PERÚ Ministerio de Comercio Exterior y Turismo

prom perú

Ruta Exportadora

Seminarios Miércoles del exportador

Ciberseguridad en el Comercio Exterior

Lima, 10 de septiembre de 2025

VIGILANTIUM

Índice

1 Panorama local y mundial de la Ciberseguridad

"El cibercrimen mueve casi el 'doble' que el tráfico de armas, drogas y personas juntos".

Secure&IT, 2023

Risk categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

2 years

1st	Misinformation and disinformation
2nd	Extreme weather events
3rd	Societal polarization
4th	Cyber insecurity
5th	Interstate armed conflict
6th	Lack of economic opportunity
7th	Inflation
8th	Involuntary migration
9th	Economic downturn
10th	Pollution

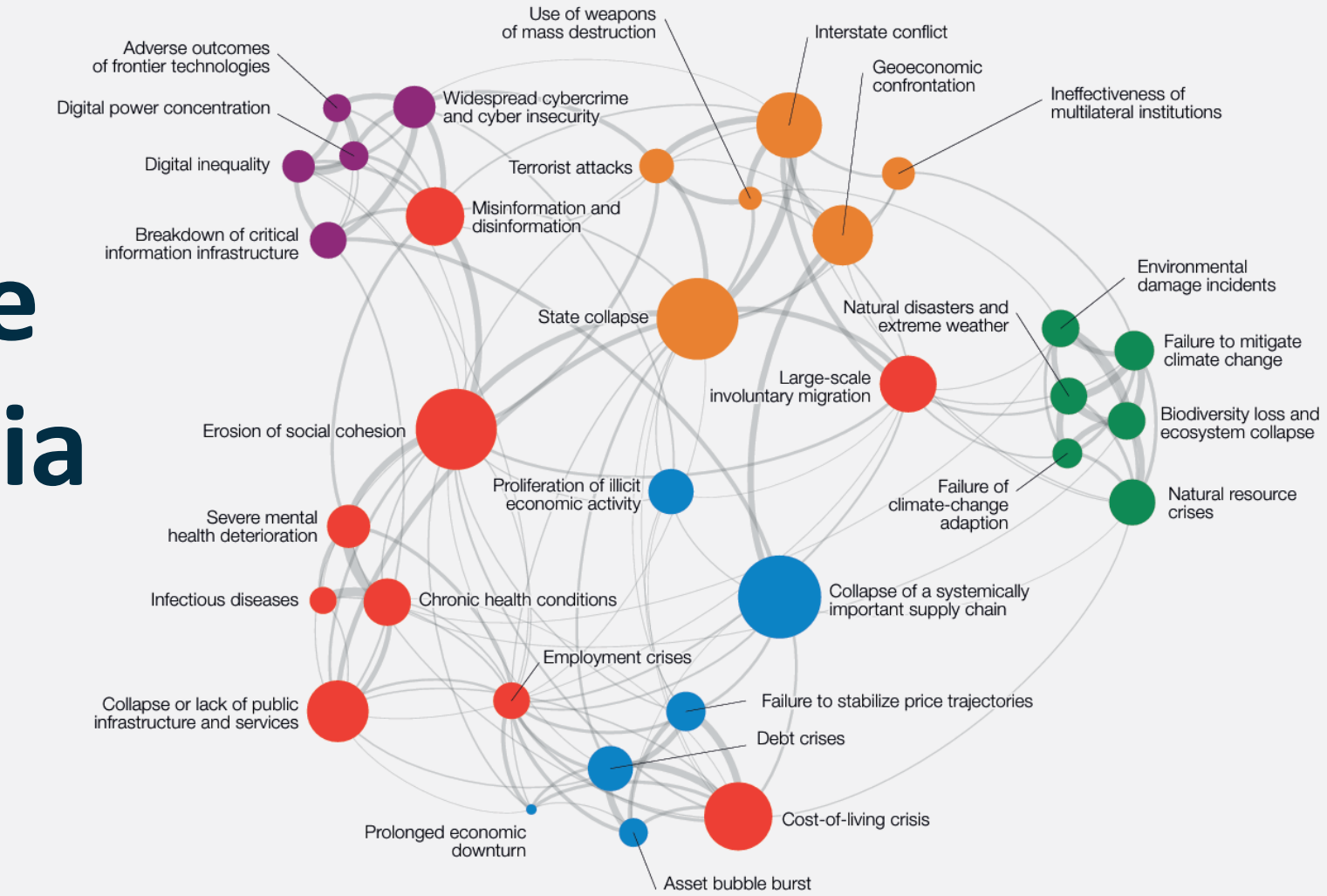
10 years

1st	Extreme weather events
2nd	Critical change to Earth systems
3rd	Biodiversity loss and ecosystem collapse
4th	Natural resource shortages
5th	Misinformation and disinformation
6th	Adverse outcomes of AI technologies
7th	Involuntary migration
8th	Cyber insecurity
9th	Societal polarization
10th	Pollution

Source

World Economic Forum Global Risks Perception Survey 2023-2024.

Mapa de influencia



Ciberataques en el mundo

+ 1 Millón de delitos Cibernéticos reportados en el Perú

Fuente: La República, 2024

Impacto mundial

Global: $24 Trillones al 2027

WTW, 2023

Alemania: $262 Mil Millones

Bloomberg, 2020

Latam: $90 Mil Millones

BID, 2020

Perú: $400 Millones

Esset, 2020

Perú, Julio 2025

Instituto Superior Pedagógico Indoamérica

Trujillo, S/ 1.3 Millones robo cibernético

Gobierno Regional de Cajamarca

Cajamarca, S/ 300 Mil robo cibernético

Municipalidad Distrital de Yura

Arequipa, S/ 1.5 Millones robo cibernético

UGEL, Caylloma

Arequipa, S/ 130 Mil Fraude cibernético

Ciberataques

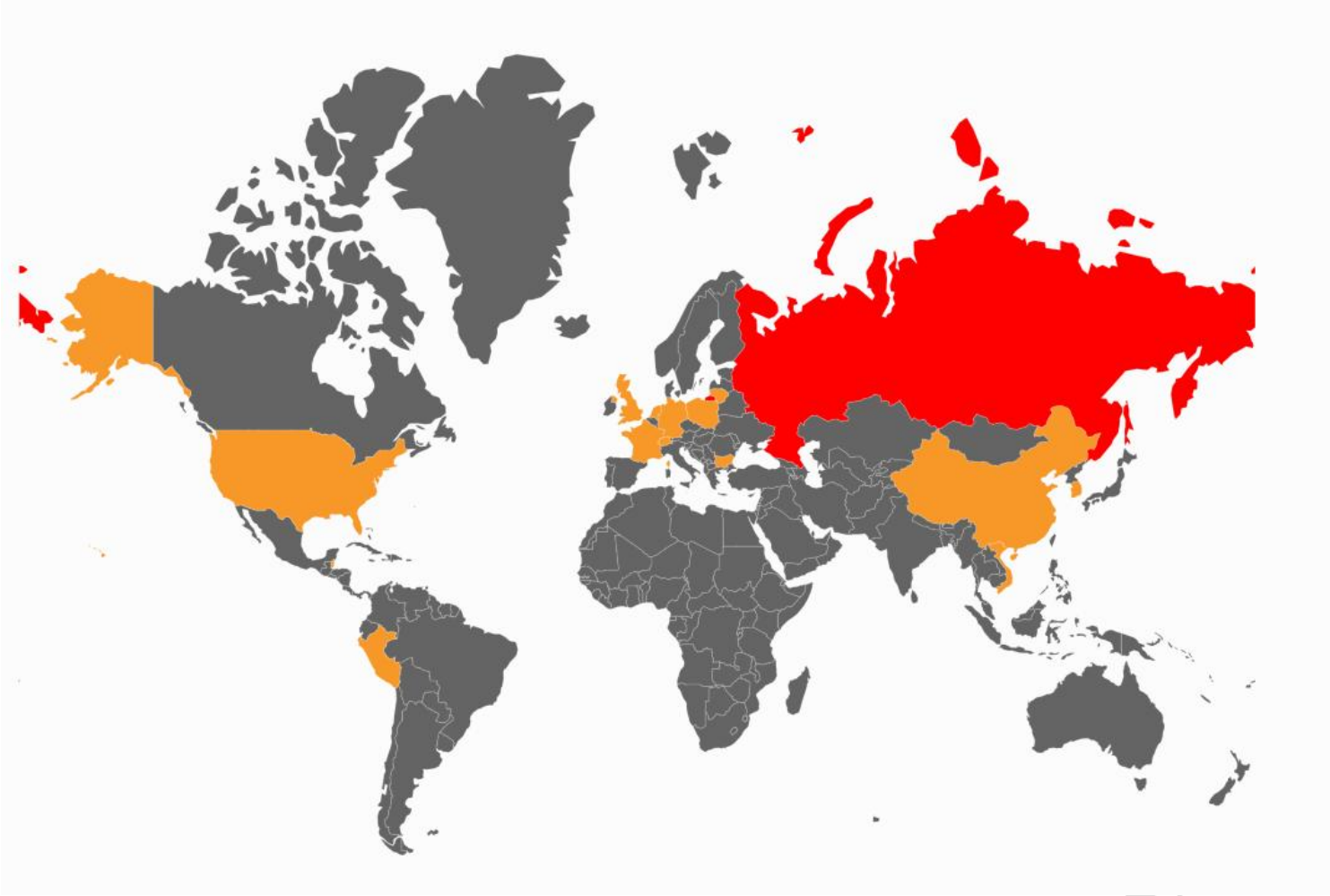
Perú recibe 32 Millones de Ciberataques al día. Si no conoces estas respuesta, tu compañía puede ser la próxima víctima:

¿Cuántos ciberataques recibe tu compañía? ¿De qué tipo son? ¿De donde provienen? ¿Qué servidores y colaboradores están siendo atacados? ¿Cuáles son tus vulnerabilidades? ¿Cuándo fue la última vez que hiciste una evaluación de Ciberseguridad?

19.6K
Russian Federation

943
Mexico

188
France

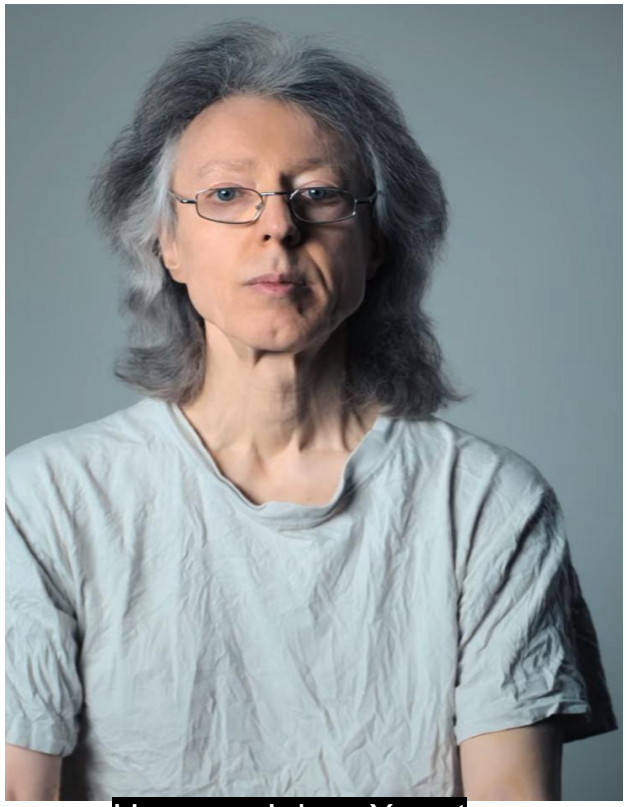


PERÚ Ministerio de Comercio Exterior y Turismo

2 Ciberataques en vivo

EN VIVO

Cibercriminales



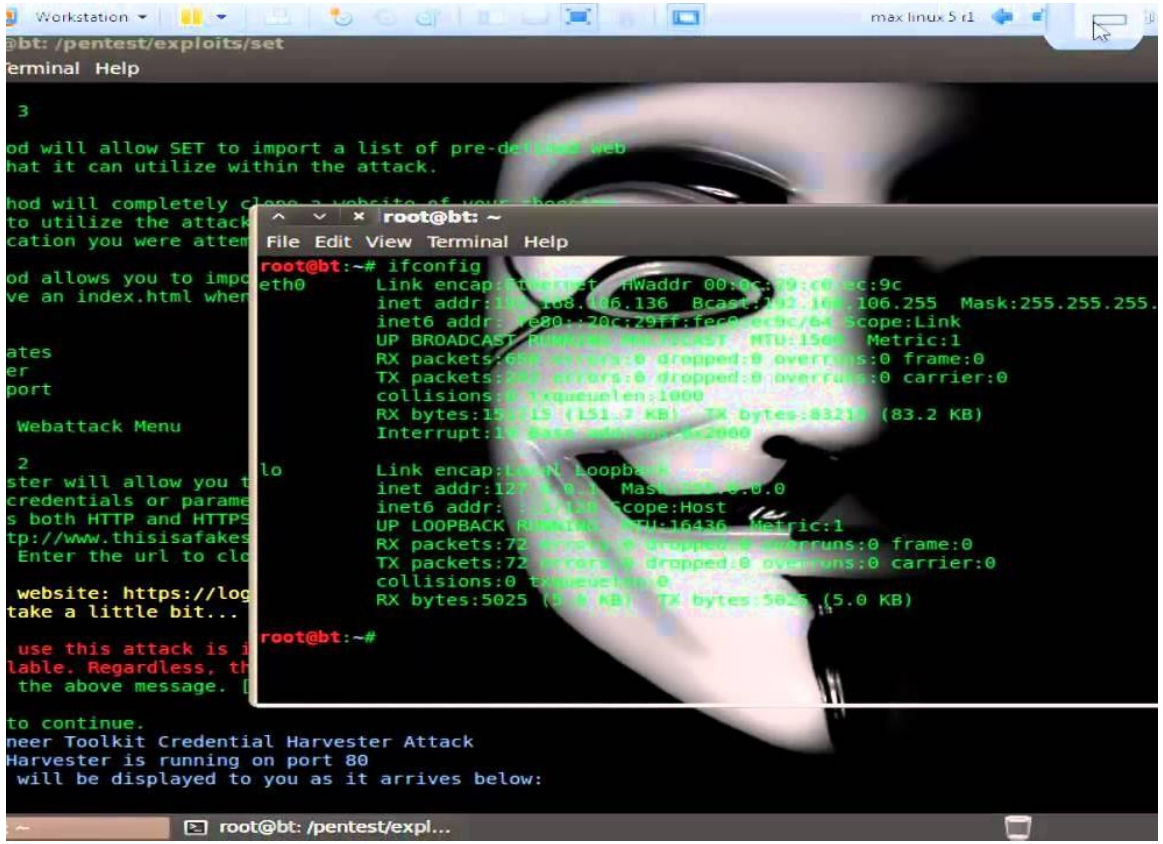
Herman-Johan Xennt

“Si el cibercrimen fuera un país, sería la ‘tercera’ Economía mas Fuerte del mundo”.

CISCO, 2022

¿Cuánto cuesta?

+ Daños a los sistemas y Datos
+ Extorsión
+ Costos de recuperación y mitigación
+ Servicio de análisis forense
+ Servicio de protección
+ Gastos urgentes de tecnología
+ Costo legales
+ Sanciones o Multas
+ Daño reputacional
+ Pérdida de clientes



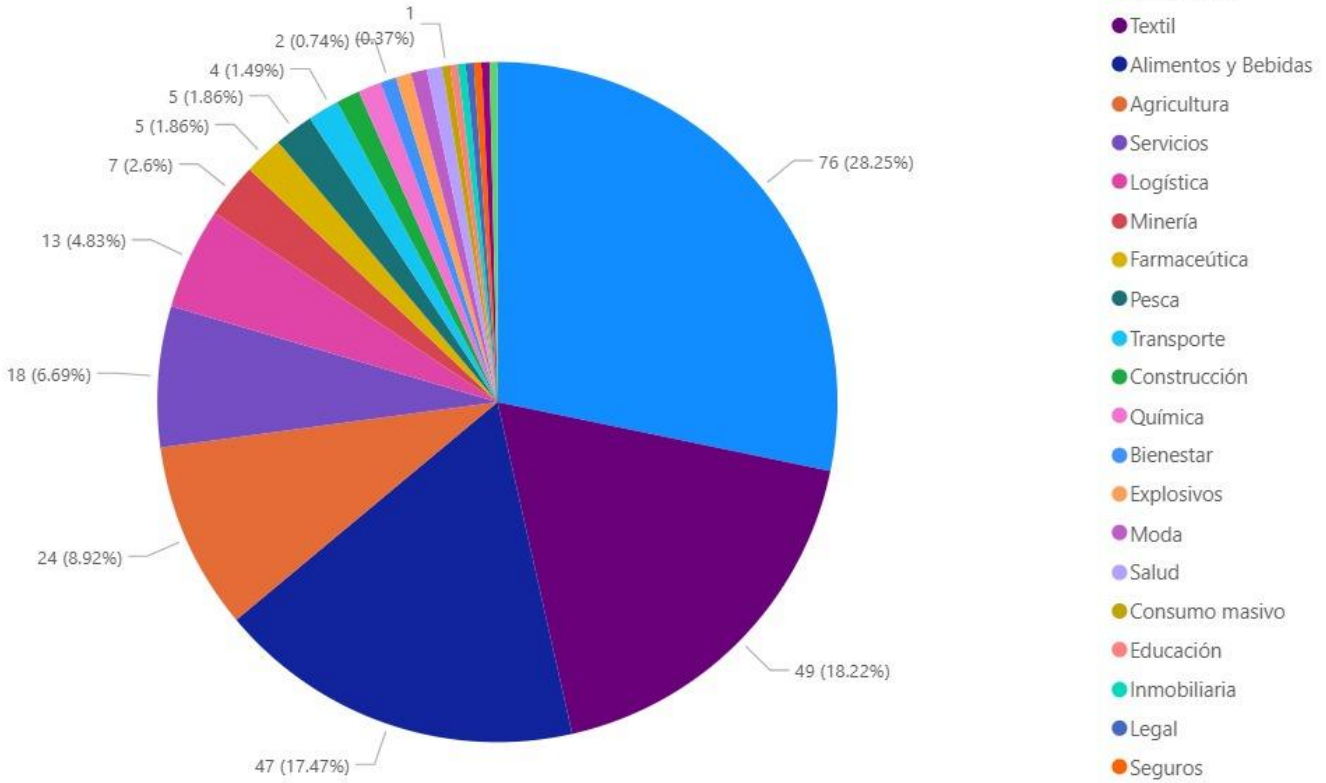
3 Ciberseguridad en las empresas de exportación

Estudio

Estudio sobre 269 Sitios Web de 115 empresas realizado entre Enero y Julio del 2025.

El sector de Manufactura cuenta con mayores riesgos cibernéticos, seguido por Textil, Alimentos y Bebidas, y Agricultura.

Fuente: ADEX CONSULTING Y VIGILANTIUM, 2025

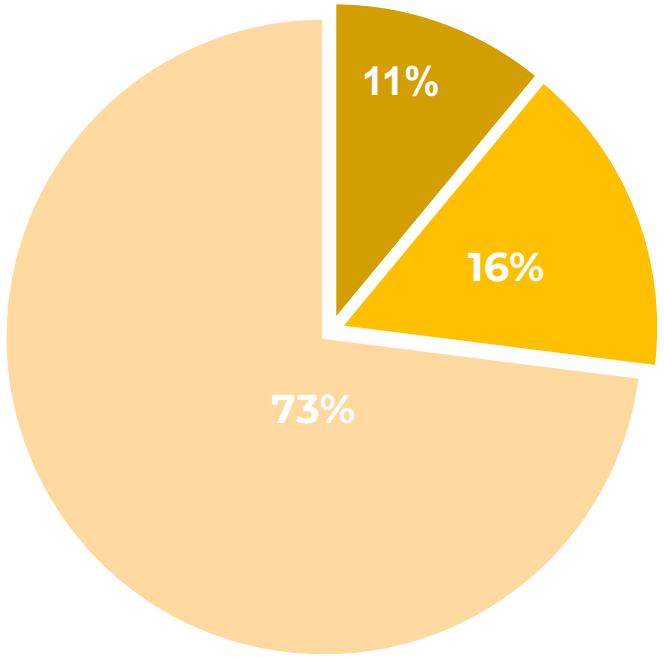


Críticas

25 Empresas cuentan con 62 vulnerabilidades críticas que requieren atención inmediata porque compromete la seguridad total del sitio y posiblemente de la compañía.

Fuente: ADEX CONSULTING Y VIGILANTIUM, 2025

Riesgo de intrusión
Vulnerabilidad: Remote Code Execution (RCE)



Riesgo de datos y reputación
Vulnerabilidad: OpenSSL 3.0.0 < 3.0.15

Riesgo reputacional
Vulnerabilidad: Software sin soporte vigente

Hallazgos

89 empresas cuentan con vulnerabilidades comunes:

85 empresas
Expuestas a robo de datos sensibles, afectando reputación y confianza. *Vulnerabilidad: HSTS Missing from HTTPS Server (RFC 6797)*

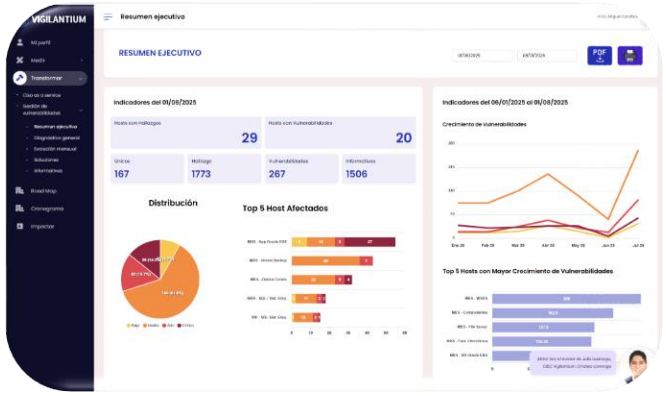
81 empresas
Cuenta con una Web que puede ser manipulada, engañando así al visitante, que podría descargar un archivo malicioso al hacer click en un botón. *Vulnerabilidad: Clickjacking*

61 empresas
Tienen una Web que facilita el robo de contraseñas almacenadas en el navegador, comprometiendo datos y credenciales. *Vulnerabilidad: Web Server Allows Password Auto-Completion*

Fuente: ADEX CONSULTING Y VIGILANTIUM, 2025

4 Casos de estudio

Manufactura



Antecedentes

- Empresa con 50 años, factura $70 millones al año
- 300 Colaboradores, 2 plantas en Perú y oficinas comerciales en 5 países
- Servicio de seguridad gestionada contratado
- Incidente secuestró el acceso a sistemas y datos
- Backup encriptado
- Hacker solicitó $250 mil dólares por el rescate
- Restauraron un backup con 6 meses de antigüedad
- Afectó la continuidad del negocio, el flujo de caja y la moral de los colaboradores de la compañía

Diagnóstico

- Carecía de seguridad a pesar de tener contrato
- Reportaba muchos eventos críticos
- 3500 ciberataques al mes.
- 351 vulnerabilidades en 17 servidores
- 02 servidores afectados con un malware
- Políticas y configuraciones débiles en servidores de correo, BD, Sistemas, Usuarios, antivirus, en la red y en el firewall.
- Personal no estaba preparado y podía ser engañado por un ataque de correo. 33 (11%) personas cayeron en la simulación de ataque descargando un falso malware.

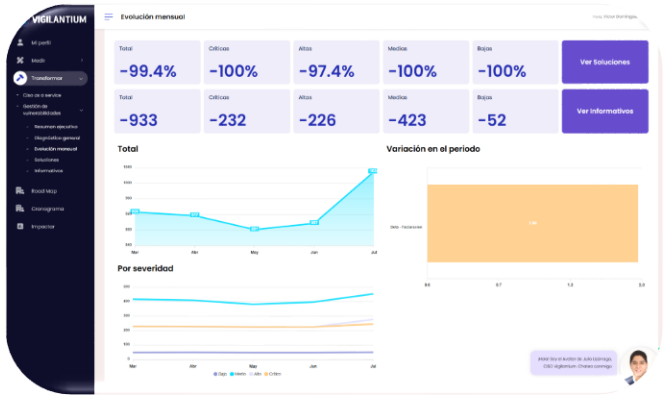
Resultados

- Apoyo completo desde la alta gerencia
- Personal sensibilizado, capacitado y fortalecido
- 50% de sus brechas reducidas en un mes y 89% en 6
- 90% de reducción en ciberataques
- Gestión permanente de sus vulnerabilidades y amenazas
- Reducción del riesgo cibernético en $5 Millones de dólares
- Evidencias permanente de una mejora integral
- Los sistemas y la tecnología optimizada y con mayor productividad
- Gestión y control de su Ciberseguridad y Riesgos

Agroexportación

Antecedentes

- Empresa líder en la agro exportación
- 3 mil usuarios con correo y acceso a sistemas
- Navegación internet muy lenta
- Habían tenido un incidente 2 años atrás
- Contrato con un proveedor de seguridad gestionada
- Sin embargo, tenían desconocimiento total de cuál era la situación real de la ciberseguridad de la empresa



Diagnóstico

- La plataforma detectó 264 vulnerabilidades
- Se identificó 16 eventos de severidad crítica
- 6,900 ataques al mes de diversos tipo: Masivos, Escaneo de puertos y de rompimiento de contraseñas
- Personal no estaba preparado y podía ser engañado por un ataque de correo. 300 personas cayeron en la simulación de ataque descargando un falso malware.
- Carecía de seguridad a pesar de tener contrato de seguridad

Resultados

- Apoyo completo desde la alta gerencia
- Personal sensibilizado, capacitado y fortalecido
- 80% de sus brechas reducidas en 03 meses
- 85% de reducción en ciberataques en 01 mes
- Gestión permanente de sus vulnerabilidades y amenazas
- Fortalecimiento de la seguridad de los servidores, aplicaciones, estaciones de trabajo y colaboradores
- Evidencias permanente de una mejora integral
- Reducción del riesgo cibernético en $5 Millones de dólares

5 Riesgos en las empresas de Exportación

Riesgos

Resultado del estudio realizado sobre los Sitios Web y Sistemas públicos de 115 empresas del sector exportación.

Robo de credenciales y accesos

16% de las empresas son vulnerables a accesos no autorizados y al robo de contraseñas. *Vulnerabilidad: OpenSSL 3.0.0 < 3.0.15*

Filtración, Manipulación y secuestro

11% de las empresas están expuestas a un ataque en que pueden acceder a datos, robar información sensible, manipularla y/o usarla para extorsión o venta.

Extorsión y costos financieros

73% de las empresas están vulnerables a un ataque de Ransomware ocasionando fallos críticos o detenimiento de operaciones claves sostenidas por los sistemas que han sido encriptados y exigen el pago de un rescate para liberar la información.

Fuente: ADEX CONSULTING Y VIGILANTIUM, 2025

Riesgos

Interrupción del negocio

73% de las empresas pueden verse seriamente afectadas por interrupciones en sus sistemas, base de datos, correo, etc. Por lapsos de 12 a 72 horas, lo que ocasionaría pérdidas económicas significativas.

Daño a la reputación y marca

11% de las empresas tienen riesgo de verse afectada por un daño a la reputación y a la marca debido a manipulación o suplantación de identidad del sitio Web y/o sistema. Quienes visiten la Web o aplicación se verían afectados por el robo de datos o de descargar Malware en sus equipos. La confianza y credibilidad de la empresa se vería seriamente afectada.

Multas y sanciones

73% de las empresas están expuestas a multas y sanciones al verse afectada por filtración de datos así como por la falta de políticas y procedimientos claro en el tratamiento de los datos personales de acuerdo a la Ley de Protección de Datos Personales.

Fuente: ADEX CONSULTING Y VIGILANTIUM, 2025

¿Cómo iniciar?

Autoevaluación

- ¿Cuántos ciberataques recibe tu compañía?
- ¿De qué tipo son?
- ¿De donde provienen?
- ¿Qué servidores y colaboradores están siendo atacados?
- ¿Cuáles son tus vulnerabilidades?
- ¿Cuándo fue la última vez que hiciste una evaluación de Ciberseguridad?

Si conoces estas respuesta, puedes convertirte en la próxima víctima.

Recomendaciones

Transformar

Concéntrese en su negocio, apóyese de expertos.
Acompañamiento en la remediación y evidencias de mejora.

Medir

Lo que no se mide, no se puede gestionar.
Auditoría, Detección de vulnerabilidades de servidores, aplicaciones y colaboradores.

Impactar

Un usuario capacitado es una gran defensa.
Capacitación y sensibilización

Beneficio

Por asistir, descarga un informe de vulnerabilidades gratuito y accede a una cita gratuita de 30 minutos para evaluar tu ciberseguridad

Seminarios Miércoles del exportador

Preguntas y respuestas

Cesar Ramirez

Gerente General de Vigilantium

VIGILANTIUM