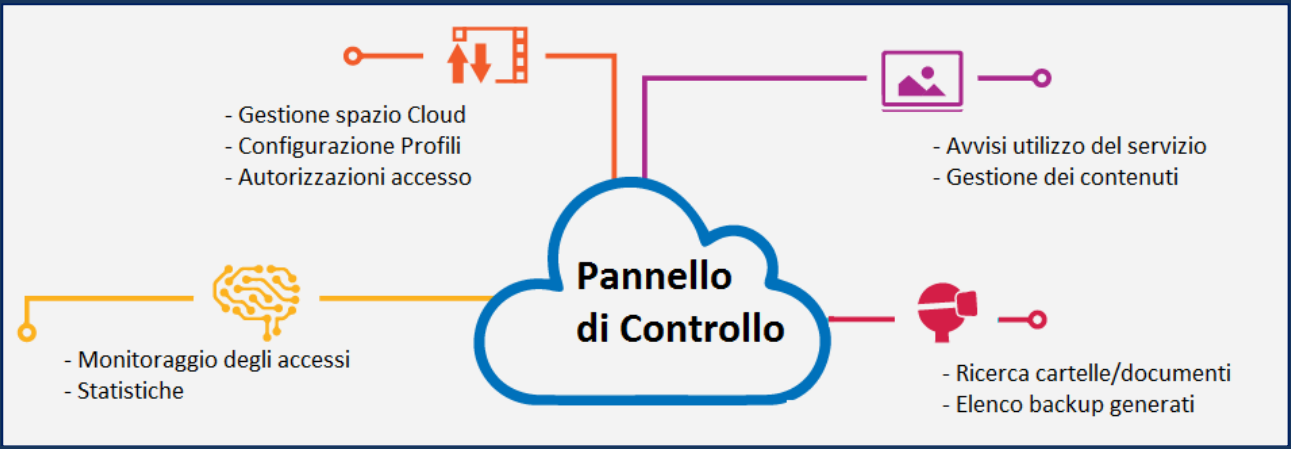
e-Cloud

Vantaggi

- Protezione ed accessibilità secondo i parametri del cloud hosting a disposizione dell'infrastruttura Fortres Tech
- Area creata dentro della piattaforma della Azienda
- Pannello di controllo per la gestione completa del servizio Cloud disponibile per il responsabile dati
- Ridondanza e continuità del servizio
- Accesso ai dati da remoto, disponibilità e accessibilità 24/24 tutti i giorni dell'anno
- Formati specifici dei file, per evitare virus e altre minacce informatiche
- Caricamento file fino ad un primo livello pari a 100GB
- Trasferimento dati usando il protocollo HTTPS
- Invio e-mail per ogni accesso e aggiornamento del backup dei dati
- Ogni cartella ha delle impostazioni di sicurezza e condivisione personalizzata
- Integrazione con il backup del database, incrementando maggiori livelli di sicurezza
- Riduzioni dei costi nella configurazione, installazione e manutenzione di dispositivi, eventuale recupero di dati/informazione, evitando principalmente la perdita di informazione.
- Backup e protezione documenti in base alle normative GDPR

Pannello di controllo – Responsabile Dati



Il 25 maggio 2018, entrava in vigore la General Data Protection Regulation (GDPR) dell'Unione Europea, una articolata normativa sulla privacy e la protezione dei dati personali. L'obiettivo principale del regolamento è quello di rafforzare e rendere omogeneo il trattamento dei dati personali dei cittadini.

Con il passare dei mesi, l'argomento è stato da molti accantonato ma invece è ancora oggi più che mai attuale ed è importante ricordare che chi non è adeguato potrebbe subire delle sanzioni nel caso di verifiche.

Tra i numerosi punti toccati dalla regolamentazione GDPR, uno di quelli sicuramente più importanti riguarda la **protezione dei dati e il backup** degli stessi.

La normativa relativa ai backup è definita dalla **lettera c), comma 1 dell'art. 32 del GDPR**: il responsabile del trattamento dei dati, ovvero il soggetto che immagazzina dati sensibili, deve assicurarsi di avere delle procedure di cifratura dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico. Questo significa avere delle procedure di backup dei dati sempre attive, e che consentano inoltre di cifrare il contenuto del backup stesso, in modo tale da renderlo inaccessibile a chi non conosca le necessarie password.

Ricordiamo che il backup deve riguardare tutti i dati personali e informazioni sensibili presenti in azienda e quindi dovrà riguardare file (documenti) e cartelle, database, posta elettronica.

1. il backup deve essere eseguito con le seguenti modalità: almeno 3 backup, su almeno 2 sistemi differenti di cui 1 off-site. Si possono sfruttare i supporti FTPS/SFTP e cloud;
2. adottare un metodo di cifratura dei dati;
3. effettuare un monitoraggio continuativo dello stato dei backup utilizzando le notifiche e-mail o adottando servizi specifici per tale funzionalità;
4. fare delle verifiche a campione sulla funzionalità di restore dei backup con cadenza regolare.