Piano della continuità operativa ICT

Indice

Piano di continuità operativa ICT

L'art. 15 "Digitalizzazione e riorganizzazione" del CAD sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la digitalizzazione dei servizi.

La Pubblica Amministrazione, e quindi il nostro Istituto, ha l'obbligo di assicurare la continuità dei processi che presiedono all'erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento delle attività. L'utilizzo delle tecnologie ICT nella gestione dei dati e dei procedimenti dei singoli enti rende necessario adottare tutte le iniziative tese a salvaguardare l'integrità, la disponibilità e la continuità nella fruibilità dei dati. Le Pubbliche Amministrazioni devono predisporre appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili per fornire i servizi e il ritorno alla normale operatività.

Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

• il Dirigente Scolastico dott.ssa Elena Venturini;
• il DSGA dott. Felicia Della Coletta;
• il responsabile della continuità operativa ICT, così come indicato nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011, individuato nel responsabile dei sistemi informatici dell'Istituto;
• il personale amministrativo dell'Istituto (la segreteria);
• la comunità di riferimento territoriale e sociale (famiglie e imprese) dell'Amministrazione;
• le organizzazioni, associazioni e/o istituzioni che interagiscono con l'Amministrazione in modalità informatiche.

Piano dei Sistemi

Il nostro Istituto deve rispondere in maniera efficiente ad una situazione di emergenza ipotizzando e analizzando:

1. i possibili livelli di disastro

2. le criticità dei sistemi/applicazioni.

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

• **Critici:** Le relative funzioni non possono essere eseguite in altro modo se il funzionamento del sistema viene interrotto. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa.

• **Vitali:** Le relative 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. Nonostante ciò 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 relative funzioni possono rimanere interrotte per un lungo periodo di tempo, e lo sforzo di ripartenza quando il sistema viene ripristinato è limitato.

Punti critici e vitali dell'Istituto

Nel nostro Istituto identifichiamo i punti critici e vitali:

• Il server CENTOS che gestisce i dati utilizzati dalla segreteria, composto da un server CENTOS uno WINDOWS 2000 (virtuali) situati nella segreteria, protetto in un armadio rack chiuso a chiave.

• Il firewall, situato nello stesso armadio rack del server, che permette di proteggere gli accessi indesiderati possibili minacce.

• I dispositivi di backup individuati dall'Istituto in un disco di rete.

• il sito web e i sistemi di iscrizione online.

• le classi virtuali e gli account GSuite.

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

Prevenzione dei danni

Si illustrano alcune precauzioni e indicazioni di massima adottate dal nostro Istituto per prepararci ad un evento critico o vitale e limitare o prevenire i danni:

• Backup dei dati. È la condizione minima indispensabile: tutti i dati importanti vanno salvati su altri dispositivi. Lo strumento che ospita il backup dovrebbe essere custodito in un luogo ed edificio fisicamente distante. Vanno svolti regolarmente test di ripristino e di verifica dell'integrità dei dati, e deve essere eseguito un monitoraggio quotidiano dei dati salvati.

• Protezione dei sistemi da accessi indesiderati o furti. Utilizzo di rack protetti da chiusure e chiavi di sicurezza per rendere inaccessibile il server della segreteria.

• 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.

• UPS. Unità di energia supplementare per ovviare a situazioni di mancanza di energia elettrica per permettere di portare in sicurezza i dati dell'Istituto e al limite chiudere il sistema.

• monitoraggio del firewall del server.

• monitoraggio e aggiornamento del firewall del sito web.

Tecniche di Disaster Recovery

Sistemi e dati considerati importanti vengono ridondati in un sito secondario per far sì che, in caso di evento critico (terremoto, inondazione, incendio, attacco hacker, ecc...) 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. Il nostro Istituto utilizza una tecnica di ridondanza con queste modalità, spostando sul CLOUD (account su server Google) i dati che sono il risultato dalla tecnica di backup impostata. Con questa modalità anche nel caso di disastro i dati non essendo "in loco" sono sempre disponibili al ripristino.

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 a:

- assicurare l'accesso solo ad utenti registrati (autenticazione),
- permettere la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (permessi),
- garantire 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 è un problema sempre più sentito in ambito tecnico-informatico per via della sempre più spinta digitalizzazione della società e dei servizi e della parallela diffusione e specializzazione degli *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. Risulta evidente che per capire le strategie migliori di sicurezza informatica sia necessario entrare nella mentalità dell'hacker e poterne prevedere ed ostacolare le mosse.

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: eventi inaspettati come gli attacchi Hacking fatti tramite la rete internet. Si tratta di utenti che si intrufolano abusivamente all'interno del sistema informatico riuscendo ad accedere e a gestire risorse e dati senza avere i requisiti richiesti tramite software costruiti da loro stessi. Oppure l'accesso al sistema da parte di utenti non autorizzati tramite le stesse apparecchiature dell'Istituto.
- Eventi accidentali: eventi causati incidentalmente dall'utente stesso, tipo uso difforme dalle norme del sistema, guasti imprevisti, ecc...

Alcune indicazioni attuate dal nostro Istituto per garantire la sicurezza e l'integrità dei dati:

- Il server di ARGO 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 di ARGO è garantita da una procedura di backup che avviene giornalmente in orario notturno, attraverso un'unità di backup di rete.
- Tutti i PC della rete amministrativa vengono protetti da password per impedire al

personale non autorizzato l'accesso alla rete.
- Il sito web è protetto da un firewall che monitora e blocca tentativi di accesso non autorizzati al backend. Inoltre la visibilità del sito è consentita solo ad utenti italiani, mentre è bloccata ad ip esteri.

Tipi di sicurezza

Tipologie di sicurezza attuabili:

- 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.
- 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 tutela di un sistema.
Il nostro Istituto utilizza sia meccanismi di sicurezza passiva (rack chiusi a chiave) che attiva (firewall).

Altri strumenti di protezione applicati nel nostro Istituto

- 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 suo migliore utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC. Inoltre è buona pratica che l'utente controlli tutti i file ricevuti o 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 online dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.

- Firewall: garantisce un efficace sistema di controllo degli accessi verificando tutto il traffico che attraversa il pc. 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, e 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 del software Infocert. Aprire un file p7m (se pdf) con Adobe Reader è possibile ma non offre la garanzia di verifica dell'identità di appartenenza.

Gestione e aggiornamento del piano di continuità operativa

Il piano della continuità operativa ICT non è un documento statico e, pertanto, è necessario pianificare, sia le modalità di verifica dei contenuti (test), sia le modalità di revisione e aggiornamento. Per quanto attiene ai test, ce ne sono di diverse tipologie.
E' buona norma verificare l'effettiva disponibilità di tutte le precauzione e gli accorgimenti attuati in caso di evento critico (nomina del responsabile della continuità operativa, nomina Comitato di crisi ICT, gestione delle reperibilità, disponibilità e funzionamento degli impianti del sito secondario, disponibilità delle risorse elaborative e di rete ecc.).
Il test cosiddetto "walkthrough" si svolge con una simulazione (cioè, senza attivazione fisica dei sistemi) eseguita da tutto il personale coinvolto nel Piano di Continuità Operativa ICT.
Il test degli impianti e delle risorse verifica l'effettiva attivazione delle risorse fisiche a fronte della simulazione di un'emergenza. Un test di questo tipo richiede una attenta predisposizione e un sensibile impegno per il personale, ma garantisce la reale verifica della soluzione di continuità del Piano di Continuità Operativa ICT.