



Inova Solutions IT Mixology

*Crafting premium service
solutions*

Presented by: Néstor Díaz
Date: 2025-May-15



Inova Solutions es *Tu pasaporte a la nube!*



Inova Solutions es el proveedor de confianza de Microsoft para soluciones en la nube en el Caribe y Ecuador. Somos un socio de soluciones de Microsoft con amplio conocimiento en licencias de software. Nuestra historia comenzó en 2009 y seguimos escribiéndola hoy.

Conozca los MDs

Misión

Empoderar a empresas de todos los tamaños a crear ventajas de negocio a través de la transformación digital.



Johan Rog

Financial Managing Director

Hans Kruithof

Commercial Managing Director

La tecnología nos *fascina*

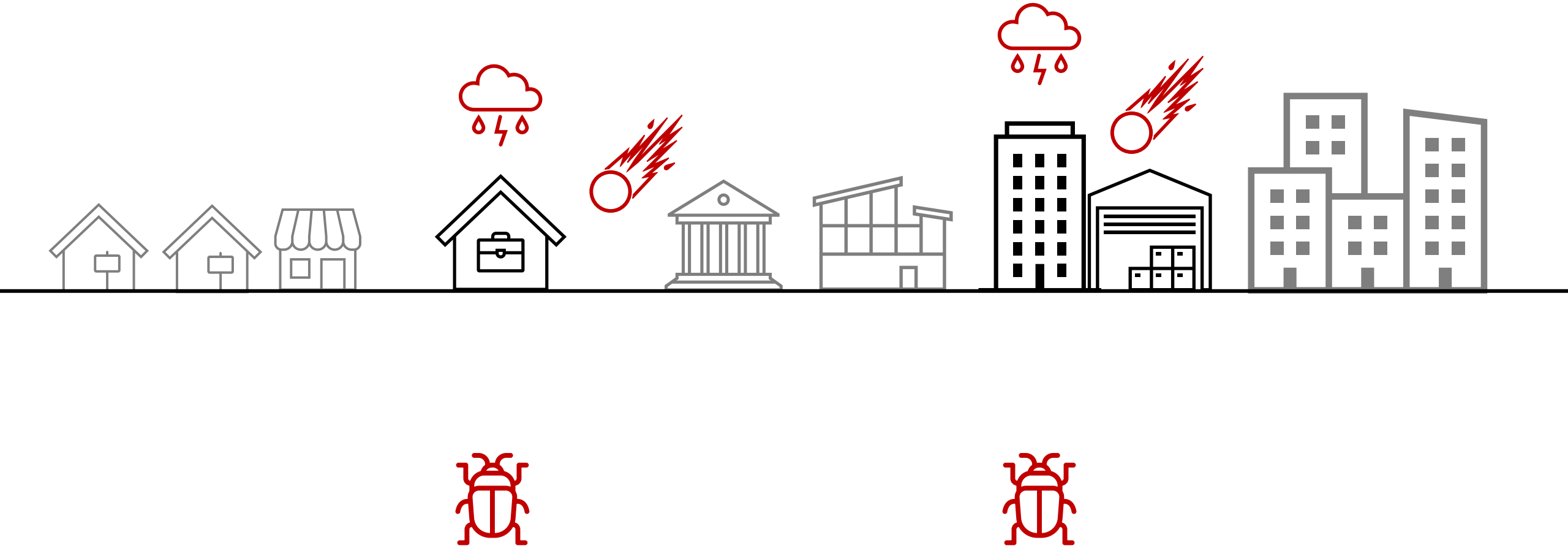
Seguridad,
cumplimiento y
gobernanza

El panorama digital es cada vez más complejo

- **Más datos:** crecimiento acelerado de aplicaciones y generación de datos
- **Más lugares:** Datos viven en múltiples nubes; trabajo híbrido requiere acceso seguro desde cualquier ubicación.
- **Más amenazas:** número y escala de ataques está aumentando, y las herramientas maliciosas son cada vez más fáciles de acceder
- **Más requisitos:** cambios legislativos, nuevas regulaciones y nuevas tecnologías todos tienen impacto en seguridad y gobernanza



Las organizaciones, pequeñas y grandes, enfrentan las **mismas amenazas**





Tres retos que apremian

Dado que enfrentamos un panorama tan complejo, enfoquemonos hoy en tres retos de particular importancia en 2025. Sin importar el tamaño de su empresa, estos tres temas son clave para su organización.

Inteligencia
Artificial

Continuidad de
negocios

Protección de
identidades

Inteligencia Artificial: **no divulgue sus datos**



10
PM

DO YOU
KNOW
WHERE YOUR
CHILDREN
ARE?



La IA existe
en su
empresa
aunque no lo
sepa

Shadow AI

78%

...de los usuarios están accediendo a sus propias herramientas de IA, sin supervisión ni controles¹.

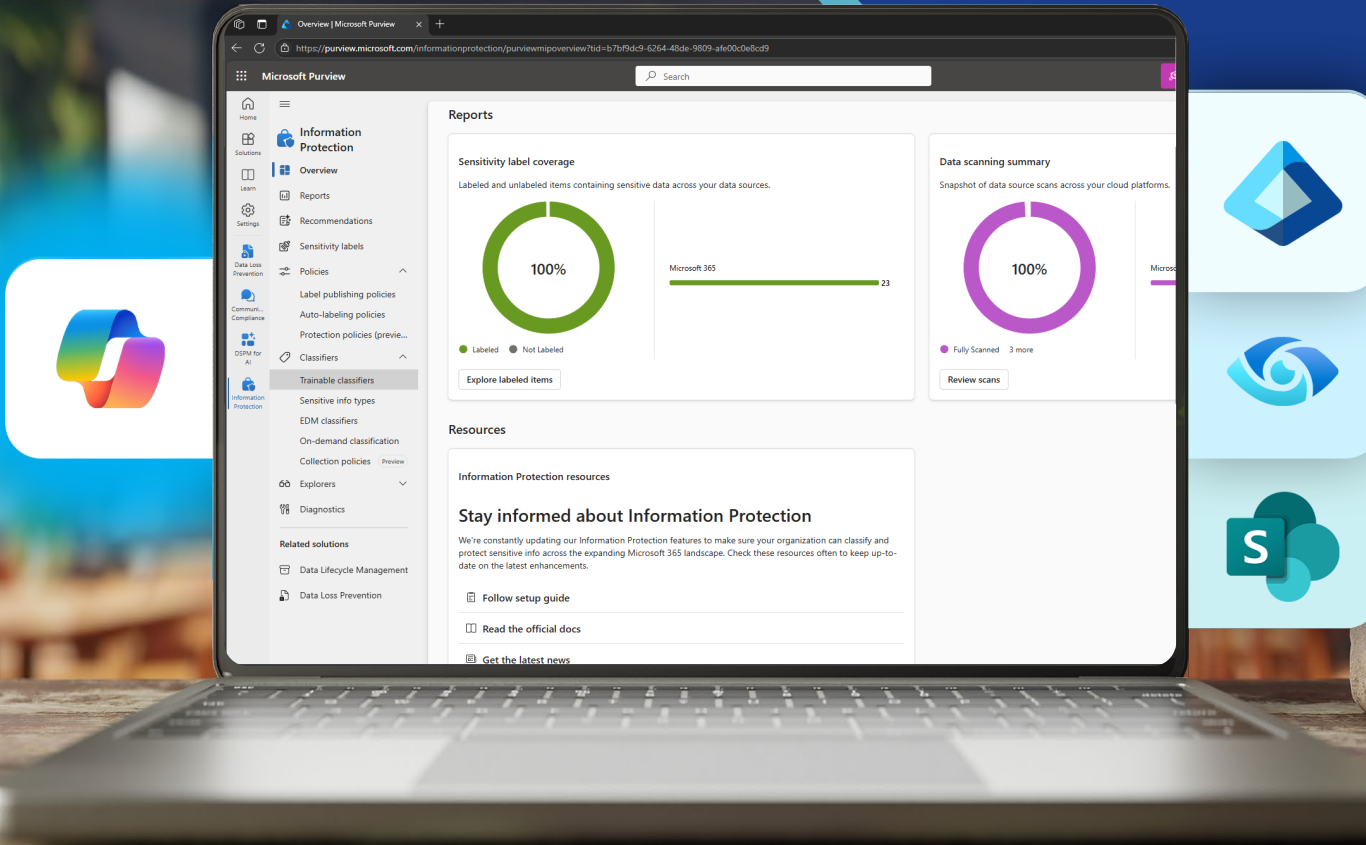
"Sin control"

97%

...de las organizaciones tienen preocupaciones sobre la IA debido a la falta de controles para mitigar los riesgos de fuga de datos².

1. 2024 Work Trend Index Annual Report from Microsoft and LinkedIn: AI at Work Is Here. Now Comes the Hard Part
2. Securing data in an AI-first world with Microsoft Purview, Nov 15, 2023

¿Cómo logro tomar el control?



- ✓ Entra ID y accesos
- ✓ Sensitivity labels y DLP
- ✓ SAM y DSPM for AI

Configure usuarios, grupos y accesos

The screenshot displays the Microsoft Entra ID Groups management interface. The left sidebar contains navigation options: Home, What's new, Diagnose & solve problems, Favorites, Identity (expanded), Overview, Users, Groups (selected), Overview, All groups (active), Deleted groups, Group settings, Devices, Applications, Protection, Identity Governance, External Identities, Show more, Protection, and Learn & support.

The main content area is titled 'Groups | All groups' and shows a list of 5 groups found. The search mode is set to 'Contains'. The groups listed are:

Name	Object Id	Group type
All Company	ce4052bc-64a0-4586-a443-0bb4f757a6ad	Microsoft 365
Copilot Journey	eb293a9a-9d88-467c-a8ed-c84e4aa9042b	Microsoft 365
Equipo de prueba	e818d40f-e314-4f57-ace0-1e582bf0b247	Microsoft 365
Hospitales El Coqui	18d453af-a1fa-4c5f-b894-ae16c2b9a7fb	Microsoft 365
Inova Service Delivery	1da079a6-a394-46cf-9603-412c4f274b1a	Microsoft 365

Asegure que sus datos estén etiquetados



Sensitivity labels

① You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first [complete these steps](#) to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish labels Export Refresh

5 items

☐		Name	Priority	Scope	Created by	Last modified
☐		Personal	⋮ 0	Files & other data assets, Email		Sep 20, 2023 5:19:23 PM
☐		Public	⋮ 1	Files & other data assets, Email		Mar 14, 2025 7:19:18 AM
☐	▼	General	⋮ 2	Files & other data assets, Email		Sep 20, 2023 5:19:24 PM
☐		Anyone (unrestricted)	⋮ 3	Files & other data assets, Email		Sep 20, 2023 5:19:25 PM
☐		All Employees (unrestricted)	⋮ 4	Files & other data assets, Email		Sep 20, 2023 5:19:26 PM
☐	▼	Confidential	⋮ 5	Files & other data assets, Email		Sep 20, 2023 5:19:27 PM
☐		Anyone (unrestricted)	⋮ 6	Files & other data assets, Email		Sep 20, 2023 5:19:30 PM
☐		All Employees	⋮ 7	Files & other data assets, Email		Sep 20, 2023 5:34:55 PM
☐		Trusted People	⋮ 8	Files & other data assets, Email		Sep 20, 2023 5:19:36 PM
☐	▼	Highly Confidential	⋮ 9	Files & other data assets, Email		Sep 20, 2023 5:19:37 PM
☐		All Employees	⋮ 10	Files & other data assets, Email		Sep 20, 2023 5:34:56 PM
☐		Specified People	⋮ 11	Files & other data assets, Email		Sep 20, 2023 5:19:42 PM

Utilice data loss prevention (DLP)

Data Loss Prevention

Overview

Policies

Alerts

Classifiers

Trainable classifiers

Sensitive info types

EDM classifiers

On-demand classification

Collection policies

Preview

Explorers

Diagnostics

Related solutions

Information Protection

Insider Risk Management

Overview

Nestor, complete the listed tasks to access analytics with insights and tailored DLP policy recommendations

Learn about analytics

Review the provided Microsoft documentation and instructional videos to learn the functionality.

Optional

2 minutes

Turn on analytics for risk detection and policy refinement opportunities (preview)

Enabling analytics allows you to detect potential risks, discover blind spots and find opportunities for policy improvement or fine-tuning.

Highly recommended

2 minutes

Explore DLP analytics

DLP resources

Stay informed about DLP

We're constantly updating our DLP features to make sure your organization can identify, monitor, and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

Follow setup guide

Read the official DLP docs

Get the latest news on DLP

Protect sensitive info

Protect Sensitive Information

Insight

157 unprotected docs in SharePoint and OneDrive contain sensitive financial, healthcare, human resource (HR), IP and trade secrets, or customer account info.

Recommended action

Create the recommended DLP policies that detect these types of documents and notify you when it's shared with people outside your org.

147 Documents containing medical/healthcare data

1 Documents containing IP and trade secrets data

10 Documents containing customer account data

68 Documents containing financial data

71 Documents containing human resources data

Top activities detected

No activity detected

Either there's been no file activity or you haven't turned on auditing to track user and admin activity.

Device health overview

All devices are updated

These devices may not be fully protected until they are correctly configured and policies have synced.

Empiece rápido con **Restricted Sharepoint Search**

PowerShell

 Copy

```
Set-SPOTenantRestrictedSearchMode -Mode Enabled
```

📌 Note

Once enabled, any new sites created are excluded unless they're added to the allowed list.

Restricted SharePoint Search is off by default. If you decide to enable it, Copilot and non-Copilot users are able to find and use content from:

- An allowed list of curated SharePoint sites set up by admins (with *up to 100 SharePoint sites*), honoring sites' existing permissions.
- Users' OneDrive files, chats, emails, calendars they have access to.
- Files from their frequently visited SharePoint sites.
- Files that were shared directly with the users.
- Files that the users viewed, edited, or created.

SAM: Sitios de SharePoint con acceso restringido

SharePoint admin center

Home

Sites

Active sites

Deleted sites

Containers

Policies

Settings

Content services

Migration

Reports

Advanced

More features

Advanced management

Customize navigation

Show all

Active sites

Use this page to sort and filter sites and change site settings.
Learn more about managing sites

Create

Edit

Membership

Hub

Sharing

Site name	URL
Deutschland	.../sites/de
Employees	.../sites/Employees
Finance 10	.../sites/finance10
Governance	.../sites/Governance
Group Paris	.../sites/groupparis
GT365	.../sites/GT365
Home	.../sites/Home
Ignite	.../sites/ignite
Intranet	.../sites/Intranet
IT-News	.../sites/it-news
IT-Project Chicago	.../sites/IT-ProjectChicago
IT-Project Orlando	.../sites/projectorlando
IT-Project Seattle	.../sites/IT-ProjectSeattle
IT-Project Wien	.../sites/IT-ProjectWien
IT-Team Alpha	.../sites/IT-TeamAlpha

Ignite

Private team

Email

Open in Teams

View site

Delete

Demos for Ignite

General

Activity

Membership

Settings

Email

Privacy

External file sharing

Sensitivity label

Restrict content from Microsoft 365 Copilot

Restricted site access

Let people outside the organization email this team

Send copies of team emails and events to team members' inboxes

Don't show team email address in Outlook

Private

Public

New and existing guests

More sharing settings

None

On

Off

Site access restriction is off at the organisation level.

Edit

Save

SAM: Maneje los **sitios inactivos**

Site lifecycle management PRO

Use this page to create and manage policies that automate tasks across the lifecycle of your sites.

[Learn more about managing the lifecycle of your sites](#)

Inactive site policies

Number of policies: 0

Create and configure policies to:

- Identify inactive sites
- Send notifications to site owners or admins
- Automatically archive or mark sites in read-only

Open

SAM: Maneje los **sitios inactivos**

☰

Home

Sites

^

Active sites

Deleted sites

Containers

∨

Policies

^

Sharing

Access control

Site lifecycle management

Settings

Content services

∨

Migration

Reports

^

App insights

Change history

Data access governance

OneDrive accounts

Advanced

^

API access

Create an inactive site policy

● Overview

○ Scope

○ Configuration

○ Finish

Manage inactive sites

This policy will:

- 🔍 **Generate reports of inactive sites**
Sites are included in a monthly inactive sites report if they have had no visits, edits, or file actions, and no activity on any connected resources like Microsoft Teams, Viva Engage, and Exchange within a time period that you set.
Sites excluded from policy: OneDrive, System, App catalog, Root, Home and Admin sites.
- ✉️ **Send monthly emails to site owners or site admins**
Site owners receive an email each month asking them to review their inactive sites and choose whether to keep or delete them.
- 📊 **Act on sites that are inactive for more than 3 months**
If there is no action from site owners or admins after 3 notifications, you can configure the policy to:
 - Archive sites or set site access to read only
 - Opt to take no action

[Learn more about managing inactive sites](#)

inovacorporation.com 19

SAM: Maneje los **sitios inactivos**

Create an inactive site policy

☒ Overview

☒ Scope

☒ **Configuration**

☐ Finish

Configure policy

How long after the last activity should a site be considered inactive?
Includes activity on the site, files, and any connected resources like Microsoft Teams, Viva Engage, or Exchange.

6 months ▾

Who should be notified via email if site has been inactive? *
Recipients will be able to certify the site to keep it active.

☒ Site owners

☒ Site admins

What action should the policy take on inactive sites that have not been certified by site owners or site admins after 3 notifications? *

① Enforcement actions cannot be edited after policy creation

☐ Do nothing

☒ **Take an enforcement**
Users will be able to access the site content depending on the selected action.

Select an enforcement type:

☒ **Read-only access**
Users can view site content, but can't edit it.

☐ Archive sites after mandatory read-only period **RECOMMENDED**

Turn on Microsoft 365 Archive

Free up storage space without deleting any data by archiving inactive sites. Archive lets you store sites you don't use, but need to keep, at a lower cost. You can reactivate archived sites when you need them.

[Learn how to turn on Archive](#)

SAM: Maneje los accesos a sus sitios



Home

Sites

Active sites

Deleted sites

Containers

Policies

Sharing

Access control

Site lifecycle management

Settings

Content services

Migration

Reports

App insights

Change history

Data access governance

OneDrive accounts

Advanced

API access

More features

Advanced management

Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

Unmanaged devices

Restrict access from devices that aren't compliant or joined to a domain.

Idle session sign-out

Automatically sign out users from inactive browser sessions.

Network location

Allow access only from specific IP addresses.

Apps that don't use modern authentication

Block access from Office 2010 and other apps that can't enforce device-based restrictions.

Site-level access restriction

Allow SharePoint and Global Administrators to restrict access to sites.

OneDrive access restriction

Restrict access to OneDrive content by security group.

SAM: Maneje los accesos a sus sitios

Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

Unmanaged devices
Restrict access from devices that aren't compliant or joined to a domain.

Idle session sign-out
Automatically sign out users from inactive browser sessions.

Network location
Allow access only from specific IP addresses.

Apps that don't use modern authentication
Block access from Office 2010 and other apps that can't enforce device-based restrictions.

Site-level access restriction PRO
Allow SharePoint and Global Administrators to restrict access to sites.

OneDrive access restriction
Restrict access to OneDrive content by security group.

Site-level access restriction

This setting lets you and other Global or SharePoint Administrators restrict access to sites across your organization. You can restrict the site access to security groups and Microsoft 365 groups. This applies to group-connected, Teams-connected, and non-group connected sites, giving you control over who can access the site's content.

[Learn more about Restricted Access Control for SharePoint sites](#)

☐ Allow access restriction

Continuidad de negocios: proteja sus datos



Las empresas
pierden data
SaaS **todos**
los días

77%

...de las empresas que usan aplicaciones SaaS han experimentado alguna pérdida de datos en los pasados 12 meses.

64%

...de los casos de pérdida de datos son resultado de error humano

Los proveedores de aplicaciones SaaS son responsables por remediar sus propios errores, no los de clientes.

Su Responsabilidad

- ✓ Fallos en hardware
- ✓ Fallos en software
- ✓ Desastres naturales*
- ✓ Pérdidas de energía
- ✓ Solicitudes de eliminación de datos

- ✓ Error humano
- ✓ Error en su configuración
- ✓ Actividad maliciosa interna/externa
- ✓ Ransomware y virus

Responsabilidad del proveedor



Protección

Sus datos están protegidos, con tres backups diarios automáticos y backups *on demand*.



Recuperación

Restaura su data a la fuente o a otra ubicación rápidamente. Sus datos siempre estarán a salvo con espacio y retención infinitas.



Cumplimiento

Cumpla con requisitos regulatorios de continuidad de negocios y protección de datos.



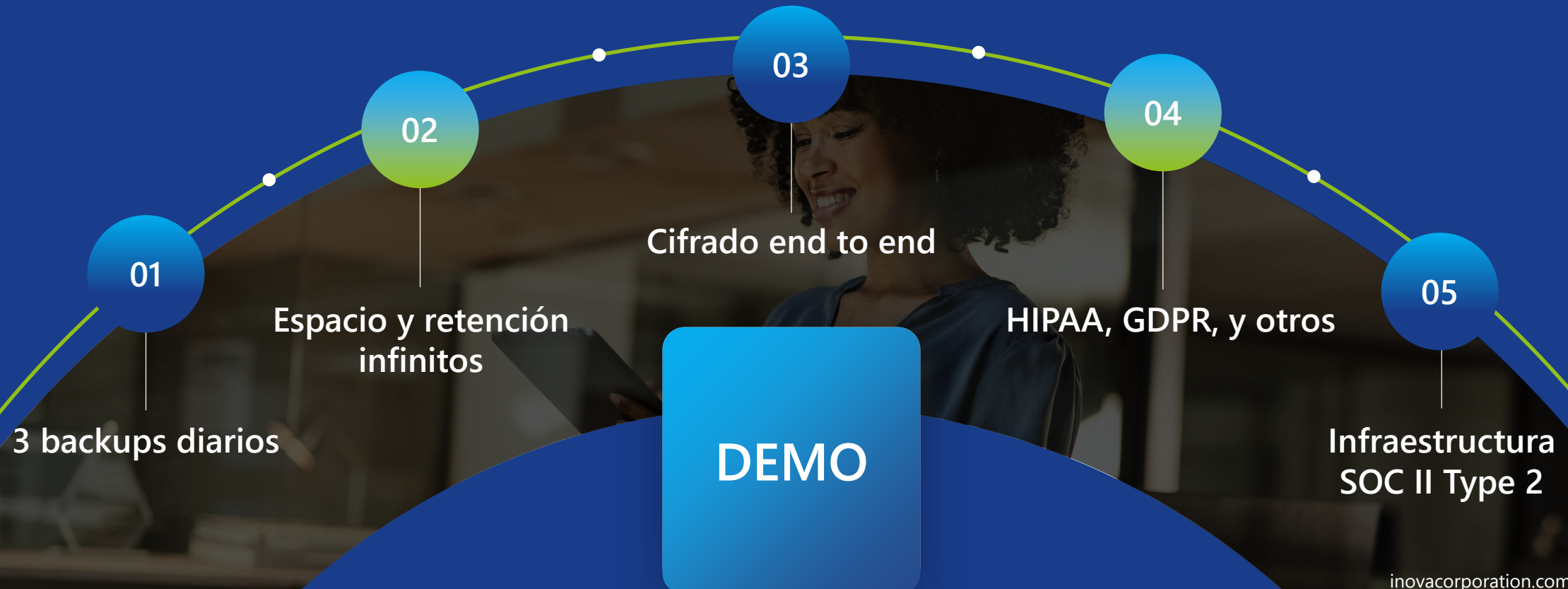
Compatibilidad

Nuestra solución puede hacer backup de Microsoft 365, G Suite y Salesforce.

Una solución confiable *cloud to cloud*

Guardian 360 – Data Backup

Nuestra solución de backups se instala de manera rápida y facil. Funciona a través de *app registrations*, así que no almacena credenciales. Sus datos están cifrados end-to-end, asegurando su seguridad.



Protección de identidades: **no basta con poner la alarma**

Las identidades son su nuevo perímetro:



Sus
identidades
son las "llaves
del Reino"

- Ya no basta con proteger la red local
- Pero ojo: tampoco basta con solo MFA
- "Zero Trust" es cada vez más importante
 - *Verify Explicitly*
 - *Least privilege access*
 - *Assume breach*
- No basta con el seguro, hace falta una alarma con monitoreo continuo

Entonces, ¿qué hago?
¿Dónde empiezo?

3 pasos para comenzar a asegurar su empresa

1. Determine si el aplican regulaciones y cuáles
 - A. GDPR, HIPAA, ISO27001, etc.
 - B. *Mapping* de controles a configuraciones
2. Configure y verifique
 - A. Despliegue configuraciones a sus usuarios y asegure que permanezcan
3. Monitoree
 - A. Nada es infallible
 - B. Monitoree actividad sospechosa para mitigar brechas

DEMO

Tres soluciones para su empresa

A pesar de que enfrentamos un panorama complejo, hemos visto soluciones que le pueden ayudar a hacer frente a sus retos.

Labels, DLP, SAM,
DSPM for AI

Guardian 360
Data Backup

Guardian 360
Security
Management

Soy muy pequeño.
No tengo recursos
para **gestionar tantas
cosas**

Solo para PyMES: Inova Shield



Servicios incluidos

Todo en uno

Este servicio premium es su solución todo en uno para:

- Seguridad
- Backup
- Manejo de cloud
- Soporte de TI
- Optimización de gastos
- Cuota mensual predecible

Con Inova, tendrá



Soporte *Always-On*

Expertos listos para ayudar, en cualquier momento



Mejor Seguridad

Defensa contra amenazas y pérdida de datos.



Costos predecibles

Precio mensual fijo sin sorpresas



Paz mental

SLAs claros, herramientas comprobadas y equipo regional de confianza

Monitoreo 24/7 y mantenimiento

- Monitoreo de PC, servidor y M365
- Mantenimiento y parches
- Informes de comprobación del estado del sistema

Ciberseguridad y backup

- Monitoreo de antivirus e EDR
- Guardian 360 Data Backup
- Guardian 360 Security Management
- Configuración de mejores prácticas de M365
- Simulación de phishing y *awareness training*

Virtual CIO y Optimización

- Planificación y *roadmap* de TI
- Optimización de costos de M365 y Azure
- Revisión y planificación de la adopción de M365
- *Status Updates* trimestrales

Apoyo técnico y helpdesk

- Incidencias ilimitadas/mes incluidas
- Asistencia remota y resolución de problemas
- SLA rápido para reducir el *downtime*

Inova Solutions **les puede ayudar**

1 Copilot Security Assessment

- Una evaluación profunda de sus políticas de protección de datos
- Ajustado a su licenciamiento
- Incluye implementación de mejores prácticas

Desde

USD \$1,200

2 G360 – Data backup

- Solución de backup para M365, G Suite y Salesforce
- Seguridad y cumplimiento *built-in*
- Puede ser manejado por su equipo o el nuestro

Desde

USD \$3^{P/M}

3 G360 – Security management

- Solución de monitoreo para la seguridad de su tenant de M365
- Evalúe su tenant contra un *baseline* personalizado
- Planes incluyen monitoreo, remediación de incidentes e informes continuos

Desde

USD \$6^{P/M}

4 Inova Shield – Managed Services

- Una única suscripción para las necesidades de TI de su PyME.
- Al momento, limitado a empresas de 50 asientos o menos.

Desde

USD \$125^{P/M}

La oferta: solo por los próximos 7 días

1 Copilot Security Assessment

- > Una evaluación profunda de sus políticas de protección de datos
- > Ajustado a su licenciamiento
- > Incluye implementación de mejores prácticas

Desde
USD \$850

2 G360 – Data backup

- > Solución de backup para M365, G Suite y Salesforce
- > Seguridad y cumplimiento *built-in*
- > Puede ser manejado por su equipo o el nuestro

Desde
USD \$1.95^{P/M}

3 G360 – Security management

- > Solución de monitoreo para la seguridad de su tenant de M365
- > Evalúe su tenant contra un *baseline* personalizado
- > Planes incluyen monitoreo, remediación de incidentes e informes continuos

Desde
USD \$4.75^{P/M}

4 Inova Shield – Managed Services

- > Una única suscripción para las necesidades de TI de su PyME.
- > Al momento, limitado a empresas de 50 asientos o menos.

Desde
USD \$90^{P/M}



¡Gracias!

¿Dudas o preguntas?
Luego, a disfrutar.

Let's connect

📞 (787) 793 2414

✉️ sales@inovacorporation.com

🌐 inovacorporation.com