

Sicurezza Servizi Online Mediasoft

GESTIONALE CGWEB

Versione 1.0.0 del 20 dicembre 2017

Registro delle versioni

Versione	Data	Modifiche apportate	Osservazioni
1.0.0	20-12-2017	Prima stesura del documento	

La versione più recente di questo manuale è scaricabile dalla sezione protezione dati personali - DL 196/2003

Indice

Tavola dei contenuti

Indice.....	2
Storia.....	3
Note Tecniche.....	3
Sicurezza e protezione dei dati e procedure.....	3
Trasparenza.....	3
Politiche di sicurezza.....	4
Criteri e modalità di ripristino della disponibilità dei dati.....	4
Protezione dei dati.....	6
Qualità del servizio.....	7
Infrastruttura.....	7
Personale tecnico.....	7
Manutenzione programmata.....	7
Sistemi di alimentazione.....	7
Sistemi di condizionamento e controllo della temperatura.....	8
Prevenzione incendi.....	8
Contatti.....	9
Responsabile del trattamento.....	9
Dati Società.....	9

Storia

Mediasoft, azienda presente da più di venti anni nella scuola per la produzione di software e servizi, dal 2000 ha elaborato programmi in versione web. Il progetto dei Servizi Online, a partire dal 2001, si è sviluppato in modo da permettere la digitalizzazione e la gestione in rete delle Graduatorie, Supplenze, Foglio Chiamata Supplenti, TFR, Gestione ANAC e di tutte le Attività delle Segreterie Scolastiche.

Note Tecniche

Le procedure dei Servizi Online in SaaS (Software as a Service) sfruttano le potenzialità della rete (Internet) e consentono all'utente o a più utenti contemporaneamente l'accesso ai dati e alle procedure da qualunque postazione o sede (succursale, plesso, sede distaccata) senza necessità di costose dotazioni tecniche).

Consentono inoltre telelavoro e assistenza telematica.

L'utilizzo dei programmi è riservato agli utenti che accedono con credenziali e autorizzazioni personalizzate per garantire la sicurezza e la trasparenza dei dati.

Manutenzione e aggiornamento dei programmi vengono effettuati in tempo reale presso i server del datacenter Mediasoft che diviene garante della sicurezza dei dati.

Aggiornamenti, News e Aiuti sono in linea sul sito.

Sicurezza e protezione dei dati e procedure

Le politiche di Sicurezza analizzate in questo documento mirano a prevenire le diverse situazioni di criticità e a pianificare e mettere in atto tutti gli interventi necessari per assicurare continuità operativa agli utenti e garantire la sicurezza e la privacy dei dati, come da Circ. AGID 2/2017.

Trasparenza

Il presente documento è disponibile e scaricabile on line sul sito dei Servizi MSW, oltre che conservato presso la sede Mediasoft di Pavullo nel Frignano - Modena.

Politiche di sicurezza

Le politiche di sicurezza rispettano i requisiti minimi della Circolare AGID 2/2017.

Criteria e modalità di ripristino della disponibilità dei dati

Estratto dal Manuale procedure interne Mediasoft

Sezione 6 – Criteri e modalità di ripristino della disponibilità dei dati

Tabella 6.1 – Criteri e procedure di salvataggio e ripristino delle banche dati

- **B003 – CGWEB on line, Archivi Gestionale Web**
 - **Salvataggio/ripristino**
Server con archivi duplicati in mirror raid. Salvataggio giornaliero (Dump) su area appoggio. Estrazione e copia giornaliera su supporto rimovibile (DVD/HD) che verrà conservato in cassaforte a cura del Responsabile del trattamento. Per il ripristino deve essere utilizzata la procedura apposita a cura dei responsabili del trattamento.
 - **Pianificazione delle prove di ripristino**
Le verifiche di lettura dei files di backup vengono effettuate entro 12 ore dalla procedura di copia. La prova di ripristino e' effettuata settimanalmente sul server adibito a recovery ogni domenica sulle copie del sabato.
 - **Incaricato alle copie**
Responsabile del trattamento.
 - **Luogo di custodia delle copie removibili**
Cassaforte. Chiavi custodite dal responsabile del trattamento.
- **B004 – SCUOLA on line, Archivi Gestionale Scuole e enti pubblici**
 - **Salvataggio/ripristino**
Server con archivi duplicati in mirror raid. Salvataggio giornaliero (Dump) su area appoggio. Estrazione e copia giornaliera su supporto rimovibile (DVD/HD) che verrà conservato a cura del Responsabile del trattamento. Per il ripristino deve essere utilizzata la procedura apposita a cura dei responsabili del trattamento.
 - **Pianificazione delle prove di ripristino**
Le verifiche di lettura dei files di backup vengono effettuate entro 12 ore dalla procedura di copia. La prova di ripristino e' effettuata settimanalmente sul server adibito a recovery ogni domenica sulle copie del sabato
 - **Incaricato alle copie**
Responsabile del trattamento
 - **Luogo di custodia delle copie removibili**
Cassaforte. Chiavi custodite dal responsabile del trattamento

I supporti delle copie criptate sono conservati nei locali server fino a verifiche di lettura dei files di backup (entro max 12 ore) e successivamente archiviati in cassaforte.

I supporti delle copie criptate del sabato sono conservati nei locali server fino a completa simulazione di ripristino nel server adibito a recovery (max 24 ore) e successivamente archiviati in cassaforte.

Le misure adottate dal Responsabile garantiscono il ripristino di qualunque banca dati oggetto di trattamento entro 12/24 ore dal verificarsi dell'evento.

Il ripristino di dati oggetto del trattamento deve essere eseguito esclusivamente dai Responsabili del trattamento.

Durante il ripristino delle copie devono essere adottate le stesse misure di sicurezza che si applicano ai trattamenti.

I protocolli dettagliati relativi alle procedure di copia, verifica e ripristino sono indicati nei documenti COPIE_01 e RECOVERY_01 che sono classificati riservati e, per motivi di sicurezza, non vengono forniti insieme al presente documento.

Protezione dei dati

La sicurezza fisica del datacenter è garantita da:

- Allarme antiintrusione.
- Videosorveglianza.
- Porte antisfondamento.
- Presenza di personale.

La sicurezza dei dati è garantita da:

- Firewall esterni che prevengono le intrusioni non autorizzate al sistema.
- Firewall interni che permettono l'accesso ai server contenenti dati e applicativi soltanto al personale autorizzato.
- Criptatura dei dati sensibili.
- Regolare analisi dei log dei server per identificare anomalie.
- Monitoraggio delle attività di rete per identificare anomalie.

Qualità del servizio

Per assicurare la continuità del servizio, i servizi online sono accessibili su tre diversi server, ognuno collegato a internet con una linea fornita da un gestore diverso. Questo garantisce che l'accesso ai dati sia virtualmente sempre disponibile anche in caso di guasto ai server o alle connessioni internet.

Infrastruttura

Il datacenter Mediasoft è composto da server di classe Enterprise con i seguenti requisiti minimi di alta affidabilità:

- **Disk mirroring (Redundant Arrays of Independent Disks – RAID)**
Il guasto di un disco interno non comporta una interruzione di servizio o perdita di dati.
- **Connessioni di rete multiple**
I server hanno più connessioni di rete così che il guasto ad una linea internet o cavo della rete interna non comporta una interruzione del servizio.
- **Unità di alimentazione multiple**
Il guasto di una unità di alimentazione e la sua sostituzione non comporta una interruzione del servizio.
- **Hot swap**
La sostituzione di componenti guasti o l'installazione di nuovi componenti possono essere fatti con i server accesi e non necessitano di una interruzione del servizio.

Nel magazzino del datacenter sono disponibili i ricambi per i componenti critici del sistema.

Personale tecnico

Il datacenter Mediasoft è gestito da personale con reperibilità 24/7. La presenza di personale tecnico in loco è sempre garantita durante i normali orari di ufficio.

Manutenzione programmata

Manutenzione e aggiornamenti hardware e software vengono programmati ed eseguiti nelle ore notturne per evitare interruzioni al servizio durante i normali orari di ufficio.

Sistemi di alimentazione

Il sistema di alimentazione del Centro Dati Mediasoft è garantito da gruppi di continuità e generatori di corrente capaci di mantenere la infrastruttura autonoma per un tempo indeterminato.

I sistemi di alimentazione dei componenti critici del sistema, come server e gruppi di continuità, sono modulari e hotswap per poter essere facilmente riparati e aggiornati senza interruzioni del servizio.

Sistemi di condizionamento e controllo della temperatura

Il datacenter Mediasoft è dotato di un sistema di condizionamento che garantisce sempre una temperatura compresa tra 22 e 24°C e con percentuali di umidità relativa comprese tra il 35 e il 50%.

Nel datacenter è presente una unità di condizionamento di emergenza che può essere attivata in caso di guasto al sistema di condizionamento principale.

Prevenzione incendi

I protocolli di prevenzione e gli impianti di estinzione antiincendio del datacenter di Mediasoft sono a norma per quanto stabilito dalle norme antincendio locali.

Contatti

Responsabile del trattamento

Francesco Scarabelli
Telefono: 0536324886
Email: media@msw.it

Dati Società

Mediasoft snc
P.IVA: 02353700368
Indirizzo: Via scarabelli, 6 – 41026 Pavullo nel Frignano (MO)
Telefono: 0536324886
Fax: 0536324887
Email: media@msw.it