UNIONE EUROPEA

FONDI STRUTTURALI EUROPEI pon 2014-2020

AICA Test Center ECDL Sede Accreditata di Esami

Ministero dell'Istruzione, dell'Università e della Ricerca

ISTITUTO COMPRENSIVO STATALE
"San GIUSEPPE CALASANZIO"
Piazza Axum, 5 – Milano – 20151 Tel. 0288444602 Fax 0288452404
CODICE MECCANOGRAFICO: MIIC8C500A CODICE FISCALE: 80128410158
E-mail: miic8c500a@istruzione.it PEC: miic8c500a@pec.istruzione.it Sito: http://www.istitutocalasanzio.it/

Milano 14/11/2017

Piano della continuità operativa ICT

Procedure di disaster recovery

A.S. 2017/2018

Indice

REGISTRO DELLE MODIFICHE		
Edizione	Sintesi della modifica	Data
1.0	Prima stesura	

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 alla erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese.
L'utilizzo delle tecnologie ICT nella gestione dei dati e dei procedimenti dei singoli enti, che rende necessario adottare tutte le iniziative tese a salvaguardare l'integrità, la disponibilità, 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 a fornire i servizi e il ritorno alla normale operatività.

Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

- il Dirigente Scolastico Prof.ssa Luisa Martiniello;
- il DSGA Dott.ssa Maria Cipriano;
- 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 informativi dell'Istituto;
- il personale amministrativo dell'Istituto (la segreteria);
- la comunità di riferimento territoriale e sociale (famiglie e imprese) dell'Amministrazione;
- le organizzazioni 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 analizzando:

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 relative 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 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. Benché queste funzioni possano essere eseguite manualmente, 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 si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Punti critici e vitali dell'Istituto

Nel nostro istituto identifichiamo i punti critici e vitali:

- Il server che gestisce i dati utilizzati dalla segreteria, composto da un server DELL con il Sistema Operativo Microsoft Windows Server 2012 situato nella stanza dei pannelli elettrici.
- Il firewall, situato nella stessa stanza del server in un armadio rack, che permette di proteggere gli accessi indesiderati e possibili minacce.
- I dispositivi di backup individuati dall'Istituto in un disco portatile USB conservato in cassaforte nella stanza della DSGA.

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

Prevenzione dei danni

Si illustrano alcune precauzioni e indicazioni di massima adottate dal nostro Istituto per prepararci ad un disastro e limitarne o prevenirne i danni:

- Backup dei dati. È la condizione minima indispensabile: tutti i dati importanti vanno salvati su altri dispositivi. Il mezzo su cui viene mantenuto il backup dovrebbe essere custodito in un luogo ed edificio 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.
- 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.

Tecniche di Disaster Recovery

Sistemi e dati considerati importanti vengono ridondati in un sito secondario 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.
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 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. Risulta evidente che per capire le strategie migliori di sicurezza informatica sia necessario entrare nella mentalità dell'attaccante per poterne prevedere ed ostacolarne 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:

1. *Eventi indesiderati*: qui ci sono quelli per lo più inaspettati come gli attacchi Hacking che vengono fatti tramite la rete internet, da parte di utenti chiamati appunto dalla società cracker 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. Invece l'accesso a sistemi da parte di utenti non autorizzati a differenza di un attacco cracker viene usata la macchina e non la rete.
2. *Eventi accidentali ovvero causati accidentalmente dall'utente stesso, tipo*: uso difforme dal consigliato di un qualche sistema, guasti imprevisti, ecc…

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

1. Il server di AXIOS 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.
2. L'integrità dei dati sul server amministrativo di AXIOS è garantita da una procedura di backup che avviene giornalmente in orario notturno, attraverso un backup in cloud.
3. Tutti i PC della rete amministrativa vengono protetti da password per impedire al personale non autorizzato l'accesso alla rete.

Tipi di sicurezza

Tipologie di sicurezza attuabili:

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.
Il nostro Istituto utilizza meccanismi di sicurezza passiva (rack chiusi a chiave) e attiva (firewall) atte a incrementare il livello di sicurezza.

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 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, 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, sono possibili varie modalità di test:

- Una semplice verifica dell'effettiva disponibilità di tutto quanto si renderebbe necessario in caso di emergenza (nomina responsabile della continuità operativa, no mina Comitato di crisi ICT, gestione delle reperibilità, disponibilità e funzionamento degli impianti del sito secondario, disponibilità delle risorse elaborative e di rete, ecc.).
- Un test cosiddetto "walkthrough": questo tipo di test si svolge con una simulazione (cioè, senza attivazione fisica dei sistemi) fatta da tutto il personale da coinvolgere previsto dal piano della continuità operativa ICT.
- Test degli impianti e delle risorse: in questo caso non solo le procedure, ma anche l'effettiva attivazione delle risorse fisiche e IT viene verificata, sempre 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 della continuità operativa ICT.