Istituto Comprensivo Statale di Certosa di Pavia
P.zza Falcone e Borsellino, 4 – 27012 Certosa di Pavia
Telefono 0382 92 57 46 – www.scuolecertosa.gov.it
C.F. 96039190184 – C.U. UFEQVV
pvic806004@pec.istruzione.it - pvic806004@.istruzione.it
dirigente@scuolecertosa.gov.it – segreteria@scuolecertosa.gov

Disaster Recovery Planning

Il Disaster Recovery Planning è un documento che non descrive solo procedure tecniche ma definisce ruoli e responsabilità nella gestione fisica dei dati, sia nella routine quotidiana che nel caso di eventi disastrosi. Ovviamente ciò che viene descritto non è applicabile al solo caso di disastro totale ma anche ai vari sottocasi di perdita parziale dei dati o dell'infrastruttura (anche la recovery della singola email, per esempio)

Il Disaster Recovery Planning diventa il punto centrale del Documento Programmatico sulla Sicurezza per quanto riguarda la sicurezza "fisica" dei dati.

Il documento è stato redatto e curato dalla dirigente scolastica dott.ssa Lorena Annovazzi.

Il nuovo CAD contiene disposizioni importanti relative alla sicurezza digitale (art.51) sia sulla continuità operativa, sia sul *disaster recovery.*

Questa Istituzione in qualità di pubblica amministrazione deve predisporre appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività.

Per Disaster Recovery si intende quindi l'insieme di misure tecnologiche e organizzative dirette a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi a fronte di gravi emergenze.

Adempimenti:

Il Codice della Amministrazione Digitale (art.50 bis) prevede che ciascuna amministrazione adotti e gestisca nel tempo un Piano di Continuità Operativa e un Piano di Disaster Recovery.

Il primo deve essere aggiornato con cadenza almeno annuale, ed entro 31 dicembre di ogni anno ed inviato (nella versione aggiornata) al DigiPA.

Piano dei Sistemi

1. i possibili livelli di disastro

2. la criticità dei sistemi/applicazioni.

Per una corretta applicazione del piano, i sistemi devono essere classificati secondo le seguenti definizioni:

- **Critici:** Le funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa.
- **Vitali:** Le funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, e queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).
- **Delicati:** Queste funzioni possono essere svolte manualmente, per un lungo periodo di tempo. Il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

- **Non-critici:** Le funzioni possono rimanere interrotte per un lungo periodo di tempo, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Le procedure applicative, il software di sistema ed i file che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente. La criticità di applicazioni, software di sistema e dati, deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere.

Un piano d'emergenza deve valutare le strategie di ripristino più opportune su: siti alternativi, metodi di back up, sostituzione dei ruoli e responsabilità dei gruppo degli operatori.

La prolungata indisponibilità del servizio elaborativo derivante in particolare situazione di disastro, e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo.

Le problematiche di natura informatica e quindi i sistemi che gestiscono i dati e le attività del nostro Istituto Comprensivo i punti su cui concentrare l'attenzione quando si deve redarre o ipotizzare un piano di analisi del rischio e disaster recovery, sono vari:

Integrità fisica dei sistemi informatici, che può essere messa a repentaglio da calamità naturali , cause accidentali o cause esterne ;

Integrità delle infrastrutture necessarie al funzionamento dei sistemi: elettricità, connettività di rete.

Integrità dei dati da azioni di cracking, errori umani, virus, guasti hardware ecc.

L'analisi dei rischi deve considerare la loro probabilità e il valore dei dati o dei beni da proteggere. E' ovvio che qualsiasi dispositivo e misura di disaster recovery non deve costare più di quanto valgano i beni stessi da proteggere.

Partiamo dal presupposto che nel concepire un piano di disaster recovery si devono considerare vari aspetti:

- Costo delle procedure di sicurezza e protezione;

- Efficacia di queste misure in riferimento a diversi tipi di rischio;

- Analisi dei rischi, delle loro probabilità e livello di pericolo;

- Valore dei dati e dei beni da preservare.

- Tempi di ripristino della normale funzionalità, o quantomeno della funzionalità minima indispensabile dei sistemi;
- Costi per il ripristino

- Impatto delle relazioni con l'utenza e con gli stackeolder e metodi per limitarne il danno d'immagine.

Possiamo illustrare alcune precauzioni e indicazioni di massima per prepararci ad un disastro e limitarne o prevenirne i danni.

Hanno campi di applicazione e costi diversi, ma riassumono la maggior parte delle procedure e accorgimenti comunemente previsti:

- **Backup dei dati**. E' la condizione minima indispensabile: tutti i dati importanti vanno backuppati. Il mezzo su cui viene mantenuto il backup dovrebbe essere custodito in un luogo fisicamente distante, test di ripristino e di verifica dell'integrità dei dati va svolta regolarmente così come un analisi di quali dati vengono effettivamente copiati e se questi sono tutti i dati da copiare.
- **Impianto elettrico** a norma, che offra inoltre sufficiente protezione da fulmini, con gruppi di continuità che suppliscano a brevi interruzioni di elettricità ed eventualmente generatori per far fronte a prolungati black-out.
- **Impianto anti incendio** a norma, in grado possibilmente di individuare ed estinguere automaticamente principi di incendio, senza compromettere la funzionalità dei dispositivi elettronici stessi.
- **Linee di backup** o di emergenza, in grado di subentrare in caso di guasti di varia natura, tali per cui ha senso utilizzare per il backup linee di fornitori diversi che si attestino su centrali diverse.
- **Piccoli accorgimenti** di costo minimo e buon senso per proteggere fisicamente i sistemi informatici: tenere le macchine sollevate da terra per limitare i danni da allagamento; fissarle a supporti per evitare cadute accidentali o causate da lievi scosse telluriche; mantenerle in

un posto riparato (da luoghi di passaggio o di lavoro fisico); sistemare i cavi vari (alimentazione, rete, video...) in modo tale da evitare che qualcuno rischi di inciamparci e via dicendo.

Tecniche di Disaster Recovery

Sistemi e dati considerati importanti vengono ridondati in un "sito secondario" o "sito di Disaster Recovery" per far sì che, in caso di disastro (terremoto, inondazione, incendio,attacco haker, ecc...) sia tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile attivare le attività sul sito secondario al più presto e con la minima perdita di dati possibile.

In particolare, i livelli di servizio sono usualmente definiti dai due parametri:

1. L'RTO (Recovery Time Objerctive)è il tempo di inattività massimo consentito prima del ripristino di sistemi, applicazioni e funzioni.
2. L'RPO (Recovery Point Objective) rappresenta il momento più recente al quale sistemi e dati devono essere ripristinati dopo un'interruzione delle attività e stabilisce la quantità massima di dati che un'azienda accetta di sacrificare a seguito di un errore.

Entrambi rappresentano un obiettivo concreto per una soluzione per la continuità e per il ripristino di emergenza.

Replica sincrona

La replica sincrona garantisce la specularità dei dati presenti sui due siti poiché considera ultimata una transazione solo se i dati sono stati scritti sia sulla postazione locale che su quella remota. In caso di evento disastroso sulla sede principale, le operazioni sul sito di Disaster Recovery possono essere riavviate molto rapidamente.

Replica asincrona

In questo caso il sito che si occuperà della replica può trovarsi anche a distanze notevoli. In questo modo è possibile affrontare anche disastri con ripercussioni su larga scala (come ad esempio forti scosse sismiche) che altrimenti potrebbero coinvolgere entrambi i siti (se questi si trovano nelle vicinanze).

Tecnica mista

Per garantire la disponibilità dei servizi anche in caso di *disastro esteso* e al tempo stesso ridurre al minimo la perdita di dati vitali si può ricorrere ad una soluzione di tipo misto: effettuare una copia sincrona su un sito intermedio relativamente vicino al primario e una copia asincrona su un sito a grande distanza

Backup, copia di sicurezza o copia di riserva

Conservazione di materiale fatta per prevenire la perdita totale dei dati archiviati nella memoria di massa dei computer (siano essi postazioni di lavoro o server).
L'attività di backup è un aspetto fondamentale della gestione di un computer in caso di guasti, manomissioni, furti, ecc., ci si assicura che esista una copia dei dati ed è quasi sempre impostata in maniera automatica e svolta normalmente con una periodicità stabilita (per esempio una volta alla settimana).Devono inoltre essere conservati in accordo con le politiche di sicurezza dell'Istituto, per esempio, ma non solo, per questioni legate alla privacy.

Funzionalità programmi di backup

Un programma di backup deve fornire alcune funzionalità indispensabili ovvero:

- Copia immagine di un disco rigido
- Copia selettiva di cartelle e singoli files
- Criteri di selezione per la ricerca dei contenuti salvati e per la scelta di quelli che devono essere oggetto di backup (per data, tipo di file, autore della modifica);
- Compressione dei contenuti per ridurre la memoria richiesta per la copia;
- Protezione dei dati copiati tramite password e crittografia.

Per il nostro Istituto una caratteristica importante del backup è che questa attività non vada a sovrapporsi con l'operatività quotidiana, caricando i sistemi informatici e rallentando i tempi di

risposta agli utenti. Per questo motivo vari sistemi di backup vengono usati quando normalmente gli utenti non lavorano su quel programma o sulla rete Lan.

Per aumentare la velocità del backup, solitamente vengono applicati uno o più delle seguenti pratiche:

- Backup differenziale

  il backup differenziale registra le differenze tra un file da copiare con quello già copiato ed è utile per file di grandi dimensioni e che necessitano di un backup completo e quotidiano, come i database.

- Compressione

  la compressione è ottenuta tramite compressione dei dati prima che vengano registrati sul supporto di backup.

La conservazione dei supporti di backup in posizioni fisicamente distinte e separate dai sistemi in uso è strettamente necessaria, per evitare che in caso di evento disastroso, le copie vadano perse insieme agli originali.
Il ripristino dei dati copiati con l'operazione di backup è detto restore . L'amministratore di sistema o gli utenti che hanno diritti di accesso analoghi provvedono al ripristino dei file richiesti.

Il Backup Remoto che è un servizio di salvataggio dati che esegue copie di backup, attraverso la linea internet, verso appositi server collegati al web. Nella maggioranza dei casi si usa tramite un software apposito. Per ottenere un processo realmente efficace è necessario pianificare e effettuare dei test di disaster recovery prima che sorga l'effettiva necessità ed organizzare preventivamente un politica di bakup.

Sicurezza Informatica

Si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione dell'integrità logico-funzionale di un sistema informatico e dei dati in esso contenuti Tale protezione è ottenuta attraverso misure di carattere organizzativo e tecnologico tese ad assicurarne l'accesso solo ad utenti registrati (autenticazione) la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (permessi), l'oscuramento (cifratura) e la correttezza (integrità) dei dati scambiati in una comunicazione nonché la protezione del sistema da attacchi di software pericolosi. La sicurezza informatica è un problema sempre più sentito in ambito tecnico-informatico per via della sempre più spinta informatizzazione della società e dei servizi in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione degli attaccanti o *hacker*.

L’interesse per la sicurezza dei sistemi informatici è dunque cresciuto negli ultimi anni proporzionalmente alla loro diffusione ed al loro ruolo occupato nella collettività.

Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, come la robustezza del software di base e applicativo oltre alla affidabilità dei computer e degli ambienti in cui essi sono collocati. Il nostro server infatti è collocato in un ambiente dotato di allarme al fine di garantire la massima sicurezza anche perché il sistema informatico deve essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia da eventi accidentali; inoltre deve impedire l'accesso abusivo ai dati.

Perdita dei dati

Le cause di probabile perdita di dati nei sistemi informatici possono essere molteplici, ma in genere le possiamo raggruppare in due eventi:

Eventi indesiderati;

Qui ci sono quelli per lo più inaspettati come gli attacchi Hacking che vengono fatti tramite la rete internet o da parte di utenti che si intrufolano abusivamente all’interno del sistema riuscendo ad ottenere piena disponibilità della macchina per gestire risorse e dati senza avere i giusti requisiti richiesti ma tramite software costruiti da loro stessi.

Eventi causati accidentalmente dall'utente stesso, tipo: uso difforme dal consigliato di un qualche sistema, guasti imprevisti, ecc…

Già nel Decreto programmatico della sicurezza del nostro Istituto (documento ora non più obbligatorio) erano state descritte chiaramente alcune indicazioni atte a garantire la sicurezza e l'integrità dei dati:

"I computer, inclusi i server, sono sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti;
il server è collegato ad un gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica.
L'integrità dei dati sul server amministrativo è garantita da una procedura di backup che avviene settimanalmente attraverso un'unità di backup a nastro.
Tutti i PC della rete amministrativa vengono protetti da password per impedire al personale non autorizzato l'accesso alla rete.
L'introduzione di password di BIOS all'accensione dei personal computer, di password dello screen-saver e di password per l'accesso in rete determina un soddisfacente livello di protezione dei dati contenuti nei PC.
L'introduzione delle password e di apposito software antivirus inibisce ad estranei l'uso dei personal computer, attraverso i quali si accede alla posta elettronica.
Per l'invio di messaggi email a più destinatari, sono state fornite al personale istruzioni affinché quale destinatario venga sempre indicata la scuola con l'indirizzo email e in CCN i destinatari, in modo che non possano essere individuati gli indirizzi email degli altri destinatari attraverso la funzione di proprietà."
Nel DPS si affermava che per garantire la sicurezza delle aree in cui i dati sono trattati elettronicamente, sono state introdotte sui personal computer password di BIOS e password di rete, trimestralmente cambiate. Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabili dei dipendenti e degli alunni) sono ubicate in modo tale che ciascun addetto possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee.

Analisi del rischio

Dobbiamo procedere necessariamente alla valutazione di tutte le possibili minacce in termini di probabilità di occorrenza e relativo danno potendo così stimare il relativo rischio: in base a tale valore si decide se, come e quali contromisure di sicurezza adottare.

La protezione dagli attacchi informatici viene ottenuta agendo su più livelli: innanzitutto a livello fisico e materiale, ponendo server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi; anche se questo accorgimento fa parte della sicurezza normale e non della "sicurezza informatica".

Il secondo livello è normalmente quello logico che prevede l'autenticazione e l'autorizzazione di un'entità che rappresenta l'utente nel sistema. Successivamente al processo di autenticazione, le operazioni effettuate dall'utente sono tracciate e questo processo di monitoraggio delle attività è detto audit. Tutto il personale del nostro Istituto sarà a tal fine registrato come utente del sito.

Tipi di sicurezza:

1. Sicurezza passiva:

sono le tecniche e gli strumenti di tipo *difensivo*, ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

2. *Sicurezza attiva*

sono tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (riservatezza) sia dalla possibilità che un utente non autorizzato possa modificarli (integrità)

È evidente che la sicurezza passiva e quella attiva siano tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema.

Le possibili tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico, realizzando più barriere fra l'attaccante e l'obiettivo.

Le violazioni possono essere molteplici: vi possono essere tentativi non autorizzati di accesso a zone riservate, furto di identità digitale o di file riservati, utilizzo di risorse che l'utente non dovrebbe potere utilizzare ecc. L'uso della firma digitale di un documento informatico è uno strumento efficace per confermare la verifica del soggetto proprietario del documento stesso e garanzia di veridicità.

Strumenti di protezione

Antivirus

consente di proteggere il proprio computer da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC per verificare la presenza di virus e per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus correttamente configurato a tale scopo

Antispyware

software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato utilissimo per la rimozione di "file spia", gli spyware appunto, in grado di carpire informazioni riguardanti le attività on line dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.

Firewall

garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente.

Firma digitale e crittografia

La firma digitale, l'utilizzo di certificati digitali e crittografia per identificare l'autorità di certificazione, un sito, un soggetto o un software.

Nel nostro Istituto si procede all'archiviazione digitale dei documenti in formato p7m e si indica all'utente la modalità di verifica della firma del dirigente Scolastico tramite l'utilizzo della firma messa a disposzione da SIDI

Steganografia

Ha l'obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli, mentre per la crittografia è non rendere accessibili i dati nascosti a chi non conosce la chiave. La crittanalisi è l'attacco alla crittografia, che mira ad estrarre i dati cifrati senza chiave. L'obiettivo della steganalisi non è quindi quello di estrarre i dati nascosti, ma semplicemente di dimostrarne l'esistenza.

Sistema di autenticazione sofisticato

Altro sistema, più sofisticato, è quello del riconoscimento dell'utente tramite l'utilizzo dell'impronta digitale come forma di autenticazione che potrebbe essere uno strumento molto sicuro.

Sicurezza della rete Internet

Con la crescita a dismisura di internet e e del "www", le problematiche di sicurezza si sono estese anche ad essa e sul fronte tecnico le misure di protezione in rete si concretizzano nell'uso di opportuni protocolli di rete come per es. HTTPS che non fanno altro che applicare i metodi crittografici su uno o più livelli di architettura di rete modello ISO OSI.

Safer Internet

Introdotto dal parlamento Europeo nel 2005, vuole promuovere l'uso sicuro di internet soprattutto per i bambini: una rete europea di 21 linee nazionali attraverso le quali gli utenti finali possono denunciare anonimamente la presenza di contenuti illegali su internet. È indispensabile che genitori e insegnanti seguano con costanza i ragazzi nella navigazione, fornendo loro gli strumenti critici necessari per un approccio consapevole alla rete.

L' Istituto Comprensivo Certosa di Pavia adotta il piano di disaster recovery che costituisce parte integrante della continuità operativa del CAD nel rispetto delle linee guida di DigitPA e della Direttiva europea 114/2008 che regolamenta le modalità di identificazione delle infrastrutture critiche europee (ICE).

GLOSSARIO DELLE PRINCIPALI DEFINIZIONI

Nell'ambito del presente documento si intende per:

- ***Agenzia per l'Italia Digitale*** *(AGID*): istituita con la L. 134/2012 con attribuzione, tra le altre, delle competenze di DigitPA in tema di attuazione dei diritti digitali e di vigilanza sull'attuazione del CAD, con particolare riferimento, in relazione al presente documento, al rispetto delle prescrizioni dell'art. 50bis ("Continuità operativa");
- ***Agenda Digitale Europea o Digital Agenda for Europe (DAE)****:* iniziativa cardine della strategia Europa 2020 (ora Horizon 2020), che grazie a una maggiore diffusione e ad un uso più efficace delle tecnologie digitali nell'ambito della Strategia 2020 , ha l'obiettivo di stimolare l'innovazione e la crescita economica e migliorare la vita quotidiana dei cittadini e delle imprese. L'Agenda mira in particolare a: creare i presupposti per un mercato digitale unico e dinamico, che consenta di sfruttare i benefici dell'era digitale; garantire un'effettiva interoperabilità tra i prodotti e i servizi delle tecnologie dell'informazione; adottare una politica rafforzata in materia di sicurezza delle reti e delle informazioni; rendere l'accesso ad internet veloce e superveloce, garantendo la copertura universale della banda larga a velocità sempre maggiori e la promozione di reti di nuova generazione; incentivare la ricerca e l'innovazione in materia di tecnologie digitali, sfruttando il mercato unico; abolire il c.d. Digital Divide, migliorare l'alfabetizzazione, le competenze e l'inclusione nel mondo digitale; ridurre i consumi energetici, migliorare i servizi ai cittadini attraverso l'e-government delle amministrazioni, migliorare l'efficienza dei trasporti e la mobilità, migliorare l'assistenza sanitaria (rafforzare la consapevolezza dei pazienti e favorire l'inclusione dei disabili) ecc. ecc.;
- ***Agenda Digitale Italiana (ADI)****:* è l'insieme degli obiettivi e azioni che l'Italia, attraverso la Cabina di Regia istituita con la legge n. 35/2012 e l'Agenzia per l'Italia Digitale, istituita con la legge n. 134/2012, intende portare avanti per l'attuazione dei *pillar* e azioni della DAE, che comprende, fra le altre, azioni per potenziare la sicurezza dei sistemi e delle infrastrutture;
- ***Archivio****:* complesso organico dei documenti, dei fascicoli e delle serie archivistiche di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento della propria attività, che si distingue in relazione alle diverse fasi di gestione in: archivio corrente, archivio di deposito e archivio storico (come precisato dalle relative regole tecniche);
- ***Codice dell'Amministrazione Digitale*** *(CAD*): D.Lgs. n. 82/2005 e s.m.i., aggiornato alla luce del D. Lgs. n. 235/2010, dalla L. n. 135 del 7 agosto 2012 e dalla legge n.221/2012 di conversione del D. L. n. 179 del 18 ottobre 2012;

- ***Continuità Operativa Generale dell'Organizzazione***: condizione in cui, pur in presenza di un'emergenza, sono attive tutte le misure tecnico-organizzative e gestionali volte ad assicurare, al massimo possibile, le prestazioni rese dai processi critici. Le regole per la gestione, a livello generale dell'organizzazione, della continuità operativa dei processi critici in situazioni di emergenza viene definita in un apposito documento (Piano di Continuità Operativa Generale dell'Organizzazione) le cui prescrizioni si applicano alle situazioni di emergenza di rilievo generale;
- ***Continuità Operativa ICT (CO):*** la capacità di un organizzazione di adottare - per ciascun processo critico e per ciascun servizio istituzionale critico erogato in modalità ICT, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative - misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi e funzioni istituzionali. Il processo ICT è un caso tipico di processo critico;
- ***Copia dei dati e delle applicazioni (Data Mirroring)****:* un processo con cui dati ritenuti critici vengono copiati secondo precise regole e politiche di backup al fine di garantire l'integrità, la custodia e la fruibilità degli archivi, dei dati e delle applicazioni e la possibilità di renderli utilizzabili, ove fosse necessario, procedendo al ripristino degli archivi, dei dati e delle applicazioni presso un sito alternativo a quello primario;
- ***Database*****:** collezione di dati registrati e correlati fra loro;
- ***Digitalizzazione ICT:*** il richiamo ai principi del CAD che comportano la dematerializzazione, la formazione, gestione, conservazione e trasmissione dei documenti informatici, che, portando le Amministrazioni ad una razionalizzazione e informatizzazione della gestione documentale, rafforzano l'importanza di assicurare una corretta attuazione delle politiche di sicurezza e di backup e la predisposizione, gestione e manutenzione di soluzioni di CO/DR, ai sensi dell'art. 50bis del CAD;
- ***Disaster****:* l'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'organizzazione;
- ***Disaster recovery (DR*****)**: nell'ottica dell'art. 50bis del CAD, l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate;
- ***Fruibilità di un dato****:* la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;
- ***Gestione informatica dei documenti***: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle Amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;
- ***Log****:* la registrazione cronologica delle operazioni eseguite su di un sistema informatico, e quindi su archivi, per finalità quali ad es.: controllo e verifica degli accesi (access log), registro e tracciatura dei cambiamenti che le transazioni introducono in un Data-base (log di transazioni o log di base dati), analisi delle segnalazioni di errore (error log), produzione di statistiche di esercizio;
- ***Piano di Continuità Operativa Generale dell'Organizzazione***: Piano che fissa gli obiettivi da perseguire da parte dell'Organizzazione; descrive i ruoli, le responsabilità e le procedure per la gestione della Continuità Operativa Generale dell'Amministrazione, tenuto conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche. In realtà particolarmente complesse il Piano può essere solo un documento di primo livello cui vanno associati, per esempio, documenti di secondo livello, quali procedure relative a servizi/processi e/o sistemi specifici (per esempio il Piano di Continuità Operativa ICT) e finanche documenti di terzo livello (per esempio sotto forma di istruzioni di lavoro che riportano indicazioni operative specifiche);
- ***Piano di Continuità Operativa ICT (PCO)***: Documento operativo che descrive le attività finalizzate al ripristino delle funzionalità ICT, a seguito di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi classificati come "critici"; per una realtà di dimensioni limitate, soprattutto sotto il profilo ICT.
- ***Piano di Disaster Recovery (PDR/DRP):*** Documento operativo che descrive le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità delle funzioni ICT a supporto dei servizi definiti "critici", il ripristino delle stesse, entro un arco temporale predefinito, tale da rendere, il più possibile, minime le interruzioni nell'erogazione dei servizi.
- ***Piano per la Sicurezza dell'Operatore (PSO)****:* il Piano che deve identificare i beni dell'infrastruttura critica e le soluzioni in atto o in corso di implementazione per la loro protezione;
- ***Processo critico*****:** processo essenziale per l'erogazione dei servizi di natura istituzionale ovvero di quelli a loro diretto supporto e la cui interruzione, per un tempo superiore a un limite

predefinito, provoca danni non accettabili dal punto di vista organizzativo sociale, reputazionale, economico-finanziario.

- ***Risk Assessment (RA)**:* l'analisi per determinare il valore dei rischi di accadimento di un evento che possa interrompere l'erogazione di un servizio;
- ***RPO: Recovery Point Objective,* i**ndica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto.
- ***RTO: Recovery Time Objective**,* indica il tempo di ripristino del servizio: è la durata di tempo entro il quale un business process ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili;
- ***Servizi istituzionali ICT:*** la base di partenza nell'individuazione delle soluzioni di salvaguardia dei dati e delle applicazioni; sono i processi critici e i servizi istituzionali che l'ente eroga in modalità ICT o mediante l'apporto delle tecnologie ICT;
- ***Situazione di emergenza generale***: situazione nella quale si determinano le condizioni per una riduzione rilevante o per l'interruzione delle prestazioni rese dai processi critici. All'emergenza effettiva è assimilata anche l'emergenza potenziale, nella quale cioè il rischio di riduzione rilevante o di interruzione dell'operatività è elevato e imminente;
- ***Strumento di autovalutazione**:* è il tool messo a disposizione dall'Agenzia sul proprio sito - ai fini della predisposizione degli studi di fattibilità tecnica e dei PCO e PDR - per supportare le Amministrazioni nell'identificazione delle soluzioni tecnologiche idonee alla CO, avendo come base di partenza essenzialmente i "servizi" che l'ente eroga nei confronti della collettività;
- ***SPC**:* Sistema Pubblico di Connettività (artt. 73 e segg. del CAD); è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della PA, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna PA.

Il dirigente scolastico
Lorena Annovazzi

Lorena Annovazzi