degli stessi.

- Blackout.

In relazione a tal guasti la scuola ha inserito un sistema di UPS (Gruppi di Continuità) per poter chiudere il lavoro correttamente durante l'eventuale Black-out.

C.4 Eventi distruttivi, naturali o artificiali accidentali o dovuti ad incuria

Include tutti gli eventi di effetto distruttivo sui supporti fisici contenenti i dati o sulle apparecchiature informatiche, indipendentemente dalla loro natura, qualora non siano già inclusi nelle casistiche precedenti.

Il rischio che si può determinare sui dati è quello di danneggiamento, indisponibilità temporanea o perdita parziale o totale degli stessi.

- Incendio parziale o diffuso;
- Scariche atmosferiche;
- Allagamenti;
- Condizioni ambientali estreme.

In relazione alla possibilità di allagamento, la scuola ha posto i computer non direttamente sul piano di calpestio, frapponendo un supporto ad hoc, ovvero ha programmato ciò

C.5 Errori umani nella gestione della sicurezza fisica

Ci si ferisce, ad ogni evento determinato da un errore umano nella gestione della sicurezza sugli ambienti fisici ospitanti gli apparati e gli strumenti informatici. In questa categoria di eventi sono da ricomprendersi, a mero titolo esemplificativo, sia le ipotesi di serrature di porte ovvero di armadi e cassetti lasciate erroneamente aperte che le ipotesi di protezioni fisiche non presenti ovvero installate in modo non conforme alla norma tecnica. Il rischio correlato a tale tipologia di evento va dall'accesso non autorizzato ai dati fino alla perdita ed alla distruzione degli stessi nei casi più gravi.

6.3.2 Sicurezza Informatica

L'accesso al sistema informatico dell'Ente viene garantito attraverso la verifica di apposite credenziali costituite da un codice identificativo (User ID) e da una password, attribuite in via esclusiva a ciascun dipendente individuato quale incaricato del trattamento dei dati e il Server di Dominio conserva tutte le informazioni sulle utenze e sui permessi di accesso alle risorse disponibili, previa verifica della validità delle login e delle password fornite dai Client.

Ogni utente risulta inserito in un Gruppo (relativo al settore di competenza) al fine di avere una serie di dati e cartelle *Private* (per l'utente Responsabile di Area), di *Gruppo* (per tutti gli utenti del servizio relativo), o *Pubbliche* (per tutti gli altri utenti che devono attingere dati di loro possibile interesse)

Per quanto attiene alla gestione del sistema e delle procedure per l'autenticazione informatica, si è provveduto ad attribuire a tutti i dipendenti individuati quali Incaricati del trattamento dei dati, una credenziale di autenticazione costituita da una User-Id e da una Password. Tuttavia la Password, che rappresenta la componente riservata della credenziale di autenticazione, anche laddove attribuita, risulta essere sempre composta da un numero di caratteri alfanumerici pari almeno ad otto, secondo quanto espressamente dettato dalla Regola 5 contenuta nell' Allegato B del D. Lgs. 196/03. La stessa Password inoltre, viene autonomamente modificata da ciascun utente al primo utilizzo e, successivamente, con cadenza periodica.

Per quanto riguarda l'utilizzo di strumentazioni informatiche di altro genere (es. dispositivi di firma digitale), con possibilità di utilizzo con conseguenze giuridiche ed economiche interne od esterne (es.: mandati di pagamento, ordinativi informatici, lettere, provvedimenti), la prassi in uso prevede che l'utilizzo avvenga o personalmente a cura del titolare del dispositivo, ovvero per mandato ad operare mediante somministrazione dei mezzi necessari - ivi compreso il dispositivo di firma digitale in caso d'urgenza, sotto il diretto controllo oppure previe istruzioni.
E' evidente che l'uso in difformità dalle istruzioni è non legittimo.
I sistemi per evitare utilizzi fraudolenti possono consistere in uno svolgimento del procedimento che coinvolga necessariamente più soggetti per poter ottenere l'effetto finale verso terzi: es. istruttoria e precaricamento dei dati da un soggetto (non in disponibilità del sistema di firma), e firma da un altro soggetto (non addetto all'istruttoria e al prevaricamento).

Per la protezione da accessi non autorizzata da parte degli Amministratori di sistema è stato predisposto un sistema SYSLOG, compatibile rispetto alle Normative sulla Privacy in merito alle Pubbliche Amministrazioni.

6.3.3 Descrizione dei casi di disastro/indisponibilità.

In questo paragrafo si trova una elencazione dei casi in cui sarà attivata la soluzione di DR per i servizi da erogare nel caso in cui si presenti l'indisponibilità del sistema informatico dell'Ente o un qualsivoglia problema legato ad esso. Nello specifico devono essere individuati i casi di disastro e/o di indisponibilità del sistema informatico dell'Ente in cui si provvederà all'attuazione della soluzione di DR.

Rischi considerati:

- Mancanza di erogazione del servizio dovuta all'impossibilità di accedere ai dati e alle banche dati;
- Distruzione delle infrastrutture IT ovvero del CED;
- Impossibilità di accedere al CED o ai locali destinati nei quali sono stati collocati server, apparati di rete e di backup;
- Mancanza di erogazione del servizio dovuta a un funzionamento non corretto degli applicativi gestionali utilizzati dai dipendenti dell'Ente.

Rischi non considerati:

- Contemporanea indisponibilità del sito primario e secondario;
- Contemporanea indisponibilità dei dati presenti nel sito primario e nel secondario;
- Indisponibilità dei servizi pubblici (esempio: rete elettrica, rete fonia, internet etc.).

7. ORGANIZZAZIONE E PERSONALE

Organizzazione, ruoli e responsabilità, strutture e personale coinvolto nelle attività.

Si rinvia alle tabelle più sopra elaborate.

I responsabili delle risorse coinvolte nelle operazioni di ripristino, in particolare i **Responsabili di Area** sono tenuti a segnalare tempestivamente al Responsabile CO condizioni di aggravamento del rischio e situazioni del pericolo per il personale alle proprie dipendenze.

In particolare, i responsabili sopra citati sono esentati dall'obbligo di applicare parzialmente o totalmente il presente piano di ripristino nel caso ravvisino l'insorgere di condizioni di rischio o di aggravamento del rischio per il proprio personale.

Nella tabella che segue vengono mostrate le responsabilità per la soluzione di disaster recovery, secondo i livelli attuativi e di ripristino dei vari sistemi e delle apparecchiature.

Modalità di attivazione del personale.

Le figure e le persone citate nella sezione precedente devono essere contattate attraverso qualsiasi mezzo di comunicazione l'Ente e/o il Responsabile della Continuità Operativa possa utilizzare, pertanto nelle pagina successiva vengono dettagliati diverse metodologie di contatto.

Tutte le figure/persone interessate vengono meglio dettagliate nel prospetto di seguito proposto, le responsabilità e i ruoli di ciascuno sono stati meglio descritti in precedenza.

Il Comitato di Gestione Crisi provvederà ad informare il Responsabile dell'Area coinvolta ovvero tutti i

responsabili in caso di evento dannoso diffuso, sul momento di rientro alla sede primaria e/o ad una diversa sede definitiva in caso d'indisponibilità di quella principale.

Il Comitato di Gestione Crisi stabilisce inoltre il momento di chiusura della crisi, comunicandolo alle funzioni coinvolte nelle operazioni di Recovery.

8. POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI

In questa sezione vengono descritte le procedure di backup e archiviazione dei dati poste in essere dall'Ente per evitare una qualsiasi perdita dei dati nel sito primario e di salvaguardia degli stessi attraverso la copia schedulata e custodita nella sede remota. Viene dato infatti forte rilievo non solo alle procedure, alla tempistica e alla schedulazione dei backup per la salvaguardia dei dati conservati e custoditi nel sito remoto, ma vengono descritte anche tutte le impostazioni e le configurazioni poste in essere per il backup dei dati presente nel sito primario.

Il backup è un punto fondamentale nelle procedure di disaster recovery e per garantire maggiori livelli di sicurezza è fondamentale la gestione in Cloud in modo che le copie di sicurezza dei dati siano collocate sui server certificati

La scuola, come già meglio descritto in precedenza, per provvedere alla conservazione dei propri dati in loco utilizza le copie di Backup locali su server disco raid. Le operazioni di backup sono eseguite automaticamente e ad intervalli prestabiliti

9. FASI DELLA SOLUZIONE DI DISASTER RECOVERY

1. Valutazione della situazione di crisi/disastro/indisponibilità del sito primario;
2. Dichiarazione del disastro;
3. Notifica, informativa ed attivazione delle strutture e del personale coinvolto nelle attività connesse alla dichiarazione di disastro;
4. Attivazione del Piano di DR e delle procedure ad esso connesse;
5. Attivazione del sito di DR e ripristino del sistema informativo primario, colpiti dal disastro o dalla situazione di indisponibilità;
6. Gestione dei sistemi informativi presso il sito di DR in condizioni di emergenza, durante il periodo di disastro o indisponibilità;
7. Ripristino del sistema primario con la formale "Dichiarazione di fine emergenza" da parte del Comitato di Gestione Crisi.

Attivazione del Piano di DR e delle procedure ad esso connesse

La responsabilità di attivazione del Piano di Disaster Recovery è del Comitato di Gestione Crisi o di altra figura/persona delegata facente funzioni.

Attivazione del sito di DR e ripristino del sistema informativo primario, colpiti dal disastro o dalla situazione di indisponibilità

La tabella di seguito riportata descrive le attività da intraprendere per ripristinare il sistema informatico e per attivare il sito alternativo. Nella tabella sono inoltre riportati i responsabili delle rispettive attività; la parte descrittiva dovrà essere compilata ed allegata da parte dei vari responsabili che in caso di dichiarazione dell'emergenza dovranno dettagliare e specificare le decisioni prese.

Durante lo svolgimento delle attività è importante che il Responsabile della Continuità Operativa tenga traccia delle decisioni prese, delle spese sostenute e dell'effettivo consumo delle risorse (sia umane che materiali) utilizzate per ripristinare i servizi in modo tale da poter fornire, alla fine delle attività, un resoconto completo da allegare al Piano stesso e da inviare all'Agenzia per l'Italia Digitale.

STEP ATTIVITA' RESPONSABILE DESCRIZIONE

Step	Attività	Responsabile	Descrizione delle decisioni intraprese
1	Comunicazione Inizio Attività Sistemi Infrastruttura	Responsabile della Continuità Operativa	
2	Comunicazione Inizio Attività	Amministratore di Sistema	
3	Verifiche Attività Sistemistiche	Fornitore Assistenza Sistemistica	
4	Verifiche delle Attività Applicative	Fornitore Assistenza del Gestionale	
5	Comunicazione di Fine Attività	Amministratore di Sistema	
6	Comunicazione Fine Attività Sistemi Infrastruttura	Amministratore di Sistema	
7	Comunicazione Inizio Sistemi Trasversali	Amministratore di Sistema	
8	Comunicazione Inizio Attività	Amministratore di Sistema	
9	Verifiche e Attività Sistemistiche	Fornitore Assistenza Sistemistica	
10	Verifiche Attività Applicative	Fornitore Assistenza del Gestionale	
11	Comunicazione di Fine Attività	Amministratore di Sistema	

12	Comunicazione di Fine Attività Sistemi Trasversali	Amministratore di Sistema	
13	Comunicazione di Fine Attività Sistemi Dedicati	Amministratore di Sistema	
14	Comunicazione Inizio Attività	Amministratore di Sistema	
15	Verifiche Attività Sistemistiche	Fornitore Assistenza Sistemistica	
16	Verifiche Attività Applicative	Fornitore Assistenza Gestionale	
17	Comunicazione Fine Attività	Amministratore di Sistema	
18	Comunicazione di Fine Attività Sistemi Dedicati	Amministratore di Sistema	
19	Comunicazione al Comitato di Crisi della Chiusura attività sul sito di DR	Responsabile della Continuità Operativa	

10. GESTIONE DEL PIANO

Descrizione delle attività per garantire l'aggiornamento/revisione del piano di DR e i principali adempimenti necessari a garantire la verifica periodica dell'adeguatezza della soluzione di DR con le esigenze di salvaguardia dei dati e erogazione dei servizi dell'Amministrazione.

Il **Responsabile della Continuità Operativa**, è tenuto a verificare l'aggiornamento periodico dei piani e degli allegati, la formazione del personale citato nei documenti, testing e esercitazioni.

L'**Amministratore di sistema** è tenuto a segnalare preventivamente al Responsabile di Area o al Responsabile della Continuità Operativa ogni cambiamento tecnologico che possa rendere inapplicabile il presente documento, variazioni rilevanti nelle criticità dei processi gestiti, e in particolare nel RTO, in modo da modificare strategia, piani e soluzioni tecnologiche contenute nel piano stesso.

AGGIORNAMENTI DEL PIANO C.O./D.R.

DATA	NOTE

11. COLLEGAMENTI/EVENTUALI INTERAZIONI CON ALTRI ENTI/SOGGETTI

Consiglio di Amministrazione dell'Educandato SS. Annunziata -Città metropolitana

12. PROCEDURE DI TEST

L'Ente deve prevedere e provvedere all'esecuzione di test periodici ed operativi in modo che sia garantito l'aggiornamento e il controllo dei piani; le modifiche del piano di Disaster Recovery saranno effettuate ogni qualvolta venga acquistata una nuova apparecchiatura o elaboratore elettronico per adeguamento del sistema informatico che vadano a impattare sull'attuazione della soluzione tecnologica. Oltre

all'adeguamento tecnologico del sistema informatico si dovrà provvedere all'aggiornamento del Piano di DR anche nel caso in cui si modifichi la metodologia utilizzata per il disaster recovery; questo dovrà essere controllato nel corso dei test periodici che dovranno essere relazionati e inseriti nel Piano.

Possono comunque verificarsi condizioni che richiedono specifiche procedure di manutenzione straordinaria per cui si dovrà provvedere ad un adeguamento del Piano:

- modifiche delle figure facenti parte del Comitato di Gestione Crisi;
- modifiche dei Responsabili delle Aree/Servizi;
- modifiche legate ai gestionali utilizzati dall'Ente e/o al fornitore;
- modifica dell'amministratore di sistema;
- modifica del fornitore dei servizi di assistenza hardware;
- modifica del fornitore dei servizi di assistenza software;
- modifiche dei contatti di qualsiasi figura interessata nelle procedure di CO e di DR o comunque sopra elencata.

L'Ente deve provvedere, periodicamente, ad effettuare i test di verifica e corretto funzionamento della soluzione di disaster recovery. I test consistono nelle seguenti simulazioni sul sito di DR:

- Il Responsabile della CO, esegue Comunicazione del Test di DR ai Responsabili di Area.
- Il Responsabile della CO attiva il Piano di DR nelle modalità operative simulate.
- L'Amministratore di Sistema controlla l'effettivo aggiornamento dei dati estraendone una serie significativa a campione. Esempio:

- Controllo del Database Gestionale;
- Controllo della data e della consistenza degli ultimi Documenti creati sul Server.

- Ogni Responsabile di Area esegue una serie di operazioni standard tipiche dell'Area/Servizio per verificare l'efficienza e l'aggiornamento del sito di DR.

Queste verifiche devono essere eseguite in considerazione delle tempistiche di aggiornamento del sito di DR concordate con il Provider.

Alla conclusione delle procedure di test deve essere redatta una relazione, a cura del Responsabile della Continuità Operativa e conservata agli atti, la quale deve essere fornita in copia alle figure che compongono il Comitato di Gestione Crisi.

La suddetta relazione deve descrivere i procedimenti effettuati per il test del disaster recovery e deve evidenziare gli eventuali discostamenti dal corretto andamento delle procedure.

In questa sezione saranno elencate e allegate le valutazioni effettuate in seguito alle procedure di test che andranno a formare le successive versioni aggiornate dei Piani in oggetto.

Si procede alla descrizione nel dettaglio delle fasi del test di disaster recovery:

SCENARIO A: PERDITA SITO PRIMARIO

La simulazione della perdita ovvero dell'impossibilità all'utilizzo del Server, consiste in:

- interruzione della sincronizzazione delle copie di sicurezza e del riallineamento dei dati effettuate presso la sede remota;
- procedure di collegamento del sistema remoto (sul sito di DR);
- procedura di avvio degli applicativi;
- procedura di avvio del singolo servizio o dei servizi;

- procedura di verifica degli applicativi testati;

- procedure di ripristino della soluzione di disaster recovery.

SCENARIO B: DATA RECOVERY

La simulazione della perdita dei dati, consiste in:

- interruzione della sincronizzazione delle copie di sicurezza e del riallineamento dei dati effettuate presso la sede di DR;
- procedure di collegamento del sistema remoto (sul sito di DR);
- procedure di recupero o di acquisizione di nuove apparecchiature elettroniche se necessario;
- procedure di ripristino della soluzione di disaster recovery.

APPENDICE A

Nome Amministrazione	Scuole Annesse all'Educandato SS. Annunziata
Sede centrale (città)	Sede operativa Piazzale del Poggio Imperiale 1
Tipologia Ente	Scuola pubblica
AOO (Area Org.Omog.)/ ENTE	Istituzione scolastica
Indirizzo PEC per le comunicazioni	five010004@pec.istruzione.it
Data compilazione	Dicembre 2022
Codice Fiscale	80020090488

Morfologia Edificio	SITO DI PRODUZIONE
Sezione Verticale	Primo e secondo e terzo piano
Piani interrati e seminterrati	n. 1
Solaio a falde inclinate o piatto	n. 1
Abbattimento Barriere Architettoniche (rampa, montascale, ascensore)	Ascensore, montacarichi
Recinzione Esterna	Presente
Cancello Esterno	Presente
Porte Blindate	Non presenti
Finestre con Grate Metalliche	Presenti
Vetri Antisfondamento	Non Presenti
Videosorveglianza interna ed esterna all'edificio	Presente

Gestione supporti registrazione video	Presente
Controllo accessi automatizzato	Presente
Vigilanza attiva della Sede	Presente
Allarme antincendio	Presente
Dispositivi Antincendio (centralizzato, estintori, ril. fumo, ril. calore)	Estintori portatili

Rilevazione automatica e spegnimento Incendi	Non presente rilevazione automatica incendi
Verifica e regolare manutenzione impianti antincendio	Revisione semestrale estintori
Sensori antiallagamento	Non presenti
Zona a rischio idrogeologico	No
Porte antipanico e uscite di sicurezza Segnalate	Si
Impianto Climatizzazione	Parzialmente presente
Impianto elettrico a norma (quadro elettrico, interruttori magnetotermici differenziali)	Presente
Impianto elettrico con linee di distribuzione sezionate	Presente
Luci di emergenza	Presenti
Verifica periodica Impianto Elettrico.	Viene eseguita verifica periodica messa a terra
intervento, automatico\manuale, autonomia)	Non presente
Gruppo elettrogeno ridondato (tempi di intervento, automatico\manuale, autonomia)	Non presente
Autonomia idrica	Non Presente
Gruppo continuità centralizzato (autonomia a pieno carico)	Non Presente
Gruppo continuità individuale (P.c., Server, Apparati)	Presente
Gruppo di continuità ridondato	Non presente
Verifica periodica dei dispositivi UPS	Attuata
Cablaggio di rete strutturato	Presente, su cavi in rame UTP CAT 5E
Ridondanza punti rete cablaggio Strutturato	Non presente

Gestione automatizzata di autenticazione al sistema informativo	Presente
Architettura elaborativa (client/server, P2P o P2P avanzata)	Client Server

Sistemi operativi Server	Windows Server 2008 - 2019
Ubicazione Server	Archivio
Protezione accessi ai Server (porta blindata, grate finestre, accesso esclusivo)	Locale ad accesso controllato
Porta tagliafuoco sala CED	Non presente
Protezione ambientale locali server (estintori, climatizzazione, rack)	Mobile Rack per gli apparati di rete, Server con Case Tower climatizzazione autonoma, estintori immediate vicinanze.
Presenza di materiale infiammabile/non pertinente in sala CED	Presente
Sistemi di protezione su Server (ridondanza alimentazione e raid)	Alimentazione ridondata: • raid 1 sui Server Dati
UPS Server (autonomia a pieno carico)	30 minuti autonomia
Replica server	Non Presente
Apparati di rete (switch, router, firewall)	GESTIONE CDA
Ridondanza Apparati di rete (switch, router, firewall)	Router Internet per Rete ADSL Wireless
Ubicazione apparati di rete	Gestione CDA
Protezione apparati di rete (UPS)	Parziali
Ubicazione dispositivi di backup custodia supporti (locale, rack, antincendio, protezione accessi)	Stanza chiusa a chiave
Protezione dispositivi di backup (UPS)	Presente

Tipologia backup	Backup completo dei dati presenti su Cloud Backup parziale in locale
Software backup	Argo backup Nettuno Backup Web
Backup dei soli dati	Si
Backup degli applicativi (software e configurazioni)	No
Backup in cloud	Si
RTO (tempo massimo per ripristino di un sistema/servizio)	giornaliero
RPO (ultima copia dati valida)	giornaliera
Servizi in hosting	Sito internet istituzionale
Posizionamento P.c. (sollevati da terra, collegati a linea dedicata, non di intralcio)	Tutti i PC, linea alimentazione dedicata
Presenza di postazioni client di importanza critica (dati e programmi solo su tali postazioni)	Programma di contabilità
Procedure e supporti backup di postazioni client	Assente
Presenza di muletti già configurati	In preparazione
Interoperabilità postazioni di lavoro	SI'
Dotazione Notebook	Si
Gestione posta elettronica (client o web mail, i dipendenti sanno come accedere alla web mail)	Mista. I dipendenti hanno ricevuto le istruzioni per l'accesso alla web mail
Backup programmi di gestione posta Elettronica	Tutta la posta è archiviata su cloud, quindi sotto backup
Esiste un archivio, debitamente custodito, con tutte le credenziali delle e-mail e PEC istituzionali	Si
Gli elaboratori vengono regolarmente Manutenuti	Si, a livello software e Sistemi operativi
Solo manutenzione straordinaria	Si, manutenzione su chiamata su guasti hardware
L'Ente ha un piano codificato di rinnovo/implementazione del sistema Informatico	No

Antivirus tipologia	Eset
Linea internet ADSL Uffici	ADSL Principale fornita da Consiglio di Amministrazione, ulteriore linea fornita da Città metropolitana
Linea internet ADSL Laboratori	linea ADSL gestite CDA
Telefono	Centralino analogico fornito da CDA
Aree di emergenza da dedicare all'attività lavorativa in caso di parziale inagibilità (cablate etc.)	Postazione retro portineria
Contratto di assistenza tecnica hardware/software	Assistenza Programmi Gestionali Argo Software e Nettuno Software Assistenza Hardware e Software apparati Firewall TCP Technology s.r.l.