LICEO ARTISTICO A. FRATTINI

Ministero dell'Istruzione, dell'Università e della Ricerca
LICEO ARTISTICO "A. FRATTINI"
Via Valverde, 2 - 21100 Varese
tel: 0332820670
e-mail: vasl040006@istruzione.it vasl040006@pec.istruzione.it
COD.MIN.:VASL040006
C.F.:80016900120

Piano di continuità operativa e Disaster Recovery

Indice

1. Piano di continuità
2. Destinatari
3. Piano dei sistemi
4. Punti critici e vitali
5. Prevenzione dei danni
6. Tecniche di Disaster Recovery
7. Strumenti di protezione applicati
8. Gestione e aggiornamento del piano di continuità operativa

1. Piano di continuità

In base all'art. 50-bis del Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione Digitale le pubbliche amministrazioni definiscono:
a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;
b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

2. Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

- il Dirigente Scolastico;
- il DSGA;
- il responsabile della continuità operativa ICT, 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.

3. Piano dei Sistemi

Il Liceo A. Frattini 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.

4. Punti critici e vitali dell'Istituto

Nel nostro istituto identifichiamo i punti critici e vitali:

- Il server fornito da Spaggiari/Infoschool denominato Green Server, che gestisce i dati utilizzati dal servizio di segreteria digitale, situato nell'Ufficio del DSGA, sempre presidiato o chiuso a chiave nei momenti in cui non è presente personale;
- Il firewall situato nell'armadio rack chiuso del locale fotocopiatore, finalizzato alla prevenzione delle intrusioni informatiche;
- Il disco di rete (NAS) situato nell'Ufficio del DSGA per la memorizzazione dei dati degli utenti amministrativi;
- un secondo NAS con funzioni di backup del primo NAS collocato nell'Ufficio del dirigente scolastico, sempre presidiato o in alternativa chiuso a chiave.

I PC in uso al personale amministrativo, al dirigente e quelli dell'area didattica vengono classificati a criticità delicata in considerazione del fatto che pur con disagio le stesse funzioni possono essere svolte con altri computer.

5. 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, tramite i dischi di rete indicati al capitolo 4. Il backup dei dati del servizio di segreteria digitale è effettuato dal fornitore del servizio
• Protezione dei sistemi da accessi indesiderati o furti. Utilizzo di rack protetti da chiusure e chiavi di sicurezza per renderli inaccessibili
• Impianto elettrico a norma, che offra inoltre sufficiente protezione da fulmini, con gruppi di continuità che suppliscano a brevi interruzioni di elettricità

6. Tecniche di Disaster Recovery

L'Istituto non dispone di un centro di elaborazione dati e pertanto le tecniche si riferiscono alle sole procedure informatiche utilizzate.
I dati considerati importanti vengono ridondati sul disco di rete di backup e/o sul servizio di segreteria digitale, gestito in cloud dal fornitore del servizio.
Vengono effettuate copie di ripristino dei computer utilizzati dal personale amministrativo.

7. Strumenti di protezione applicati

Antivirus: consente di proteggere il proprio computer da software dannosi conosciuti come virus, con funzione di aggiornamento automatico
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.
Politiche di aggiornamento: i sistemi operativi sono configurati in modo da ricevere automaticamente gli aggiornamenti di sicurezza resi disponibili dal produttore

8. Gestione e aggiornamento del piano di continuità operativa

Il piano viene sottoposto a revisione con cadenza biennale e ogni volta che si verifichino cambiamenti significativi delle strutture implicate