I.T.C.G.T. LICEO G.B. FALCONE ACRI
VIA PADRE GIACINTO DA BELMONTE, 35 - 87041 - ACRI (CS)
TELEFONI: 0984.95.35.33 - 18.61.922 - FAX 0984.91.06.29 - II SEDE: 0984.95.35.52
www.itcgtacri.gov.it - EMAIL: cstd07000t@istruzione.it - COD.FISC. 85000410788 - COD.MIN. CSTD07000T

Acri, 14.11.2016

Prot. n. 5575/07-05

Sig. Giuseppe Milordo
Assistente tecnico
Sig. Angelo Conforti
Assistente Tecnico

e p.c. Dott.ssa Marisa Paese
Responsabile del trattamento dei dati
Al Personale Amministr. e Tecnico

Rispettive sedi

OGGETTO: **PIANO DI BACK-UP, DISASTER-RECOVERY, DI CONTINUITÀ, NONCHÉ MISURE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI**

La S.V., è nominata quale incaricato delle operazioni periodiche di salvataggio dei dati contenuti nel server centrale dell'Istituto T.C.G.T. e della gestione tecnica delle politiche di sicurezza connesse alle password di accesso al server medesimo. In caso di assenza, sarà sostituita dal Sig. Angelo Conforti.

Con la presente viene trasmesso il Piano di cui all'oggetto, cui sarà necessario attenersi. La prego, comunque, di comunicare alla scrivente ogni suggerimento che possa essere utile e necessario al corretto svolgimento dell'attività connessa.

IL DIRIGENTE SCOLASTICO
Giuseppe Giudice

Firmato digitalmente da

GIUSEPPE GIUDICE

O = non presente
C = IT
Data e ora della firma: 01/12/2016 11:42:55

Piano di back-up, disaster – recovery, di continuità

Analisi delle conseguenze dell'eventuale perdita di dati

Va premesso che i dati trattati dalla scuola in forma elettronica sono moderatamente importanti in se stessi; non è un Ospedale o un centro paghe o un ufficio anagrafe. Anche il grado di urgenza con cui all'Interessato possono servire i documenti necessariamente prodotti tramite computer è decisamente molto più basso rispetto a questi esempi.

Infine va osservato che i dati trattati dalla scuola in forma elettronica non sono, per ora, mai degli originali, bensì servono:

- per produrre documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale
- per elaborare dati provenienti da documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale
- per produrre comunicazioni ad altri Enti (Tesoro, Ministero della Funzione Pubblica, MIUR, ecc.) e cessa la necessità di conservarli in forma elettronica non appena la comunicazione ha avuto effetto.
- per ricevere comunicazioni provenienti dall'esterno, delle quali di norma si fa immediatamente la copia cartacea, che viene poi conservata e che è l'unica ad avere valore legale. L'unica eccezione sono determinati allegati che non si ritiene utile stampare e determinati programmi che non è, ovviamente, possibile stampare. In entrambi i casi non si tratta mai di dati personali, né di software che tratti dati personali.

Quando si arriverà a implementare la firma elettronica e l'esistenza di documenti elettronici che di per sé costituiscano "originali" la situazione potrà cambiare.

Il programma per il protocollo

Poiché esiste un periodico back-up, le analisi che seguono riguardano la perdita di dati non ancora salvati (quindi una settimana al massimo, circa).

Il dato elettronico la cui perdita che creerebbe più problemi è il protocollo informatizzato [questa frase va mantenuta se la scuola ha tale software], in quanto viene stampato con un certo ritardo rispetto alle registrazioni, quindi la perdita delle predette registrazioni creerebbe una seria difficoltà, in gran parte, però, rimediabile perché esistono comunque sempre i documenti cartacei con il timbro di protocollo e il relativo numero attribuito. Tuttavia sarebbe estremamente laborioso ritrovare tutti i documenti cartacei necessari a ricostruire la numerazione perduta, considerato che nel frattempo tali documenti possono essere stati archiviati in mezzo a centinaia di fascicoli e a migliaia di carte.

Da un altro punto di vista, la registrazione dell'avvenuto ingresso di un documento, con relativo numero attribuito, data e oggetto, costituisce sicuramente il dato personale che più frequentemente un Interessato potrebbe chiedere se esiste e di conoscerlo. Ciò perché in molti casi può essere per lui di vitale importanza provare di aver consegnato un certo documento o addirittura provare di averlo prodotto entro una certa scadenza temporale. In tali casi, però, è possibile trovare nel fascicolo personale o in un numero limitato di fascicoli il documento in oggetto, con relativo timbro datario e numero progressivo.

In tutti gli altri casi l'eventuale perdita di dati creerebbe un po' di lavoro in più per reinserirli copiandoli dai rispettivi originali cartacei, ma niente più..

La situazione cambierà quando eventualmente si passerà ad un protocollo esclusivamente elettronico, senza copia cartacea.

Altri dati la cui perdita creerebbe problemi

Il programma gestione finanziaria, che consente di emettere mandati e riversali è sicuramente quello che potrebbe soffrire non tanto della perdita dei dati quanto del breve blocco operativo conseguente alla necessità di reinserire i dati perduti, dei quali comunque esistono i documenti cartacei facilmente rintracciabili.

Anche il programma stipendi, il programma assenze e il programma alunni creerebbero notevoli perdite di tempo per reintegrare i dati, tuttavia la perdita non sarebbe irreversibile né di per sé grave.

Conseguenze di un blocco di computer di breve durata (1 giorno circa)

Nel caso di blocco :

- di un solo computer isolato (= non in rete) che fosse l'unico ad aver memorizzati certi dati e certi programmi,

- del server di rete in cui siano memorizzati tutti i dati e i programmi

si ritiene che il danno sarebbe minimo perché rarissimamente la scuola opera con scadenze in tempo reale, quindi l'attesa di un giorno non creerebbe problemi a meno che non si fosse atteso l'ultimissimo momento per un adempimento con scadenza tassativa.
Nel caso del protocollo, per un giorno si potrebbe procedere con annotazione manuale e successiva copiatura delle registrazioni quando il computer riprendesse a funzionare.
Nel caso che tale guasto riguardasse un terminale di rete (client), se i dati e i programmi di lavorazione dei dati sono memorizzati nel server, passando a un altro terminale si risolve il problema senza inconvenienti.

Blocco del computer principale (o unico) collegato a Internet

Per quanto riguarda le comunicazioni di posta elettronica o fatte tramite internet , utilizzando il computer come terminale remoto, va precisato che raramente ci sono messaggi di posta elettronica che non possano attendere un giorno o comunicazioni che non possano ugualmente essere procrastinate. Va tuttavia riconosciuto che sarebbe buona norma avere, comunque, almeno due computers in grado di compiere tali operazioni. Ciò significa che il computer "di riserva":

- deve e essere collegabile a internet di fatto o potenzialmente in pochi minuti (quindi dovrebbe avere già installato il driver(= programma che rende utilizzabile uno specifico dispositivo) del modem e il browser (Internet explorer, netscape, altri …).
- Deve avere già caricati eventuali programmi che sono necessari per emulare un terminale remoto o per comunicare con determinati enti.

Conseguenze di un blocco di computer di media-lunga durata (oltre 1 giorno)

Nel caso di blocco prolungato :

a) di un solo computer isolato (= non in rete) che fosse l'unico ad aver memorizzati certi dati e certi programmi,
b) del server di rete in cui siano memorizzati tutti i dati e i programmi
c) dell'intero sistema

si ritiene che il danno diventerebbe serio, grave dopo circa 3-4 giorni, gravissimo dopo una settimana.
Invece, nel caso che tale guasto riguardasse un terminale di rete (client), se i dati e i programmi di lavorazione dei dati sono memorizzati nel server, passando a un altro terminale si risolve il problema senza inconvenienti.
Per intervenire nei casi a), b), c) è normalmente sufficiente una procedura di "Disaster Recovery" (= Recupero di un disastro, che ha provocato la messa fuori uso completa e prolungata, a volte irreversibile, del sistema informatico o di sue parti vitali a causa di un evento). Se essa si conclude in uno, massimo due giorni, è accettabile, mentre non sembra indispensabile un piano di continuità operativa che riduca necessariamente i tempi di sosta sotto uno-due giorni. I costi economici sarebbero infinitamente superiori ai costi dovuti al blocco temporaneo.

Procedure di Back-up. Analisi della situazione.

Attualmente il back-up viene eseguito con procedure Argo e Sissi, su Server dotato di n° 2 Hard Disk con sistema a doppia scrittura e copia di sicurezza su pen-drive USB.

Procedure di Back-up.

1) In applicazione del principio che le copie di back-up non devono essere esposte al rischio di essere rovinate da un evento che contemporaneamente distrugga i computers, custodiamo le copie di back-up dei dati nonché i dischi originali dei programmi in un "armadio di sicurezza" ignifugo, resistente all'effrazione, collocato in stanza diversa da quelle in cui sono i computers.

2) Contro il rischio di back-up malriuscito, abbiamo provveduto [oppure: abbiamo allo studio] all'acquisto di un programma in grado di testare la qualità della copia di back-up eseguita e di gestirla in modo efficiente.
Inoltre, come seconda misura, abbiamo due serie di dischi per lo stesso salvataggio. Una serie viene usata la prima settimana e l'altra nella settimana seguente, e così via alternandole. In questo modo, nel caso estremo di guasto del supporto o di cattiva esecuzione del back-up, quando ci presentasse l'effettiva necessità del ripristino dei dati e non riuscisse con la serie di dischi più recente, ci sarebbe pur sempre l'altra serie, più vecchia di alcuni giorni e quindi non in grado di ripristinare tutto, però in grado di ripristinare almeno grandissima parte dei dati.

3) Per evitare errori umani, procedurali, organizzativi o delle macchine, verranno periodicamente eseguiti test di ripristino (ovviamente dopo aver salvato i dati correnti oppure , preferibilmente, su un computer diverso da quello dove sono i dati correnti).

4) Periodicità: si ritiene che la periodicità di 15 giorni per il back-up sia al momento adeguata. Se e quando si arrivasse a veri e propri "documenti originali elettronici", andrebbe portata a frequenza di 7 giorni per tali documenti.

5) Quali dati salvare? I dati da salvare riguardano:

- Alunni, Bilancio, Personale ⟶ Programma SISSI
- Protocollo, Alunni, Personale, Emolumenti-Stipendi ⟶ Programma ARGO

Nello specifico i dati possono essere riassunti nella seguente tabella:

SALVATAGGIO		**CRITERI INDIVIDUATI PER IL SALVATAGGIO**	**UBICAZIONE DI CONSERVAZIONE DELLE COPIE**	**STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO**
STRUTTURA	**DATI SENSIBILI O GIUDIZIARI CONTENUTI**			
Dirigente Scolastico	Protocollo riservato **ARGO**	Salvataggio dati ogni 15 gg	Locale sito in SEDE, con serratura con chiavi distribuite fra i soli autorizzati	Responsabile pro tempore del servizio
Ufficio D.S.G.A.	**ARGO** **SISSI** Dati riguardanti la posizione stipendiale del personale	Salvataggio dati ogni 15 gg	Locale sito in SEDE, con serratura con chiavi distribuite fra i soli autorizzati	Responsabile pro tempore del servizio
Ufficio Personale	**ARGO** **SISSI** - Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati	Salvataggio dati ogni 15 gg	Locale sito in SEDE, con serratura con chiavi distribuite fra i soli autorizzati	Responsabile pro tempore del servizio.
Ufficio Contabilità	**ARGO** **SISSI** - dati inerenti imprese interessate ad attività negoziali	Salvataggio dati ogni 15 gg	Locale sito in SEDE, con serratura con chiavi distribuite fra i soli autorizzati.	Responsabile pro tempore del servizio
Ufficio Didattico	**ARGO** **SISSI** - Dati sensibili riguardanti gli Alunni	Salvataggio dati ogni 15 gg	Locale sito in SEDE, con serratura con chiavi distribuite fra i soli autorizzati.	Responsabile pro tempore del servizio

Per quanto riguarda i files di testo o prodotti con altri programmi standard (esempio: excell, access, ecc.) non contenenti dati sensibili, ogni utilizzatore ha avuto l'istruzione di salvare tali elaborati personali in un'unica cartella (directory) in modo da poter salvare in blocco tutti i suoi files. Sono state anche individuate con chiarezza le directory di uso comune o riservate, in modo da avere una lista sempre aggiornata delle directory di cui fare il back-up.

6) Anche sulla base del predetto censimento, viene istituito un "registro dei back-up" in cui sono elencate le directory da salvare, le periodicità, il responsabile di ciascuna operazione. Ad ogni back-up il responsabile dovrà indicare la data e controfirmare.

7) Sono state impartite precise disposizioni riguardo a tutte le procedure di back-up. Ogni mese il Titolare o suo delegato monitorerà le operazioni di back-up per verificare l'effettiva applicazione delle istruzioni date.

Procedure di "Disaster Recovery"
Nell'ipotesi che un evento distrugga o renda indisponibili tutti i computers, è stato fatto un accordo informale con un negozio perché affitti immediatamente alla scuola un computer e relative periferiche necessarie, per il tempo in cui ci si organizzerà per l'acquisizione di altri computers.
Tale computer sarà fornito con installato un sistema operativo compatibile con il software in uso alla scuola.
Nell'armadio di sicurezza sono conservati i dischi di back-up e di tutti i programmi necessari al funzionamento, in modo da poterli reinstallare. Un assistente amministrativo (o un tecnico) scriveranno in un registro da custodire nell'armadio di sicurezza, l'elenco dei programmi da caricare, l'ordine di caricamento, i particolari settaggi necessari per implementare il software (parametri e altro da configurare, ecc.), l'elenco e l'ordine di caricamento dei files di back-up.

Piano di continuità
Si sta anche esaminando la possibilità economica di acquisire un computer in tutto compatibile con il software di elaborazione dei dati usato dalla segreteria e di collocarlo in altra area della scuola, tale che sia estremamente improbabile che il medesimo evento possa rendere indisponibili contemporaneamente sia i computers della presidenza e segreteria, sia questo computer di riserva. Nel frattempo sarebbe utilizzato per attività didattiche o personali dei docenti. In tale computer sarebbero già pre-caricati i programmi e le directory utilizzate in segreteria , ma naturalmente senza i dati. In tal caso, nel tempo tecnico del ripristino dati dai dischi di back-up il sistema informativo potrebbe riprendere a funzionare dopo una o due ore, il che sarebbe in pratica un piano di continuità operativa , data l'esiguità dell'interruzione.
Sarà anche studiata la possibilità di ricorrere a strumenti di mirroring (= rispecchiamento, cioè copia perfetta del disco fisso) del disco fisso, tuttavia il costo sembra sconsigliarne l'adozione, considerato il bilancio costi-benefici e le finanze dell'Istituto. Saranno presi in considerazione anche sistemi più sofisticati come server di elevata qualità muniti di sistema raid (= doppia registrazione contemporanea su due dischi fissi, in modo che alla rottura di uno resti disponibile l'altro), ma al momento l'elevato costo sembra sconsigliarne l'adozione.
I programmi originali di tutto il software necessario saranno collocati nell'armadio di sicurezza di cui si è accennato, in modo che siano sempre disponibili e che l'evento disastroso abbia minime possibilità di distruggerli.

Prove di ripristino dei dati
Per evitare errori umani, procedurali, organizzativi o delle macchine, verranno periodicamente eseguiti test di ripristino (ovviamente dopo aver salvato i dati correnti oppure , preferibilmente, su un computer diverso da quello dove sono i dati correnti). Per ragioni di disponibilità di tempo, considerato che la scuola è oberata di lavoro nei mesi di settembre ed ottobre per l'inizio dell'anno scolastico e che tali mesi dovranno essere prioritariamente dedicati alla conclusione della formazione degli incaricati, soltanto nel mese di novembre 2004 è ipotizzabile di poter e3seguire i test di ripristino.
Per non avere problemi, anche in vista dell'implementazione di misure di disaster recovery e di un piano di continuità, il test verrà eseguito su un computer diverso da quelli dove risiedono gli archivi elettronici da ripristinare. Nell'occasione si farà quindi anche una prova di disaster recovery, caricando prima i programmi che servono per gestire i dati e successivamente facendo il test di ripristino.
Alla fine della prova i dati verranno cancellati, ma non i programmi (sempre che le licenze d'uso lo consentano) in modo che quel computer sia già predisposto per il disaster recovery.
Alle prove sarà presente un tecnico informatico per dare utili consigli e sovrintendere all'esecuzione. Saranno presenti tutti gli Incaricati che hanno avuto l'istruzione di realizzare il back-up periodico di un archivio elettronico, allo scopo anche che comprendano meglio a cosa serve e siano più motivati psicologicamente.