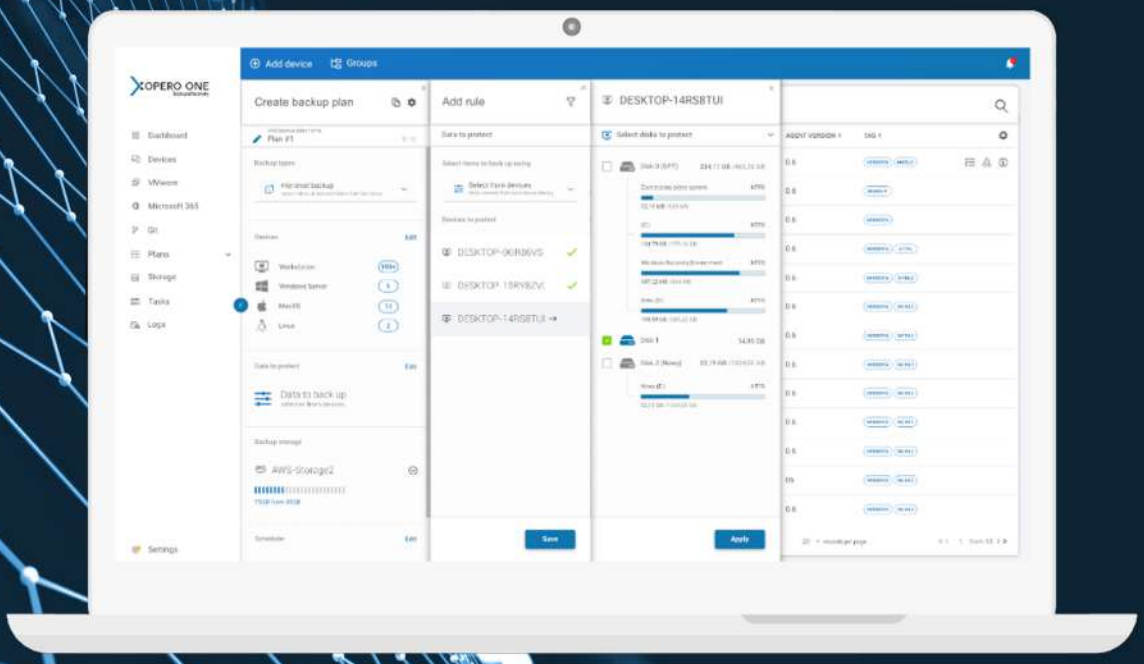
XOPERO
Backup&Recovery

# Perché eseguire il backup di Microsoft Office 365?

## Affrontare le cyber minacce e proteggere i dati nel modello di Responsabilità Condivisa



# Sintesi dei Contenuti

Migliaia di aziende nel mondo si affidano alla suite Microsoft Office 365. Gli utenti pensano che i propri dati non siano solo archiviati in modo sicuro nel cloud, ma anche che siano sottoposti a backup e quindi recuperabili. Questa è però un'interpretazione errata piuttosto pericolosa. Microsoft Office 365 è una piattaforma Software-as-a-Service affidabile che garantisce alta disponibilità e accesso alla suite e ai dati. Microsoft, però, lavora in un "modello di responsabilità condivisa" nel quale é responsabile della manutenzione delle infrastrutture. Il backup e la protezione dei dati, nel modello di responsabilità condivisa, restano di responsabilità degli utenti. Secondo questo modello, Microsoft fornisce la protezione contro eventuali incidenti o attacchi che dovessero verificarsi nei propri data center, ma non garantisce la rapidità e la velocità di ripristino nel caso i dati dovessero essere cancellati, compromessi o andare persi.

Ecco perché i team IT devono conoscere e prendere consapevolezza della loro quota di responsabilità e immaginare strategie di protezione dei dati che si affianchino al crescente uso delle app SaaS. Microsoft Office 365 mette a disposizione soluzioni per la protezione dei dati, sia native che aggiuntive, ma non riesce a fornire funzionalità di protezione dei dati di livello enterprise che potrebbero però essere necessarie alle aziende per la conformità (ad esempio alla policy di conservazione dei dati a breve e a lungo termine).

Vediamo quindi come Xopero può aiutarti a proteggere i tuoi dati nel modello di responsabilità condivisa, per assicurarti che i dati della tua suite Microsoft Office 365 siano backuppati e recuperabili in qualsiasi caso di incidente.

# Modello di responsabilità condivisa: comprendere le rispettive responsabilità

In un data center tradizionale on-premise, l'azienda che lo possiede è responsabile della gestione della sicurezza, compresa la mitigazione e il recupero in caso di incidenti. Dall'altro lato, se l'azienda  un Infrastructure-as-a-Service (come Azure o AWS), la sicurezza dell'infrastruttura è responsabilità del provider. Nel modello di Software-as-a-Service, in particolare nella suite Microsoft Office 365, Microsoft è responsabile del mantenimento dell'infrastruttura e deve assicurare che i dati restino disponibili e accessibili mentre l'utente ha la responsabilità di proteggere i propri dati Microsoft Office 365. Ciò significa, concretamente, che l'utente è responsabile del ripristino dei dati persi, rubati, cancellato o compromessi e ciò è piuttosto logico ed ovvio. Alla fine stiamo parlando dei dati degli utenti no?

E' particolarmente importante conoscere quali aspetti della sicurezza di un servizio cloud gravino sulla responsabilità del provider e quali invece dovrebbero importare all'utente. Inoltre, è molto importante sapere come garantire la protezione dei dati, il backup e il ripristino point-in-time utilizzando i servizi Xopero, così da poter condividere la responsabilità esattamente come fa Microsoft.

| Responsabilità di Microsoft | Responsabilità dell'Utente | Responsabilità di Xopero |
|---|---|---|
| Infrastruttura cloud (uptime del servizio Office 365, livello di accessibilità dei dati - SLA) | Dati aziendali (accesso e controllo dei dati Office 365 salvati nel cloud) | Backup automatico e protezione dei dati, regola di backup 3-2-1 |
| Sicurezza a livello di infrastruttura (fisica, logica, a livello di app, controlli di sicurezza utenti) | Sicurezza a livello di dati (accessibilità, integrità, sicurezza e protezione dei dati da cancellazioni accidentali / intenzionali, rischi interni / esterni, rispetto delle politiche di conservazione) | Backup e ripristino a livello dei dati (backup automatico, sicuro, criptato, ripristino ad un momento specifico nel tempo, opzioni di ricerca avanzata, funzionalità di smart disaster recovery) |
| Storage in cloud Microsoft | Mantenimento di copie multiple dei dati | On-premise, cloud pubblico / privato, Microsoft Cloud, Xopero Cloud: metti i tuoi dati ovunque vuoi! |
| Conformità di base (data processor) | Rispetto di previsioni normative, conformità alle leggi locali e alle normative del settore (data owner) | Criptazione, integrità e ripristino dei dati, disaster recovery - ti aiutamo a rispettare tutti i requisiti di conformità (data guard). |
| Conservazione di base (fino a 30 giorni per la licenza Business) | Conservazione di lungo periodo | Conservazione dati illimitata - on premise, nel backup in cloud, secondo schemi di conservazione avanzati (FIFO, GFS, incrementale). Opzioni di ripristino granulari e ad un momento specifico nel tempo. |

# I limiti della protezione dati offerta da Microsoft

Se osserviamo più da vicino la tabella sopra, noteremo i principali limiti della protezione di Microsoft Office 365, tra cui:

- **Limitazione della sicurezza a livello di infrastruttura e uptime del cloud:** Microsoft si concentra sull'infrastruttura globale e garantisce che la suite Office 365 resti online e in esecuzione. Sebbene Microsoft 365 sia un sistema innegabilmente affidabile (con una garanzia di affidabilità del 99,9% di uptime), soffre di frequenti interruzioni su base locale/regionale che possono comportare la perdita di dati. Ecco quindi che i clienti sono responsabili dell'accesso, il controllo e la sicurezza dei propri dati ospitati nell'infrastruttura Microsoft 365.

- **Solo archiviazione cloud:** Microsoft Office 365 si basa su Azure Cloud e garantisce la replica integrata dei dati e la ridondanza geografica da data center a data center. Questi sono dei must per garantire disponibilità e affidabilità del servizio. Tuttavia, una replica non è un backup e non è neppure sotto il tuo controllo, dato che non ti appartiene neppure.

Non protegge i tuoi dati da cancellazioni o manomissioni - in questi casi i dati cancellati o corrotti vengono anch'essi replicati assieme ai dati corretti, così la tua replica comprenderà anche quei dati corrotti. Ecco perchè mantenere più copie dei dati è una tua responsabilità. Ti invitiamo a tenere a mente della regola di backup 3-2-1 e mantenere almeno tre diverse copie dei dati in due differenti location, compresa una che sia esterna all'azienda. Xopero ti aiuta a implementare la regola 3-2-1 offrendoti backup on-premise, backup in cloud e opzioni multiple di archiviazione.

- **Conformità di base:** Microsoft lo afferma chiaro e tondo: il suo ruolo è quello del data processor. Si concentra quindi sulla privacy dei dati, dispone di una vasta gamma di certificazioni, garantisce l'autenticazione a due fattori ma l'adeguamento agli obblighi normativi e di settore resta una responsabilità del proprietario dei dati (utente).
- **Conservazione di base:** Microsoft offre un tempo di conservazione limitato dei dati per gli utenti businees, con l'uso del Cestino. Tieni presente che il Cestino può essere svuotato accidentalmente o intenzionalmente e non c'è modo poi di ripristinare quei dati. La scelta di avvalersi di Policy di archiviazione comporta un pagamento extra per lo storage (0,20 dollari/GB/mese - 5000 dollari al mese per 50 GB extra per un'azienda con 500 dipendenti). Anche in questo caso, è responsabilità dell'utente quella di garantirsi una soluzione di conservazione dei dati illimitata e avanzata, così come opzioni di ripristino granulare e ad un determinato momento nel tempo.

## Responsabilità dell'utente nel modello di responsabilità condivisa

Gli utenti Office 365 possono fare affidamento su Microsoft, che fornisce una suite molto affidabile, ma devono contare su sé stessi per quanto riguarda la protezione dei propri dati. E' cioè responsabilità dell'utente quella di assicurarsi che i suoi dati restino accessibili, disponibili, protetti e sempre ripristinabili a qualsiasi momento nel tempo per avere la certezza che nessun disastro o incidente possa causare perdita di dati, inattività e perdite finanziarie.

Secondo il modello di responsabilità condivisa, la protezione dei dati è responsabilità e dovere dell'utente. Perchè la protezione sia effettiva ed efficace, le aziende dovrebbero assicurarsi di impiegare processi di data backup e data recovery. Microsoft non offre questi servizi nel modello di responsabilità condivisa, ma sono necessari perchè l'utente rispetti la sua parte di responsabilità.

Il backup e la protezione dei dati sono "il core" delle responsabilità dell'utente Microsoft office 365. Il principale obiettivo del backup dei dati è quello di garantire che, in caso di qualsiasi incidente / disastro, i dati critici dell'azienda siano accessibili e recuperabili in un lasso di tempo più breve possibile. Una soluzione di backup efficace dovrebbe garantire più funzionalità di classe entreprise - automazione, on-premise, archiviazione in cloud, criptazione, ottimizzazione, conservazione illimitata, e altre impostazioni avanzate.

Conservazione di lungo periodo: come ricordato poco sopra Microsoft offre un periodo limitato di conservazione dei dati con l'uso del Cestino per gli utenti business. Una soluzione di backup efficiente deve garantire una conservazione illimitata e convieniente dei dati, così da poterli ripristinare a qualsiasi momento nel tempo.

Data recovery: è il processo di ripristino dei dati dal backup per prevenire tempi di inattività, mantenere un basso RTO ( il tempo necessario al recupero della piena operatività), fornire rapido accesso ai dati e tornare velocemente operativi in qualsiasi momento. E' importante disporre di opzioni di ripristino granulari così che le operazioni di recovery possano spaziare da un singolo file al ripristino immediato di un intera libreria dati di Office 365.

# Le minacce più comuni ai dati Microsoft 365

L'idea (sbagliata) che Microsoft sia responsabile del backup dei dati per conto dell'utente è piuttosto diffusa. Ora sappiamo, invece, che rientra nella "quota" di responsabilità dell'utente proteggere i dati residenti nella suite Microsoft Office 365. Questa è una consapevolezza essenziale, senza la quale si rischiano situazioni in cui i dati finiscono incustoditi.

Ora veniamo alla domanda delle domande (nonché titolo di questo documento): perchè fare il backup di Microsoft Office 365? Che cosa potrebbe succedere ai dati salvati nel cloud Azure? Come prevenire gli incidenti? Diamo uno sguardo alle più diffuse minacce ai dati Microsoft 365.

### # 1 - Cancellazione accidentale

La cancellazione accidentale, come puoi immaginare, è l'eliminazione involontaria dei dati effettuata da un utente autorizzato. Questo rischio può sembrare innocuo, o comunque poco grave, ma è piuttosto comune e può creare danni significativi se passa inosservato o viene fatto nel corso di una manutenzione ordinaria. E, come ricorderai, Microsoft office 365 offre alcune funzionalità integrate come il Cestino e gli Elementi Recuperabili ma, in base alla policy di conservazione, i file cancellati possono essere recuperati solo entro il periodo limitato di conservazione. Questo lasso di tempo è quello che chiamiamo di "soft deletion" (puoi ancora recuperare i dati dal Cestino). Trascorso il periodo di conservazione, i file sono cancellati permanentemente. E' quello che chiamiamo "hard deletion".

I tool di conservazione nativi in Microsoft 365 sono orientati al breve periodo e obbligano al fatto che l'utente si renda conto dell'errore entro la scadenza del periodo di conservazione. Queste funzionalità servono solo a correggere errori commessi da singoli utenti nel corso dello svolgimento del lavoro. Inoltre non hanno la capacità di ripristinare interi account o caselle di posta elettronica - in caso di errore a livello di amministrazione, potresti anche perdere tutti i tuoi dati Microsoft 365.

A meno che tu non abbia a disposizione...

...un backup di terze parti che ti garantisca policy di conservazione dei dati di lungo periodo e personalizzabili, il recupero di intere caselle di posta elettronica o il ripristino granulare, il ripristino ad un determinato momento nel tempo e solo di tipologie di dati scelti in precedenza.

### #2 - Cancellazione intenzionale

Intenzionale? Chi potrebbe mai farlo? Bene, credi o meno a quanto ti diciamo, ma dipendenti insoddisfatti o ex dipendenti potrebbero avere molte ragioni per cancellare intenzionalmente i tuoi dati (anche dal cestino). L'accesso ai file e ai contatti cambia rapidamente: è difficile tenerlo sempre d'occhio. Microsoft non ha strumenti per differenziare utenti regolari e un ex dipendente che tenta di eliminare dati aziendali critici prima di lasciare l'azienda. La risposta è ovviamente quella di attivare controlli utenti rigorosi, classificare i dati e...

...fare il backup dei dati come terza linea di difesa. Una garanzia al 100% di recupero dei dati eliminati in modo permanente in altre location.

### #3 - Rischi esterni

Malware, virus, ransomware, ingegneria sociale infliggono serissimi danni alle aziende in giro per tutto il mondo. La falsa credenza che gli attaccanti non prendono di mira le infrastrutture in cloud è piuttosto diffusa: eppure il fatto che sia più difficile non lo rende impossibile.

Microsoft ha la responsabilità di fornire la sicurezza di base dell'infrastruttura per proteggere l'utente dai cyber rischi. Backup sicuri e criptati minimizzano al massimo l'impatto di questi attacchi e garantiscono alle aziende di non trovarsi a dover pagare un altissimo riscatto, a perdere permanente tutti i dati aziendali, la fiducia degli utenti, la reputazione. Soluzioni di backup di terze parti garantiscono il recupero dei dati e riducono l'inattività delle infrastrutture IT. Inattività che costa alle aziende, in media 5.600 dollari al minuto, secondo Gartner.

### #4 - Sanzioni per violazione dei requisiti normativi, legali e di conformità

In Microsoft 365, l'utente gioca un ruolo cruciale (data owner) in fatto di conformità e requisiti legali / normativi. In qualità di data processor, Microsoft garanisce che le misure siano in atto, che i controlli normativi siano implementati e che le certificazioni di settore siano aggiornate. Offre poi funzionalità limitate per aiutare le aziende a rispettare gli obblighi normativi e legali. Una di queste è la funzionalità "Blocco per controversia legale" che consente di congelare permanentemente i dati, impedendone la cancellazione. Il malus di questa soluzione è che lo spazio di archiviazione è limitato a 100GB: limite che grosse aziende superano piuttosto velocemente. Inoltre il Blocco per controversia legale funziona sui dati attualmente disponibili: di conseguenza non includerà le informazioni eliminate in precedenza.

I requisiti normativi, legali e di conformità variano da settore a settore e da Stato a Stato (ad esempio abbiamo il Federal Rules of Civil Procedure e il Sarbanes-Oxley Act negli Stati Uniti, il General Data Protection Regulation - GDPR in Unione Europea). Tuttavia, il rischio di  sanzioni amministrative, multe e controversie legali è alto ovunque.

La soluzione di backup di terze parti è esattamente ciò di cui ha bisogno un'azienda per conservare i dati per tutto il tempo necessario, per soddisfare le normative finanziarie, per produrre prove in caso di controversia legale e per documentare l'utilizzo dei dati dei clienti.

### #5 - Lacune nelle politiche di conservazione

Le lacune nelle politiche di conservazione espongono le aziende non solo a lacune legali ma anche operative. A causa della sempre crescente velocità delle operazioni aziendali, c'è un continuo bisogno di aggiornare e migliorare le policy, comprese le policy di conservazione alle quali è spesso difficile stare dietro. Microsoft 365 ha criteri di conservazione limitati, utili a gestire incidenti con effetti di breve termine e perdite di dati situazionali. In quali casi si creano lacune nelle politiche di conservazione?

Per esempio, quando un impiegato lascia l'azienda, gli amministratori solitamente ne disattivano gli account. Microsoft cancellerà automaticamente gli account degli utenti inattivi e i dati relativi. Se i dati non sono backuppati, le aziende perderanno il controllo su dati importanti e non potranno recuperarli. Microsoft non fornisce infatti l'archiviazione illimitata, ripristino ad un determinato momento nel tempo e rispritino granulare - gli utenti hanno bisogno di soluzioni di backup di terze parti per ottenere queste funzionalità.

### #6 - Perdita di dati durante le migrazioni

Le aziende possono distribuire Microsoft Office 365 in ambienti on-premise, cloud o ibridi, in base alle proprie policy. Le aziende che usano Microsoft 365 solitamente necessitano di una finestra di tempo per migrare da Exchange on-premise a Exchange online. La migrazione può compromettere i processi di protezione dei dati, creare lacune nella policy di conservazione e causare perdita di dati.

Un'efficiente soluzione di backup per Office 365 dovrebbe essere in grado di gestire ambienti ibridi. Inoltre, come utente dovresti essere in grado di archiviare i dati vunque desideri: in locale, in cloud o in entrambi.

## La soluzione di backup di terze parti: la parte mancante nel modello di responsabilità condivisa

La soluzione di backup di terze parti è la tua principale arma contro tutti i cyber rischi che minacciano la suite Microsoft 365. Ma copre anche la tua parte di responsabilità condivisa, garantendoti un'efficace protezione dei dati. Xopero Backup  per la suite Microsoft Office 365 consente:

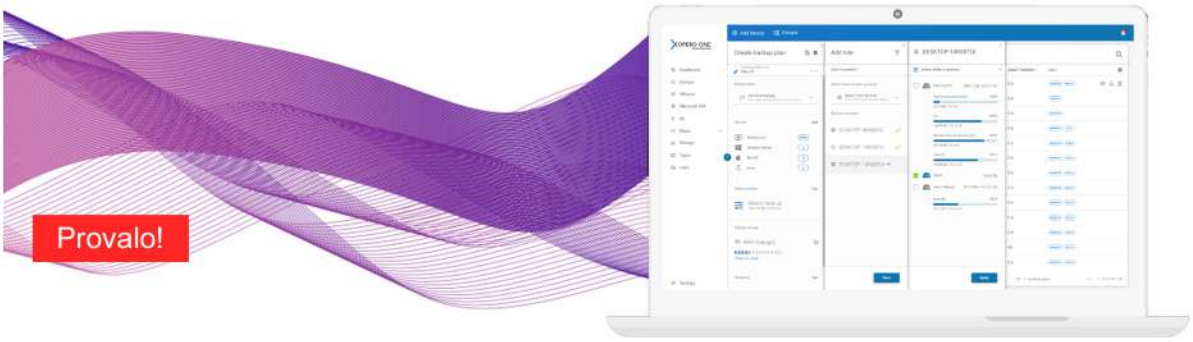
- la protezione dei dati;
- la conservazione a lungo termine (perfino illimitata);
- la sicurezza a livello dei dati;
- la possibilità di mantenere più copie in locale o nel cloud;
- rispettare i requisiti normativi, di settore e di conformità;
- fronteggiare i cyber rischi...

... insomma, le tue responsabilità nel modello di responsabilità condivisa. E molto altro!

# Perchè Xopero Backup per Microsoft 365?

Scegli la protezione più intuitiva ma completa della tua suite Microsoft 365, on premise o in cloud, dotata di un'ampia gamma di opzioni per il ripristino dei dati - dal ripristino ad un determinato momento nel tempo al ripristino solo di alcune tipologie dei dati fino ad intere caselle di posta elettronica.

Inizia a proteggere il tuo ambiente Microsofy 365 in meno di un minuto e gestisci tutto tramite un'interfaccia estremamente semplice e intuitiva. E' difficile spiegare a parole quanto sia semplice e intuitiva la nostra console ma, una volta che l'avrai vista, non cercherai altro. Sarà amore a prima vista!




**Backup completo e granulare**
Fai il backup delle Email, dei Contatti, dei Calendari di Office 365 e dei dati di OneDrive. On-premise o in cloud. Grazie al recupero granulare, ripristina tutto, in qualsiasi momento, nella stessa destinazione o anche in una differente.

**Distribuzione? Meno di un minuto!**
Aggiungi semplicemente la tua azienda Microsoft 365, scegli gli utenti da proteggere e aggiungili al piano di backup predefinito o personalizzato, per iniziare a proteggere gli account.

**On-premise o in cloud**
Scegli se archiviare le copie in locale sulla tua macchina, nel cloud - AWS o Azure -, o in entrambi. Rispetta la regola di backup 3-2-1 e rilassati: avrai la consapevolezza che i tuoi dati sono sani e al sicuro.

**Backup automatico pianificato**
Imposta il piano di backup una volta - scegline uno predefinito o personalizzalo secondo le tue necessità: stabilisci quali dati backuppare, dove, scegli le impostazioni avanzate, pianifica. Non servirà altro: il backup criptato sarà eseguito automaticamente.

**Ottimizzazione del backup**
Rispettiamo il tuo spazio di archiviazione - grazie alla conservazione, versioning e compressione il backup è più veloce, occupa meno spazio e non impatterà sul tuo lavoro.

**Conservazione illimitata**
Assciurati di poter recuperare i dati cancellati anche una volta scaduti i termini di conservazione garantiti dalla suite Microsoft grazie alla possibilità di conservare i dati senza limiti che ti offre Xopero. Rendi i tuoi dati sempre accessibili e recuperabili, rispetta i requisiti normativi e di conformità.

**Scalabilità illimitata**
Imposta un numero infinito di utenti. Aggiungili o cancellali dalla tua organizzazione e i piani di backup si adatteranno automaticamente alle tue impostazioni Microsoft 365.

XOPERO
Backup&Recovery

Xopero Software nasce nel 2009 come azienda al servizio principalmente degli utenti delle PMI. Il nostro obiettivo è quello di creare un ambiente più accessibile, semplice e al tempo stesso garantire i massimi standard di sicurezza a prezzi accessibili per qualsiasi livello di impresa.

Nel 2015 Xopero ha iniziato una collaborazione con QNAP Inc. – uno dei principali provider NAS globali. Questa aggiunta ha ampliato il nostro portfolio per includere una vera appliance di backup.

Nel 2017, Xopero è stato completamente esteso sul mercato globale grazie alla collaborazione con ESET. La nostra società ha preso il posto precedentemente occupato da StorageCraft in ESET Technology Alliance.

**DISTRIBUTORE PER L'ITALIA**

s-mart
be smart, be safe

www.s-mart.biz
richieste@s-mart.biz