Migesa®

Microsoft
Solutions

Migesa Security

Migesa

Los **retos** en un ambiente corporativo:

Migesa® | Microsoft Solutions

Usuarios dispersos

Trabajo remote e híbrido.

Dispositivos diferentes

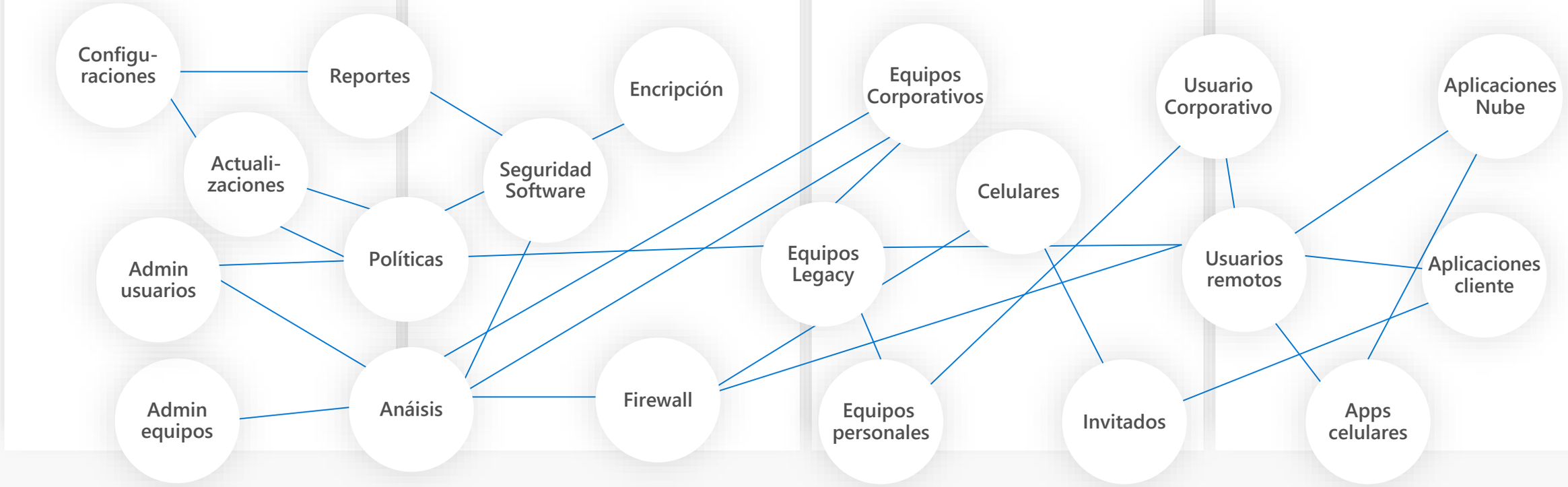
Múltiples dispositivos, muchas aplicaciones y plataformas

Satisfacción de usuarios

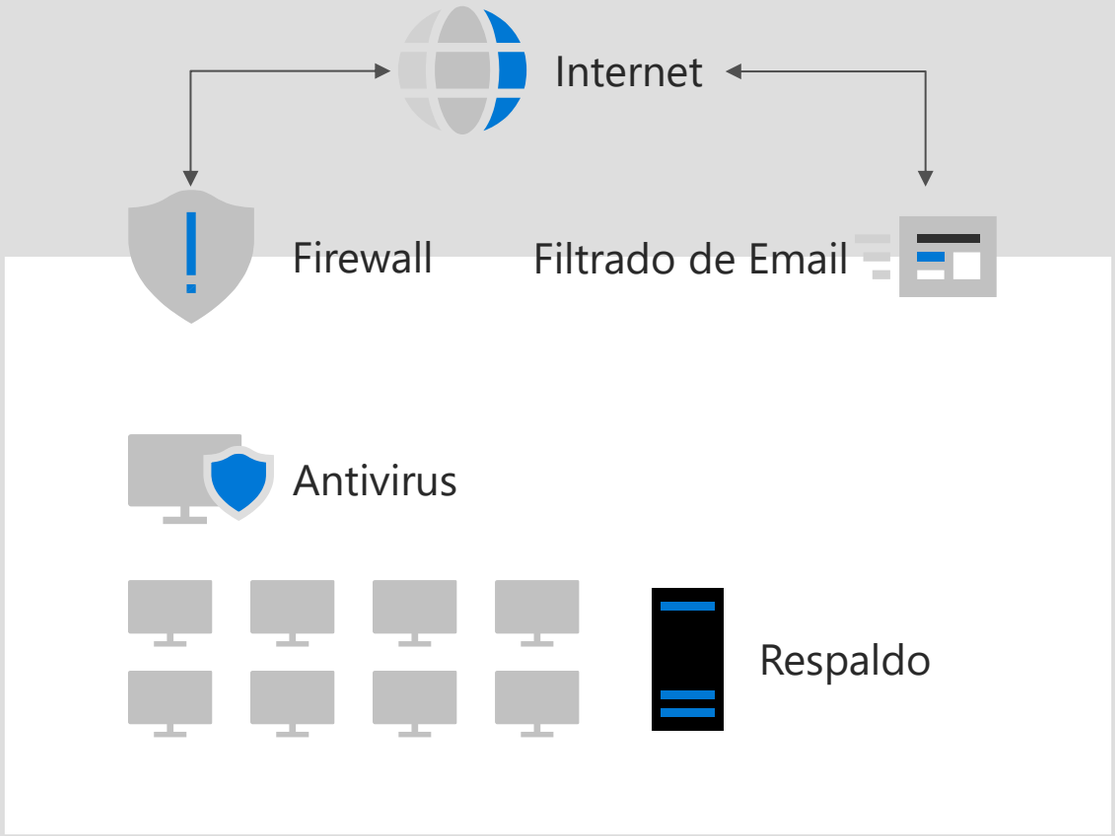
Acceso fácil y rápido a recursos de la empresa

Ciberseguridad

Mitigar riesgos y vulnerabilidades



El **reto** más evidente:



Más equipos móviles

Empleados remotos

Phishing
Ransomware
Ingeniería social

Más Información en la nube que se usa desde mayor número de equipos móviles y cibercriminales más sofisticados.

Tendencias en **seguridad**:

El trabajo está cambiando.

Por ejemplo… trabajo híbrido

38%

Fuerza laborar trabajando en híbrido

52%

Fuerza laboral considerando transición a trabajo híbrido o remoto

50%

Fuerza laboral usa equipos personales para el trabajo

Los retos y amenazas también.

83%

Empresas que han sufrido ataque de firmware en 2022-2023

25%

Empresas han identificado accesos no autorizados a Información sensible como la amenaza más importante de seguridad

921

Contraseñas atacadas cada segundo.

Migesa®

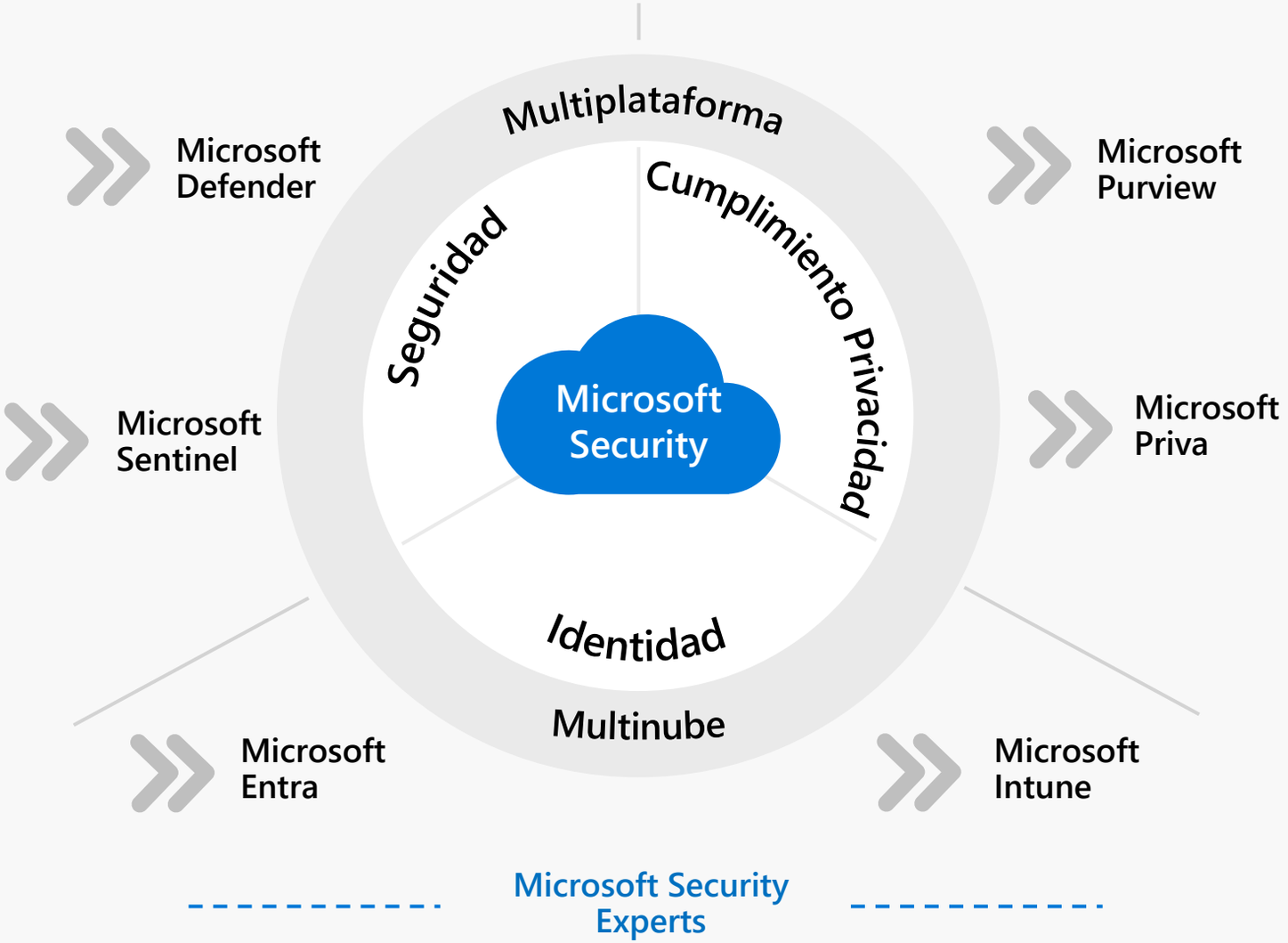
Microsoft Solutions

Migesa Security Steps

Seguridad con Microsoft

Microsoft Security

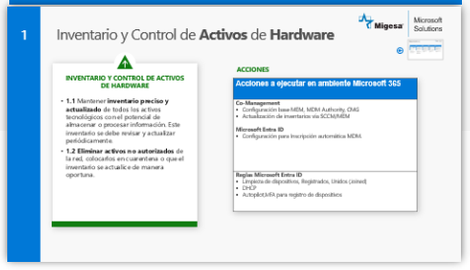
Seis familias de productos
+50 categorías



Migesa Security Steps

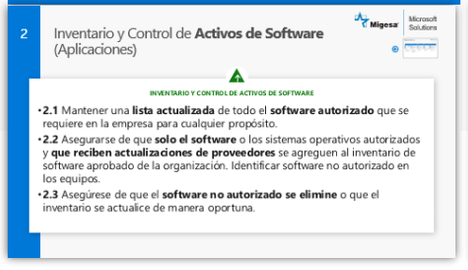
Migesa® | Microsoft Solutions

1



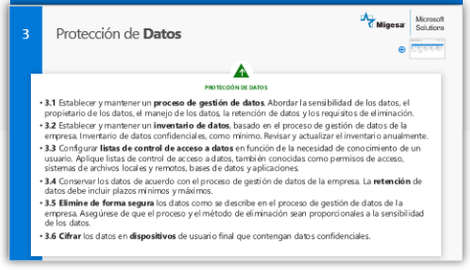
Inventario y Control de Activos de Hardware

2



Inventario y Control de Activos de Software (Aplicaciones)

3

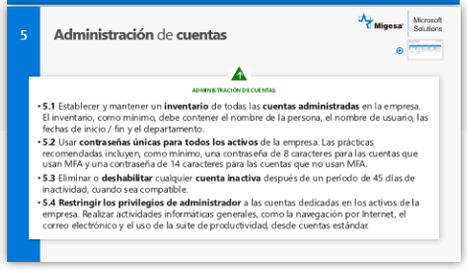


Protección de Datos

4

Configuración Segura

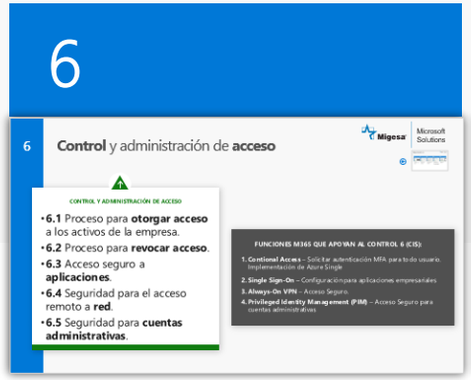
5



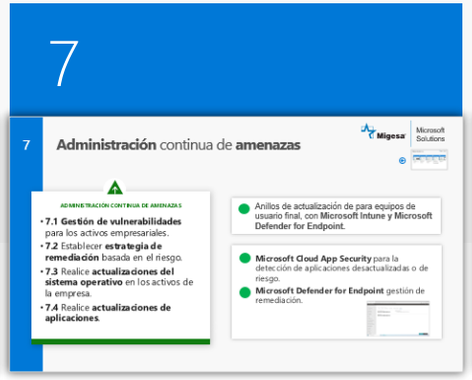
Administración de cuentas

Migesa Security Steps

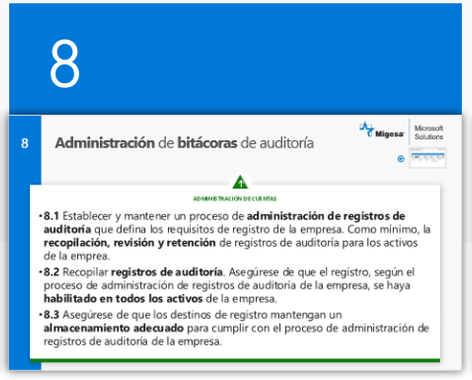
Migesa® | Microsoft Solutions



Control y administración de acceso

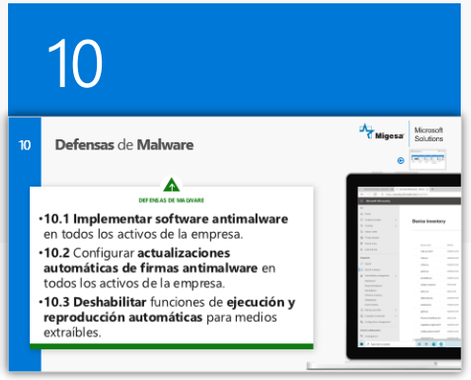


Administración continua de amenazas



Administración de bitácoras de auditoría

Protecciones a aplicaciones nube, correo electrónico y navegaciónWeb.

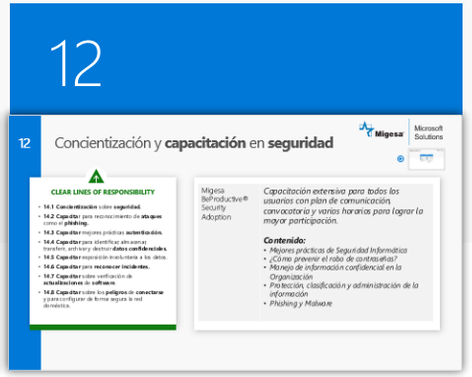


Defensas de Malware

Migesa Security Steps

Migesa® | Microsoft Solutions

Recuperación de datos

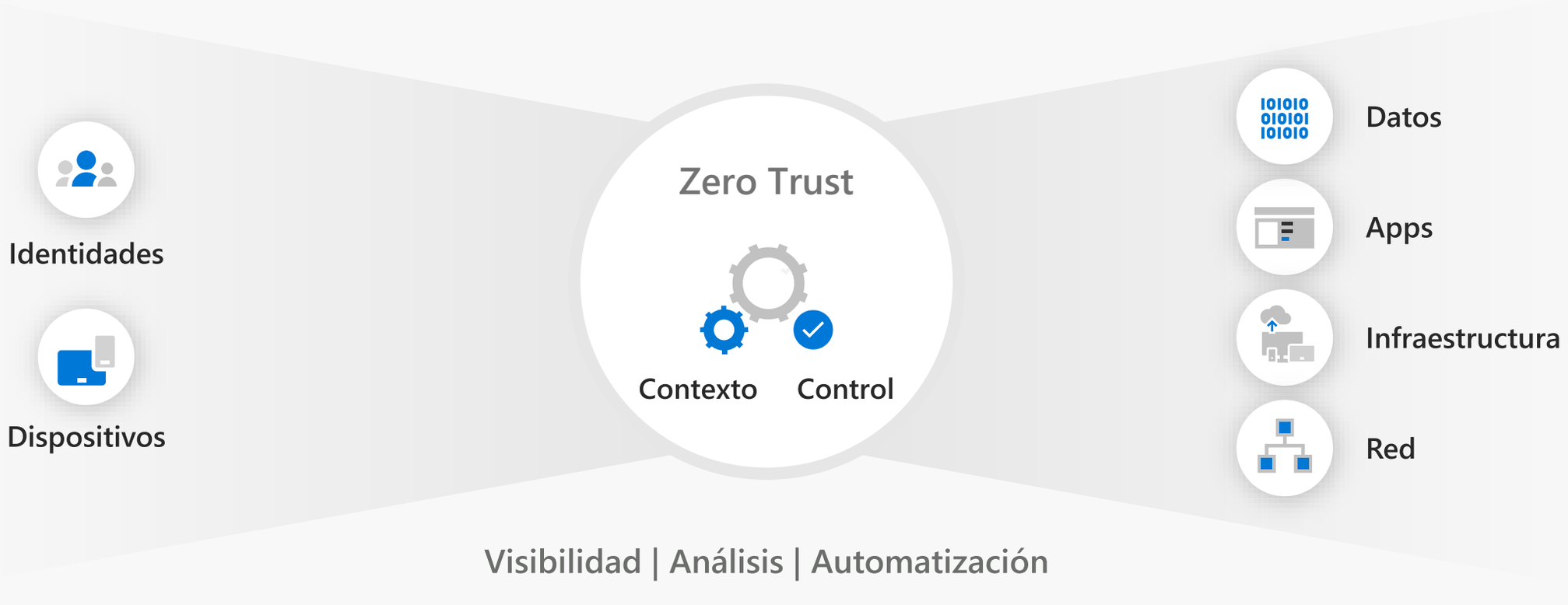


Concientización y capacitación en seguridad

Migesa Security Steps
Confianza Cero

Migesa | Microsoft Solutions

Verificación explícita | Privilegios mínimos | Asumir amenaza activa



Visibilidad | Análisis | Automatización

Migesa®

Microsoft
Solutions

¡Gracias!

1

Inventario y Control de **Activos** de **Hardware**

Migesa | Microsoft Solutions

INVENTARIO Y CONTROL DE ACTIVOS DE HARDWARE

- **1.1** Mantener **inventario preciso y actualizado** de todos los activos tecnológicos con el potencial de almacenar o procesar información. Este inventario se debe revisar y actualizar periódicamente.
- **1.2 Eliminar activos no autorizados** de la red, colocarlos en cuarentena o que el inventario se actualice de manera oportuna.

ACCIONES

Acciones a ejecutar en ambiente Microsoft 365
Co-Management ▪ Configuración base MEM, MDM Authority, CMG ▪ Actualización de inventarios vía SCCM/MEM **Microsoft Entra ID** ▪ Configuración para Inscripción automática MDM.
Reglas Microsoft Entra ID ▪ Limpieza de dispositivos, Registrados, Unidos (Joined) ▪ DHCP ▪ Autopilot,MFA para registro de dispositivos

Inventario y Control de **Activos de Software** (Aplicaciones)

Migesa | Microsoft Solutions

INVENTARIO Y CONTROL DE ACTIVOS DE SOFTWARE

- **2.1** Mantener una **lista actualizada** de todo el **software autorizado** que se requiere en la empresa para cualquier propósito.
- **2.2** Asegurarse de que **solo el software** o los sistemas operativos autorizados y **que reciben actualizaciones de proveedores** se agreguen al inventario de software aprobado de la organización. Identificar software no autorizado en los equipos.
- **2.3** Asegúrese de que el **software no autorizado se elimine** o que el inventario se actualice de manera oportuna.

Protección de **Datos**

PROTECCIÓN DE DATOS

- **3.1** Establecer y mantener un **proceso de gestión de datos**. Abordar la sensibilidad de los datos, el propietario de los datos, el manejo de los datos, la retención de datos y los requisitos de eliminación.
- **3.2** Establecer y mantener un **inventario de datos**, basado en el proceso de gestión de datos de la empresa. Inventario de datos confidenciales, como mínimo. Revisar y actualizar el inventario anualmente.
- **3.3** Configurar **listas de control de acceso a datos** en función de la necesidad de conocimiento de un usuario. Aplique listas de control de acceso a datos, también conocidas como permisos de acceso, sistemas de archivos locales y remotos, bases de datos y aplicaciones.
- **3.4** Conservar los datos de acuerdo con el proceso de gestión de datos de la empresa. La **retención** de datos debe incluir plazos mínimos y máximos.
- **3.5 Elimine de forma segura** los datos como se describe en el proceso de gestión de datos de la empresa. Asegúrese de que el proceso y el método de eliminación sean proporcionales a la sensibilidad de los datos.
- **3.6 Cifrar** los datos en **dispositivos** de usuario final que contengan datos confidenciales.

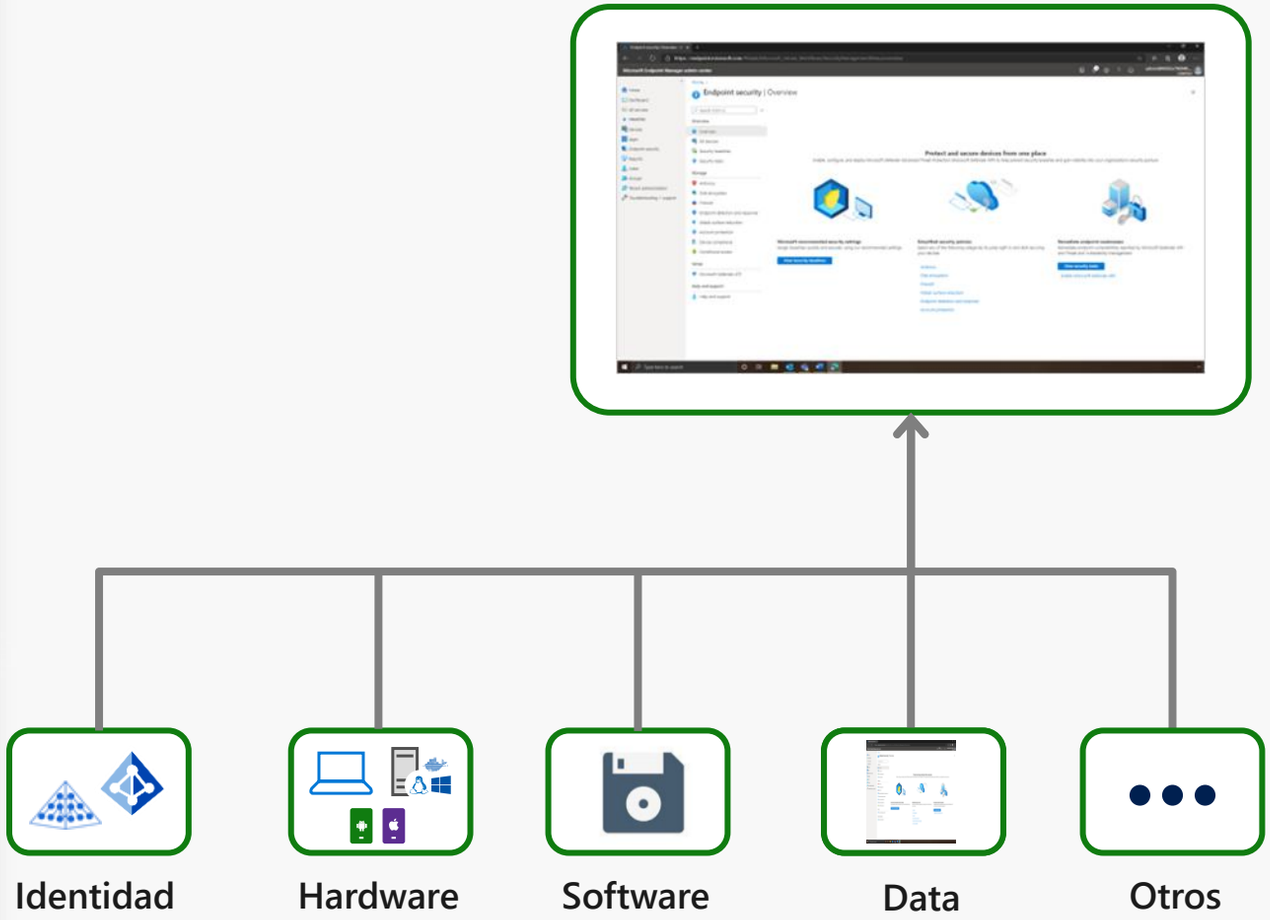
4

Configuración **Segura**

Migesa® | Microsoft Solutions

CONFIGURACIÓN SEGURA

- **4.1** Configuración segura para **dispositivos** y **software**.
- **4.2** Configuración segura de **red**.
- **4.3 Bloqueo automático** por inactividad.
- **4.4 Firewall** del sistema operativo de **servidores**.
- **4.5 Firewall** en **dispositivos de usuario** final.
- **4.6 Gestión segura** M365 (SSH, HTTPS, MFA).
- **4.7 Administración cuentas predeterminadas**.



Administración de **cuentas**

Migesa | Microsoft Solutions

ADMINISTRACIÓN DE CUENTAS

- **5.1** Establecer y mantener un **inventario** de todas las **cuentas administradas** en la empresa. El inventario, como mínimo, debe contener el nombre de la persona, el nombre de usuario, las fechas de inicio / fin y el departamento.
- **5.2** Usar **contraseñas únicas para todos los activos** de la empresa. Las prácticas recomendadas incluyen, como mínimo, una contraseña de 8 caracteres para las cuentas que usan MFA y una contraseña de 14 caracteres para las cuentas que no usan MFA.
- **5.3** Eliminar o **deshabilitar** cualquier **cuenta inactiva** después de un período de 45 días de inactividad, cuando sea compatible.
- **5.4 Restringir los privilegios de administrador** a las cuentas dedicadas en los activos de la empresa. Realizar actividades informáticas generales, como la navegación por Internet, el correo electrónico y el uso de la suite de productividad, desde cuentas estándar.

Control y administración de **acceso**

Migesa® | Microsoft Solutions

CONTROL Y ADMINISTRACIÓN DE ACCESO

- **6.1** Proceso para **otorgar acceso** a los activos de la empresa.
- **6.2** Proceso para **revocar acceso**.
- **6.3** Acceso seguro a **aplicaciones**.
- **6.4** Seguridad para el acceso remoto a **red**.
- **6.5** Seguridad para **cuentas administrativas**.

FUNCIONES M365 QUE APOYAN AL CONTROL 6 (CIS):

1. **Contional Access** – Solicitar autenticación MFA para todo usuario. Implementación de Azure Single
2. **Single Sign-On** – Configuración para aplicaciones empresariales
3. **Always-On VPN** – Acceso Seguro.
4. **Privileged Identity Management (PIM)** – Acceso Seguro para cuentas administrativas

Administración continua de **amenazas**

Migesa | Microsoft Solutions

ADMINISTRACIÓN CONTINUA DE AMENAZAS

- **7.1 Gestión de vulnerabilidades** para los activos empresariales.
- **7.2** Establecer **estrategia de remediación** basada en el riesgo.
- **7.3** Realice **actualizaciones del sistema operativo** en los activos de la empresa.
- **7.4** Realice **actualizaciones de aplicaciones**.

- Anillos de actualización de para equipos de usuario final, con **Microsoft Intune y Microsoft Defender for Endpoint.**

- **Microsoft Cloud App Security** para la detección de aplicaciones desactualizadas o de riesgo.
- **Microsoft Defender for Endpoint** gestión de remediación.

Administración de **bitácoras** de auditoría

Migesa | Microsoft Solutions

ADMINISTRACIÓN DE CUENTAS

- **8.1** Establecer y mantener un proceso de **administración de registros de auditoría** que defina los requisitos de registro de la empresa. Como mínimo, la **recopilación, revisión y retención** de registros de auditoría para los activos de la emprea.
- **8.2** Recopilar **registros de auditoría**. Asegúrese de que el registro, según el proceso de administración de registros de auditoría de la empresa, se haya **habilitado en todos los activos** de la empresa.
- **8.3** Asegúrese de que los destinos de registro mantengan un **almacenamiento adecuado** para cumplir con el proceso de administración de registros de auditoría de la empresa.

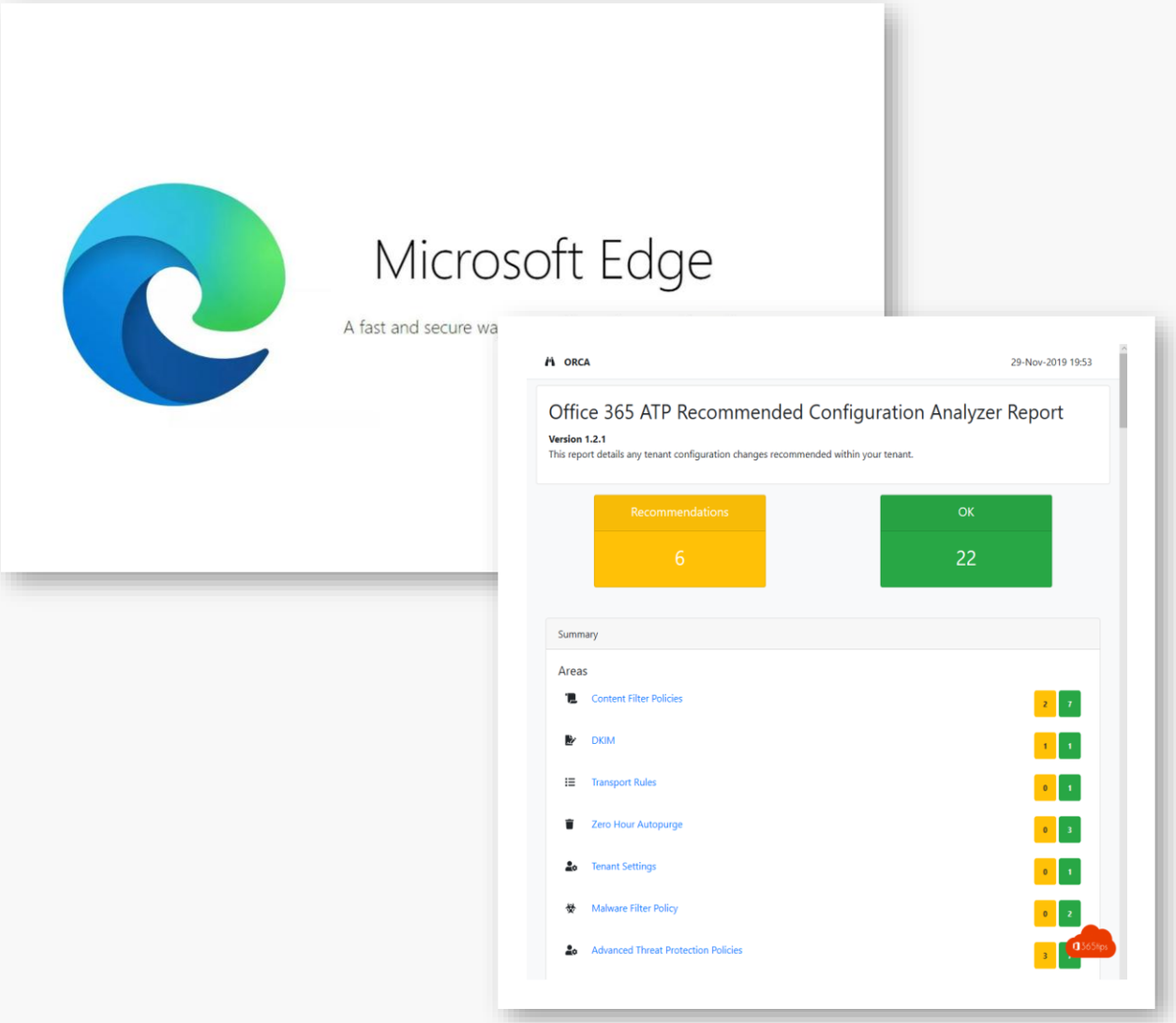
Protecciones a **Aplicaiones** de Nube

Migesa® | Microsoft Solutions

PROTECCIONES A CORREO ELECTRÓNICO Y NAVEGADOR WEB

- **9.1** Asegurar que **solo** los **navegadores** y **aplicaciones aprobadas** puedan ejecutarse en la empresa, utilizando solo la última versión.
- **9.2** Usar servicios para **navegación segura** en todos los activos de la empresa para bloquear el acceso a dominios malintencionados conocidos*.

*Ver MCAS, Control 7.

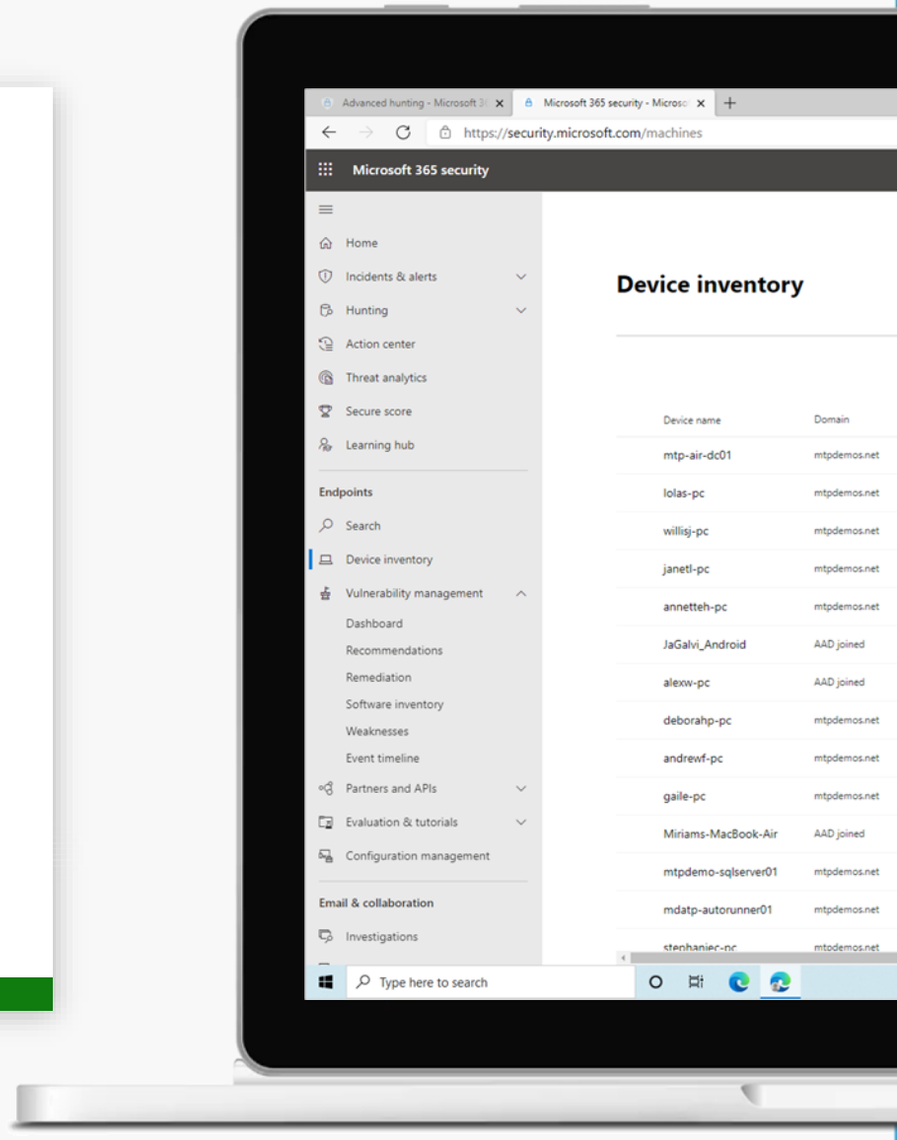


Defensas de **Malware**

Migesa® | Microsoft Solutions

DEFENSAS DE MALWARE

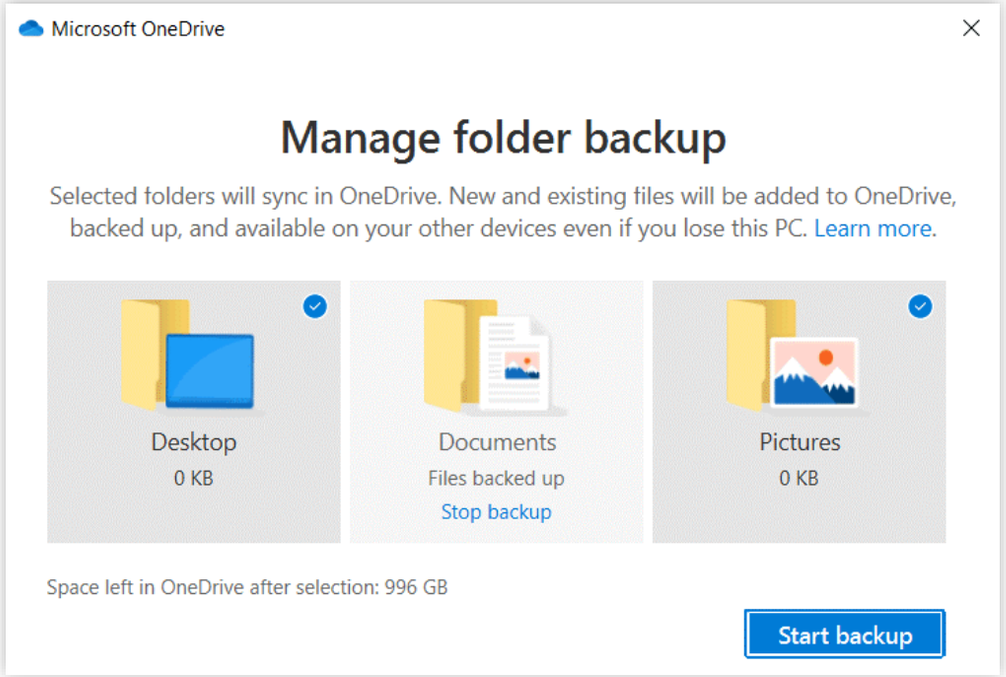
- **10.1 Implementar software antimalware** en todos los activos de la empresa.
- **10.2** Configurar **actualizaciones automáticas de firmas antimalware** en todos los activos de la empresa.
- **10.3 Deshabilitar** funciones de **ejecución y reproducción automáticas** para medios extraíbles.



Recuperación de datos

RECUPERACIÓN DE DATOS

- **11.1 Proceso de recuperación de datos**. En el proceso, aborde el alcance de las actividades de recuperación de datos, la priorización de la recuperación y la seguridad de los datos de copia de seguridad.
- **11.2 Copias de seguridad** automatizadas de los activos empresariales.
- **11.3 Proteja** los **datos de recuperación** con controles equivalentes a los datos originales.
- **11.4** Establecer y **mantener** una **instancia aislada** de datos de recuperación.



Concientización y **capacitación** en **seguridad**

Migesa | Microsoft Solutions

CLEAR LINES OF RESPONSIBILITY

- **14.1 Concientización** sobre **seguridad.**
- **14.2 Capacita**r para reconocimiento de **ataques** como el **phishing.**
- **14.3 Capacitar** mejores prácticas **autenticación.**
- **14.4 Capacitar** para identificar, almacenar, transferir, archivar y destruir **datos confidenciales.**
- **14.5 Capacitar** exposición involuntaria a los datos.
- **14.6 Capacitar** para **reconocer incidentes.**
- **14.7 Capacitar** sobre verificación de **actualizaciones** de **software**.
- **14.8 Capacitar** sobre los **peligros** de **conectarse** y para configurar de forma segura la red doméstica.

Migesa BeProductive® Security Adoption	*Capacitación extensiva para todos los usuarios con plan de comunicación, convocatoria y varios horarios para lograr la mayor participación.* ***Contenido:*** • *Mejores prácticas de Seguridad Informática* • *¿Cómo prevenir el robo de contraseñas?* • *Manejo de información confidencial en la Organización* • *Protección, clasificación y administración de la información* • *Phishing y Malware*

Migesa®

Microsoft
Solutions

¡Gracias!