Backup solutions to protect your company's data

The g-Backup for Microsoft 365 solution **protects data stored in Microsoft's platform**: Office (Excel, Word, PowerPoint, Access, OneNote, Project, Visio), Outlook (Email, Calendar, Contacts), Teams, SharePoint and OneDrive.

With three years of base retention and unlimited storage, g-Backup 365 will give you the peace of mind you need against threats like viruses, ransomware and data corruption or loss, with Gigas' full support.

Recover your data whenever you need it. Anywhere, anytime.

ADVANTAGES

Quick, granular recovery

Specific items, such as individual emails, files or folders, can be restored for a user or the entire organisation. Granular recovery is particularly useful when you only need to recover a specific item instead of an entire environment.

Maximum security

g-Backup 365 offers advanced security features, such as local encryption and encryption in transit, thus ensuring protection of your data against unauthorised access. This helps to comply with security requirements and keep sensitive data safe.

Reliable technology

Gigas uses Veeam technology. Veean is well known and respected in the data protection market, offering prompt and competent customer support. It also provides frequent updates, which continuously enhances our solution

Scalability and flexibility

With g-Backup 365, you can scale the solution to your organisation's needs from the dashboard, adding or removing licenses as required. This helps you to control costs based on demand and avoid excessive spending on unnecessary resources.

Compliance

g-Backup 365 ensures compliance with the GDPR by keeping separate copies of Microsoft 365 data in European territory. It can also respond to incidents of security breaches easily and demonstrate conformity with retention policies.

Risk reduction

Backing up Microsoft 365 data with g-Backup 365 considerably reduces the risk of data loss. Any lost data can be restored from the backup copies, which can be particularly important in certain situations, e.g., accidental deletions, system failures and malware or ransomware attacks.

Immutable repository

A perfect solution to combat threats like ransomware, viruses, and malware, ensuring that the storage where the backup is kept cannot be modified, not even by Veeam itself.

Third offsite copy

In specific cases, such as for security reasons, some companies need to create three copies, with the third copy being stored in a different location.

Features

✔ **Minimises risks** to security related to:

- Accidental data deletion and corruption
- Connectivity or infrastructure failures
- Incidents with, or confusion creating, retention policies
- Internal security threats
- External security threats
- Compliance and legal obligations
- Teams data structure

✔ Ensures compliance with the GDPR

✔ Provides initial backup through our dashboard

✔ Monitoring and reporting through the online dashboard and email

✔ Recovery through the Self-Service Restore Portal with ability to select the specific point in time

Prices

g-Backup 365

Backup of:
✔ Outlook
✔ Teams
✔ Sharepoint
✔ OneDrive

Data retention:
✔ 3 years

Storage:
✔ Unlimited

1,8 €
user/month

Aditional retention	Repositories	
	Offsite (3rd copy)	Immutable
3 years (included)	+1 €	+2€
5 years +1€	+1,5€	+2,5€
10 years +1,5€	+2€	+3€

How do I do it?

The process is easy:

1. Sign up for the service
2. Open the dashboard
3. Open your g-Backup 365 service
4. Select the items you want to back up (mailbox, OneDrive, Sites, Teams) and that's all!
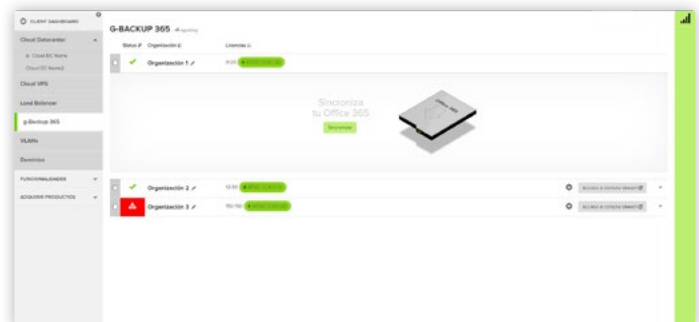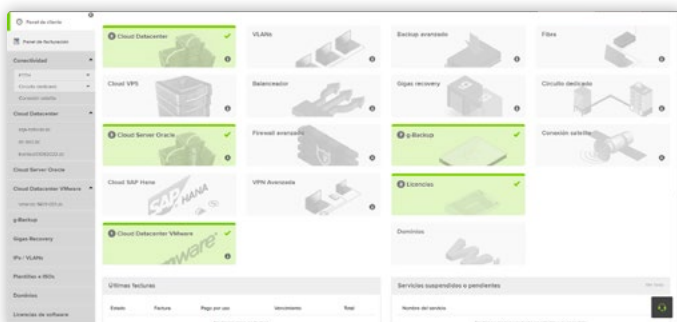
Track the status of your backup, check the number of licences used and, if necessary, make any granular restores you need. **All this is done with a user-friendly and intuitive dashboard.**

Why backup your Microsoft 365 data?

Microsoft's geographical redundancy does not guarantee a sound contingency system. With g-Backup 365, you can keep a historical copy of 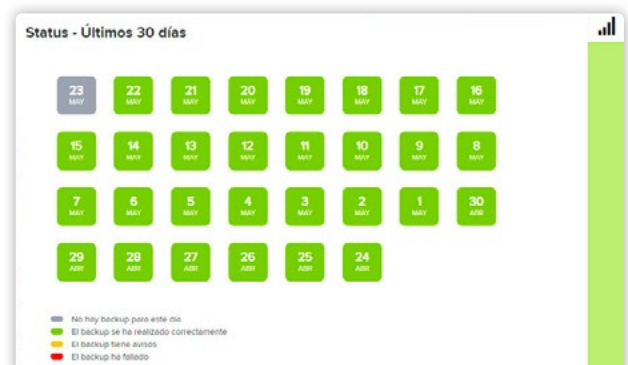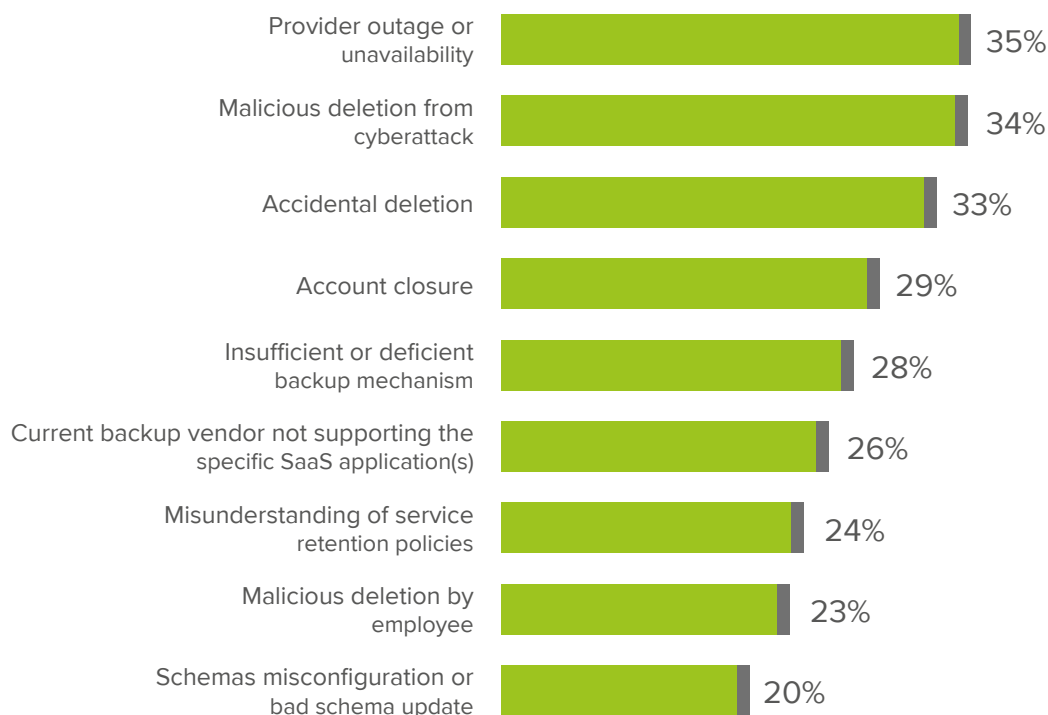data at an alternative location that can be accessed and managed directly. If data are lost, accidentally deleted or affected by a malicious attack, we can, for instance, **quickly retrieve any lost files, emails and data**. Moreover, Microsoft's retention periods are not long enough for most companies since **backup copies are not made beyond 140 days**.

Lastly, Microsoft 365 applications have different data retention periods, but only offer protection averaging from 30 to 90 days. An important issue to know is that according to Microsoft's shared responsibility model, Microsoft is only required to guarantee uptime reliability of its cloud infrastructure for the 365 platform. Microsoft 365's data replication resources are, at best, basic. They include the recycle bin for short-term data recovery and geographical redundancy in multiple data centres. Under this shared responsibility model, it is up to the customer to perform the backups and store backup data in another location if they want to have an efficient retention policy.

Take the right decision and make a backup copy of your data. Oni can keep you from having to make a huge financial and technical effort by helping you have backup copies of your data with **g-Backup 365 under the BaaS** (Backup as a Service) modeladn professional Oni support.

Peace of Mind as a Service!

Top reasons for data loss in applications on SaaS platforms

Reason	Percentage
Provider outage or unavailability	35%
Malicious deletion from cyberattack	34%
Accidental deletion	33%
Account closure	29%
Insufficient or deficient backup mechanism	28%
Current backup vendor not supporting the specific SaaS application(s)	26%
Misunderstanding of service retention policies	24%
Malicious deletion by employee	23%
Schemas misconfiguration or bad schema update	20%

Microsoft 365 shared responsibility model

	Primary responsibility	Supporting technology	Security	Regulations
Microsoft's responsibility For further information, visit the Microsoft 365 Trust Center	**Microsoft global infrastructure** Uptime of the Microsoft 365 cloud service	**Microsoft 365 data replication** DC to DC geo-redundancy **Recycle bin** Limited recovery of short-term data loss (with no point-in-time recovery)	**Infrastructure level** · Physical security · Logical security · Application security · User/administrator controls	**Roll as data processor** Privacidade de dados Controlo regulatório Certificações do setor HIPPA, Sarbanes-Oxley
Your responsibility	**Your Microsoft 365 data** Access and control of your data residing in Microsoft 365	**Microsoft 365 backup** Copy of your data stored in a different location **Full data retention** Short- and long-term retention that bridges any/all gaps in policies. Granular and point-in-time recovery options	**Data level** Internal: · Accidental deletion · Malicious internal employee · Employee retaliation · Test manipulation External: · Ransomware · Malware · Hackers · False Apps	**Roll as data owner** Comply with corporate and industry regulations Requirements of internal legal and compliance officers

Learn more: **https://www.veeam.com/blog/office365-shared-responsibility-model.html?ad=in-text-link**

MAKE IT SAFE,
MAKE IT GIGAS