Consideraciones de Ciberseguridad en el 2022+

Ing. Eli Faskha
Soluciones Seguras

20 AÑOS
SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

experiencia
y trayectoria

experiencia

20 años de experiencia en el Mercado de ciberseguridad

conocimiento

Equipo completo de Ingenieros **Entrenados y Certificados**

reconocido

Múltiples premiaciones de fabricantes y distribuidores

Great Place To Work.

presencia

Con oficinas en **4 países** de Latinoamérica

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Nuestra Misión: Ser la primera alternativa en ciberseguridad para las empresas y organizaciones de todos los sectores económicos de Centroamérica.

El Salvador
Colonia Escalón, San Salvador

Guatemala
Boulevard Los Próceres, Guatemala

Panamá
Clayton, Ciudad del Saber

Costa Rica
San Rafael de Escazú, San José

Presencia Regional

SOLUCIONES SEGURAS
20 AÑOS
Empresas Protegidas, Empresas Tranquilas

EMPRESAS PROTEGIDAS, EMPRESAS TRANQUILAS

externa

Protección contra amenazas en el perímetro, seguridad móvil y estaciones de trabajo.

interna

Protección contra amenazas internas que buscan exfiltrar datos y/o afectar servicios o aplicaciones.

monitoreo

Soluciones de gestión y monitoreo de redes y eventos de su infraestructura TI.

datos

Soluciones de protección de datos sensitivos en bases de datos y aplicaciones críticas.

cloud

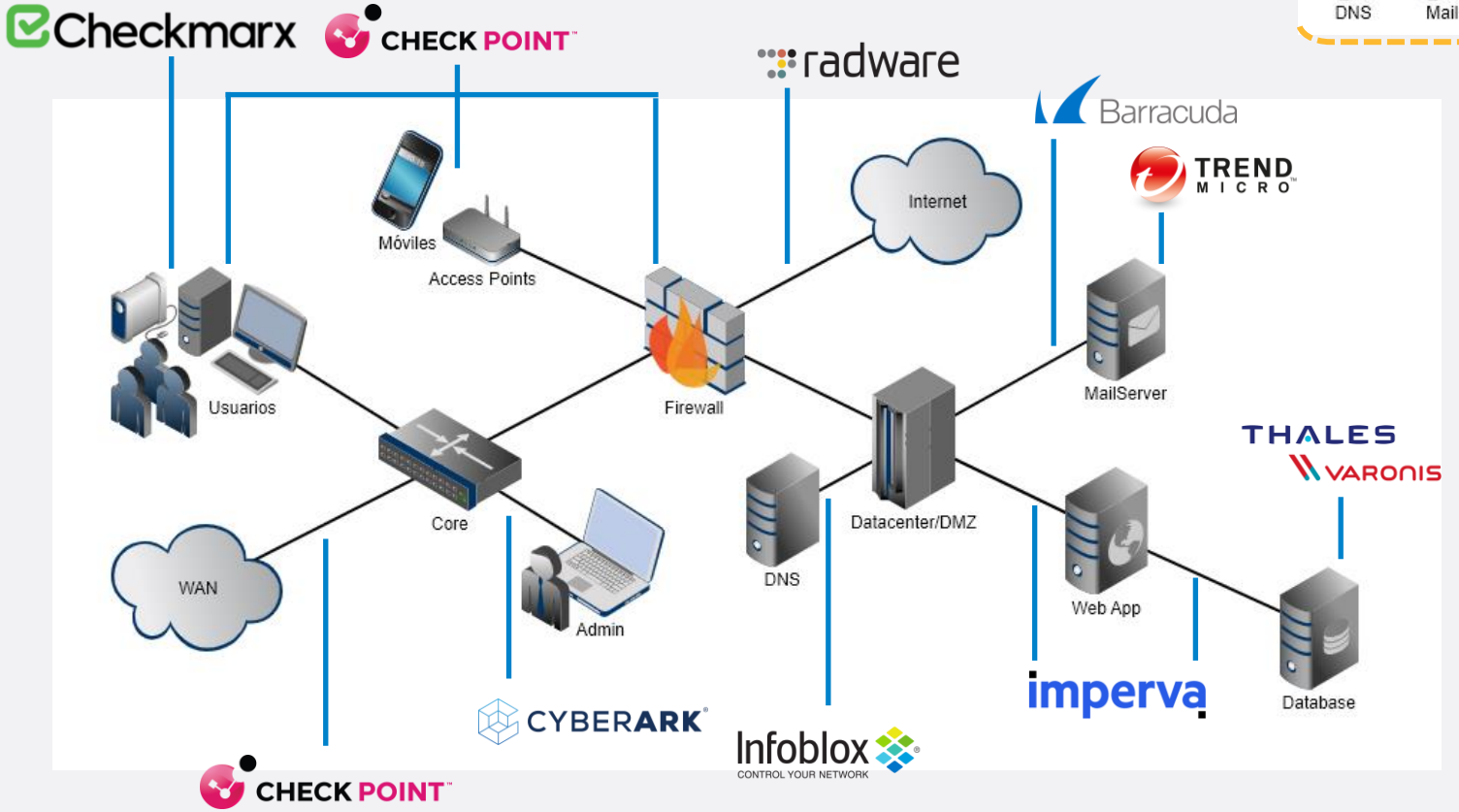
Soluciones de protección Cloud en modalidades IaaS y SaaS.

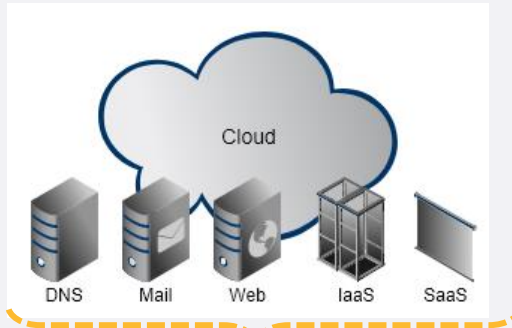
usuarios

Soluciones de protección para el usuario móvil y trabajador remoto.

seguridad de red
en todas partes

RAPID7
FORESCOUT
indeni
DARKTRACE
Progress
SMARTFENSE HARDENING DE USUARIOS
LUMU



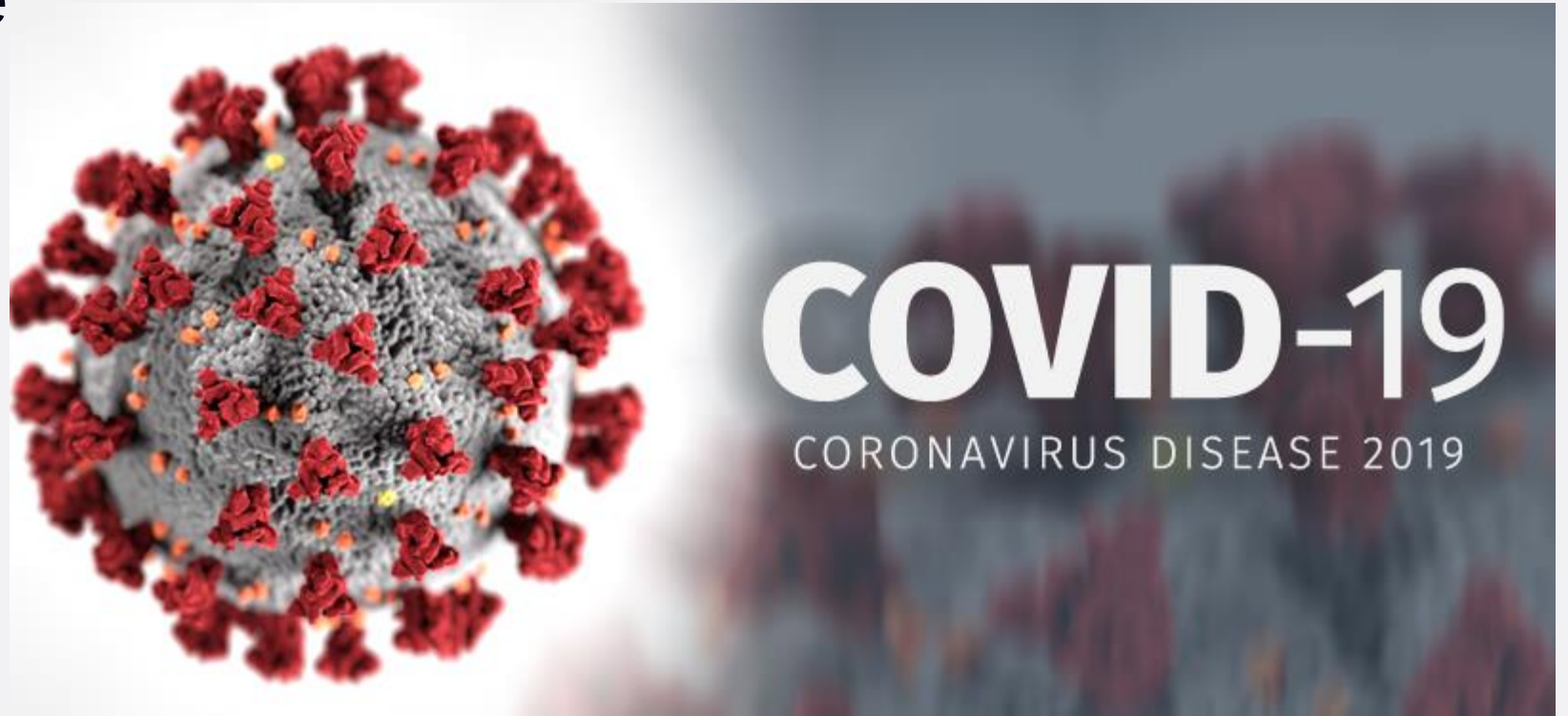


CHECK POINT
radware
imperva
CYBERARK
Barracuda
TREND MICRO
RAPID7
Infoblox
CONTROL YOUR NETWORK

SOLUCIONES SEGURAS
20 AÑOS
Empresas Protegidas, Empresas Tranquilas

La Pandemia COVID-19

- La pandemia forzó a las empresas a depender de
  - Transformación digital
  - Teletrabajo
  - E-Commerce
  - Plataformas nube

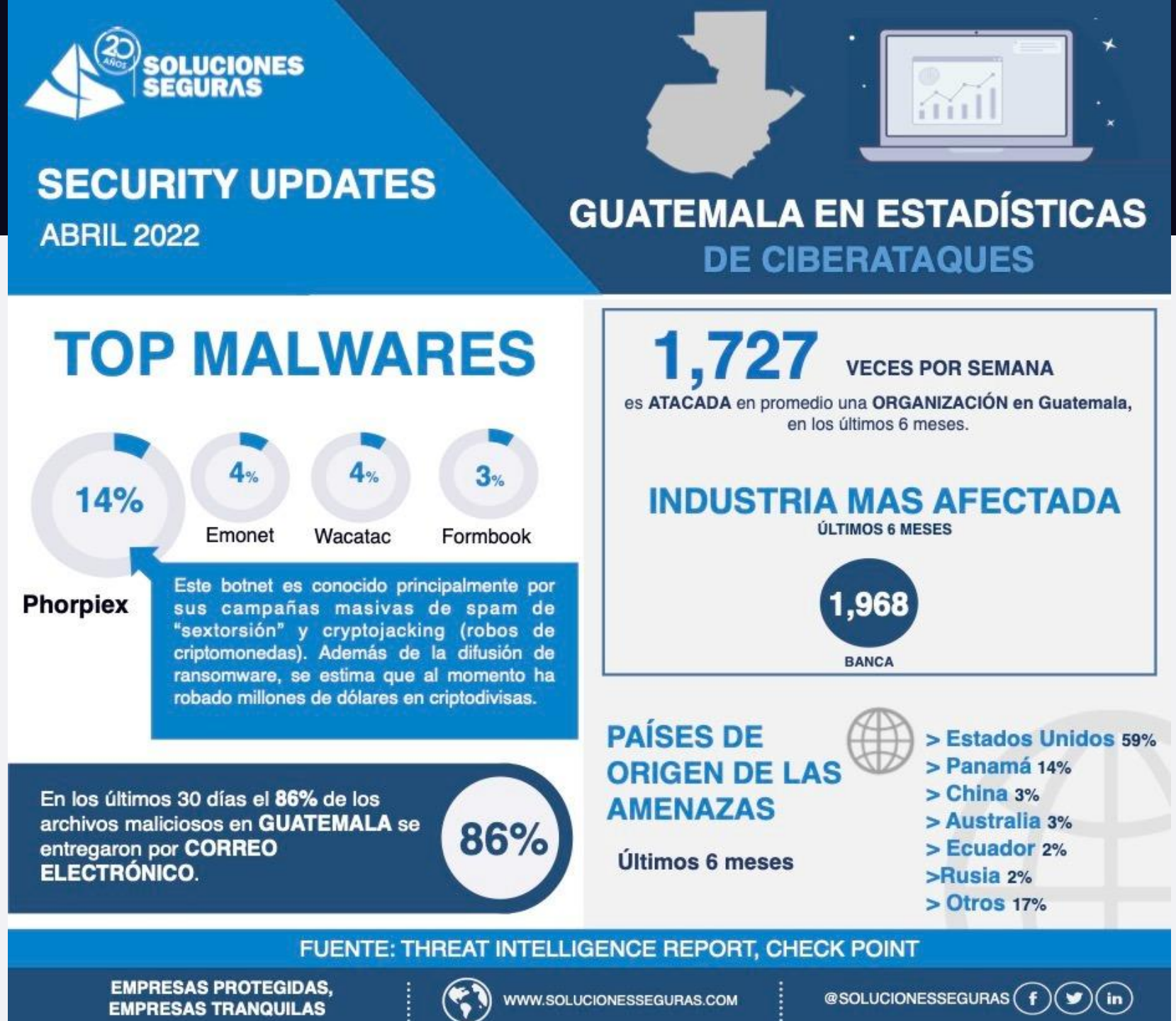


SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Transformación e Innovación Digital

- Un arma de doble filo
  - Necesaria para aumentar el rendimiento y conectividad
  - Expone a las empresas a mayores riesgos de ciberseguridad
- Muchas empresas ven ahora sus debilidades para
  - Detectar
  - Proteger
  - Responder a amenazas
  - Escenarios de continuidad de negocios

El Estado de la Ciberseguridad



SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Consideraciones Geomundiales

- Hay un aumento exponencial de ataques mundiales
- Actualizar y parchar sistemas públicos y software crítico
- Cerrar las puertas de entrada y salida de la red
- Prepararse para Ransomware y para Wipers
- Agilizar los planes de respuesta
- Bloquear IPs

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Una Al Día (31/05/22) El gobierno de Costa Rica bajo ataque de Conti

H

Hispasec | Una Al Día <noticias@hispasec.com>
To Eli Faskha

Reply | Reply All | Forward

Tue 5/31/2022 1:02

If there are problems with how this message is displayed, click here to view it in a web browser.

LinkedIn

+ Get more add-

31/05/22

El gobierno de Costa Rica bajo ataque de Conti

El gobierno de Costa Rica declaro el pasado 8 de mayo el estado de emergencia debido a múltiples ataques del popular ransomware Conti, dichos ataques tenían como objetivos 20 instituciones publicas del gobierno y decenas de perfiles privados de diferentes instituciones.

Costa Rica – Abril 18, 2022

Ministerio de Hacienda de Costa Rica
3 min ·

DTIC

Comunica

En este momento las plataformas Administración Tributaria Virtual (ATV) y TICA se encuentran fuera de servicio. Nuestros equipos técnicos trabajan para su restablecimiento en el menor tiempo posible.

Inmediatamente se solvente la situación, se comunicará por este mismo medio.

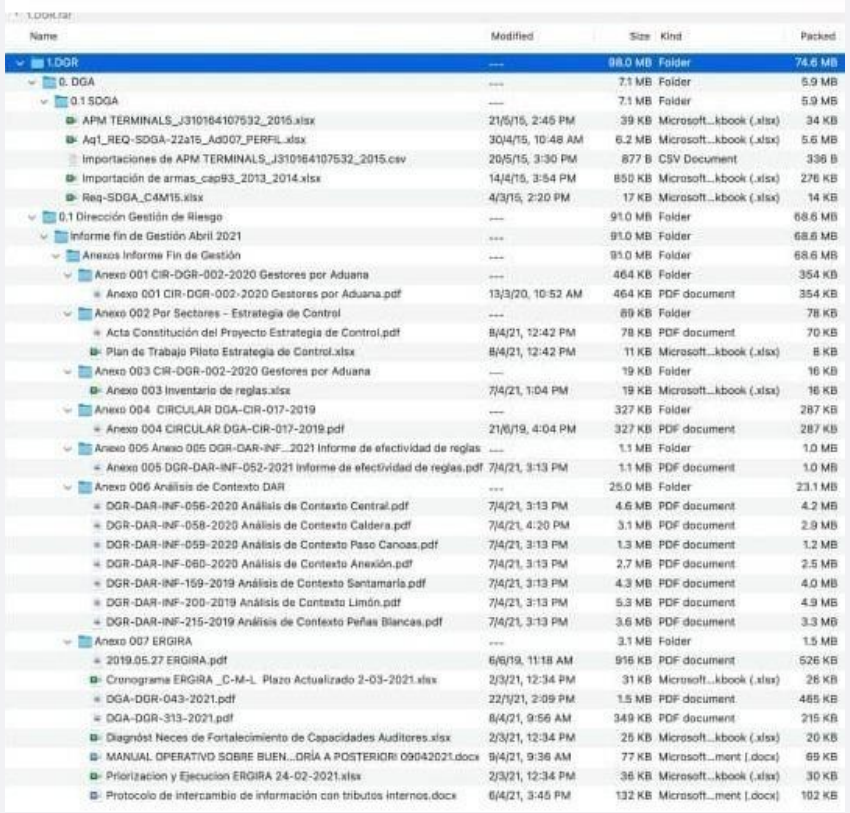
Anonymous-Costa Rica
38 min ·

Saludos pueblo de Costa Rica.

Estos días hemos estado haciendo Pen testing (pruebas de vulnerabilidad) en varias páginas web de Costa Rica, y nos hemos llevado tremendas sorpresas al notar increíbles fallos de vulnerabilidad en páginas del I.C.E, Movistar, AYA, solo por mencionar algunas... y las muchas web básicas que hay de algunas empresas que no tienen ningún método de seguridad, osea que cualquier persona con conocimiento en SQL inyection podría vulnerarlas muy fácil, y ojo que son web que tienen métodos de pago online que es aún más preocupante..
Página web del IMAS, da mucha pena en serio quienes crearon estas web dejaron un portón abierto a los piratas informáticos.

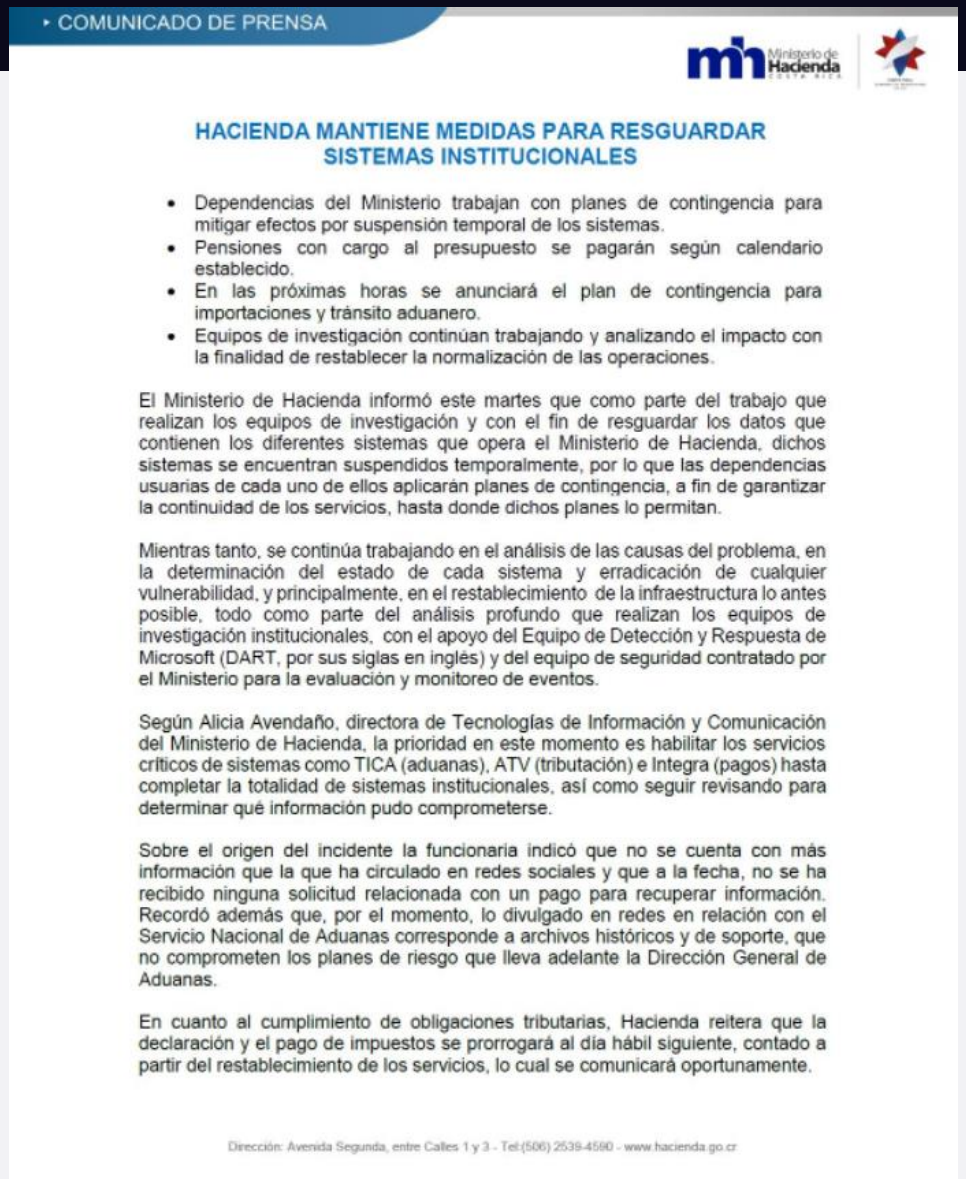
La página de movistar incluso se puede poner el modo usuario en modo administrador y hacer todo lo que se quiera, y ellos ni cuenta se dan..

152 43 comentarios • 10 veces compartido



SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Comunicado de Prensa



COMUNICADO DE PRENSA

Ministerio de Hacienda

HACIENDA MANTIENE MEDIDAS PARA RESGUARDAR SISTEMAS INSTITUCIONALES

- Dependencias del Ministerio trabajan con planes de contingencia para mitigar efectos por suspensión temporal de los sistemas.
- Pensiones con cargo al presupuesto se pagarán según calendario establecido.
- En las próximas horas se anunciará el plan de contingencia para importaciones y tránsito aduanero.
- Equipos de investigación continúan trabajando y analizando el impacto con la finalidad de restablecer la normalización de las operaciones.

El Ministerio de Hacienda informó este martes que como parte del trabajo que realizan los equipos de investigación y con el fin de resguardar los datos que contienen los diferentes sistemas que opera el Ministerio de Hacienda, dichos sistemas se encuentran suspendidos temporalmente, por lo que las dependencias usuarias de cada uno de ellos aplicarán planes de contingencia, a fin de garantizar la continuidad de los servicios, hasta donde dichos planes lo permitan.

Mientras tanto, se continúa trabajando en el análisis de las causas del problema, en la determinación del estado de cada sistema y erradicación de cualquier vulnerabilidad, y principalmente, en el restablecimiento de la infraestructura lo antes posible, todo como parte del análisis profundo que realizan los equipos de investigación institucionales, con el apoyo del Equipo de Detección y Respuesta de Microsoft (DART, por sus siglas en inglés) y del equipo de seguridad contratado por el Ministerio para la evaluación y monitoreo de eventos.

Según Alicia Avendaño, directora de Tecnologías de Información y Comunicación del Ministerio de Hacienda, la prioridad en este momento es habilitar los servicios críticos de sistemas como TICA (aduanas), ATV (tributación) e Integra (pagos) hasta completar la totalidad de sistemas institucionales, así como seguir revisando para determinar qué información pudo comprometerse.

Sobre el origen del incidente la funcionaria indicó que no se cuenta con más información que la que ha circulado en redes sociales y que a la fecha, no se ha recibido ninguna solicitud relacionada con un pago para recuperar información. Recordó además que, por el momento, lo divulgado en redes en relación con el Servicio Nacional de Aduanas corresponde a archivos históricos y de soporte, que no comprometen los planes de riesgo que lleva adelante la Dirección General de Aduanas.

En cuanto al cumplimiento de obligaciones tributarias, Hacienda reitera que la declaración y el pago de impuestos se prorrogará al día hábil siguiente, contado a partir del restablecimiento de los servicios, lo cual se comunicará oportunamente.

Dirección: Avenida Segunda, entre Calles 1 y 3 - Tel:(506) 2539-4580 - www.hacienda.go.cr

Asimismo, debido a que por ahora no es posible ingresar al Facturador Gratuito del Ministerio de Hacienda, disponible en ATV, la Dirección General de Tributación también habilitó el método de contingencia establecido para las personas usuarias de dicho facturador, quienes deberán emitir comprobantes físicos autorizados y, posteriormente, generar y enviar las facturas electrónicas, una vez que el servicio sea reestablecido. Por su parte, las personas contribuyentes que utilicen sistemas privados de facturación podrán emitir normalmente la factura electrónica en sus operaciones, por cuanto el servicio no se ha interrumpido y la recepción de información es segura.

El Servicio Nacional de Aduanas, por su parte está aplicando el plan de contingencia para exportaciones, VEHITUR, descarga de contenedores en depósitos aduaneros y exportaciones terrestres al mercado centroamericano. En las próximas horas se anunciará el plan de contingencia para importaciones y tránsito aduanero.

Unidad de Comunicación Institucional
CP 52 / 19 de abril, 2022

Servicios Caídos

ACLARACIÓN DEL MINISTERIO DE HACIENDA SOBRE COMUNICACIONES EN REDES SOCIALES CALIFICADAS COMO HACKEO

Translate Tweet

6:04 PM · Apr 18, 2022 · Twitter Web App

17 Retweets 32 Quote Tweets 40 Likes

Tweet your reply Reply

Ministerio H... @H... · Apr 18

Replying to @HaciendaCR

En relación con las comunicaciones que han sido detectadas en las redes sociales, y calificadas como hackeo, el Ministerio de Hacienda comunica lo siguiente:

1 7

Ministerio H... @H... · Apr 18

Replying to @HaciendaCR

El Ministerio ha tomado la decisión de permitir a los equipos de investigación realizar un análisis profundo en los sistemas de información, y suspender temporalmente plataformas como ATV y TICA, se estarán reiniciando los servicios una vez que los equipos concluyan sus análisis.

1 3 9

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Caja del Seguro Social CR – Abril 20, 2022

LA NACIÓN Mis Beneficios El País Puro Deporte Sucesos Economía Opinión Viva El Mundo Ingresar

Servicios

CCSS sobre 'hackeo': 'No se extrajo información sensible' ni se afectó EDUS o Sicere

Expediente digital de salud y sistema de recaudación de cuotas se mantienen funcionando con normalidad, luego de vulneración a base de datos de Recurso

Por Ángela Ávalos

20 de abril 2022, 6:00 PM

Los ataques de *hackers* contra las plataformas de la Caja Costarricense de Seguro Social (CCSS) ocurridos desde la tarde del martes, no afectaron información sensible, según aseguró este miércoles Roberto Cervantes, gerente general de la institución.

Una de estos ataques fue contra sus redes sociales, y el segundo contra el portal de Recursos Humanos.

"Producto de este ataque, no se extrajo información sensible ni se afectó ninguna otra plataforma, como EDUS o Sicere, gracias a la detección oportuna que se realizó", aseguró Cervantes en referencia al Expediente Digital Único en Salud y al Sistema Centralizado de Recaudación, que funcionan con normalidad.

Caja del Seguro Social – Mayo 31, 2022

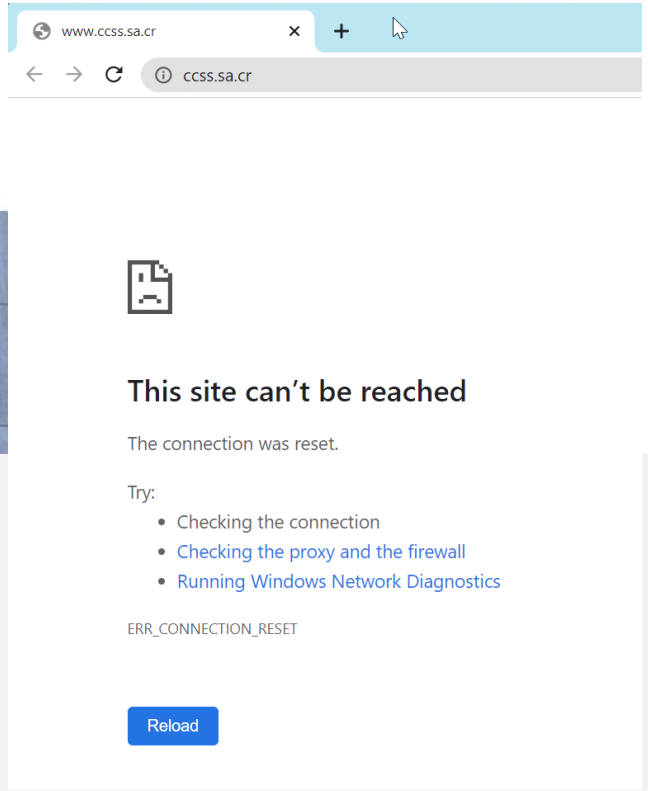
Salud

Nuevo ‘hackeo’ en CCSS la madrugada de este martes

Bases de datos de EDUS, Sicere, planillas y pensiones no se vieron comprometidas, asegura institución, pero se bajaron todos los sistemas de manera preventiva

Por Ángela Ávalos

31 de mayo 2022, 6:08 AM



Cual es el Costo del Daño de un Ataque?

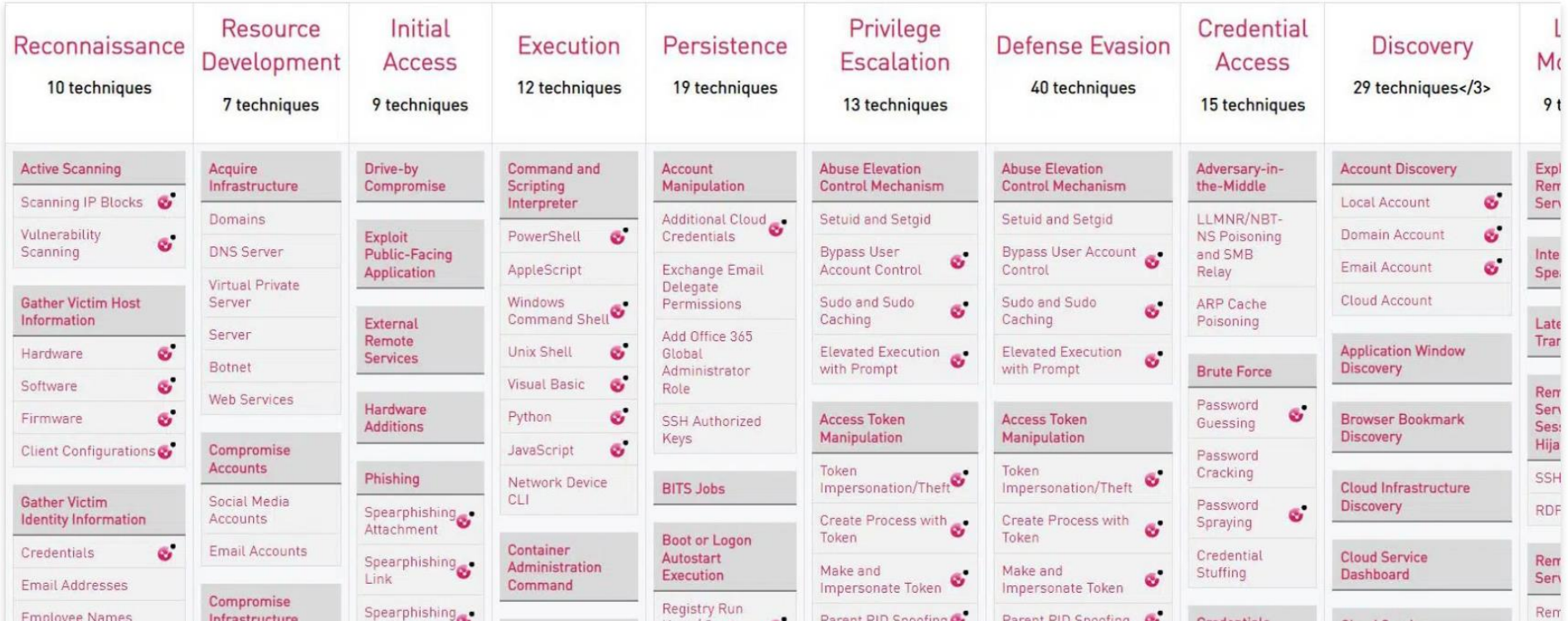
- No importa el costo!!
- En la mayoría de las empresas de la region, un ataque exitoso resulta en
  - Como mínimo: El cierre complete de Operaciones por 3 días o más
  - Pérdida de datos financieros que son difíciles o muy costosos de recuperar
  - Pérdida de la confianza de los clientes
  - Impacto severo en la moral del personal de la empresa
- El costo no es monetario!

Comience Ejercicios de Ciberseguridad Ahora Mismo

- Que harían en caso de
  - Ataque a la página web
  - Ransomware en un equipo de un usuario remoto? O en premisas?
  - Wiper en un equipo en premisas o de un usuario remoto?
  - Robo de credenciales de sus usuarios? De sus clientes?
  - Pérdida de su datacenter?
  - Equipo clave inaccessible?
- Publique internamente expectativas claras y logrables
  - Comunicación esperada
  - Tiempo de recuperación
  - Modo de operación

Check Point Offers the Industry's Widest Coverage of the ATT&CK Enterprise MATRIX

Malicious actors keep finding new techniques to diversify their attacks and cover their tracks. To outpace them, security teams are increasingly using the MITRE ATT&CK™ framework. MITRE ATT&CK™ framework is based on an extensive knowledge base of real-life malicious tactics and techniques, that is continuously updated. To leverage MITRE for better detection and response, Check Point security products are up-to-date with the recent ATT&CK enterprise matrix, offering the industry's widest coverage of tactics and techniques.



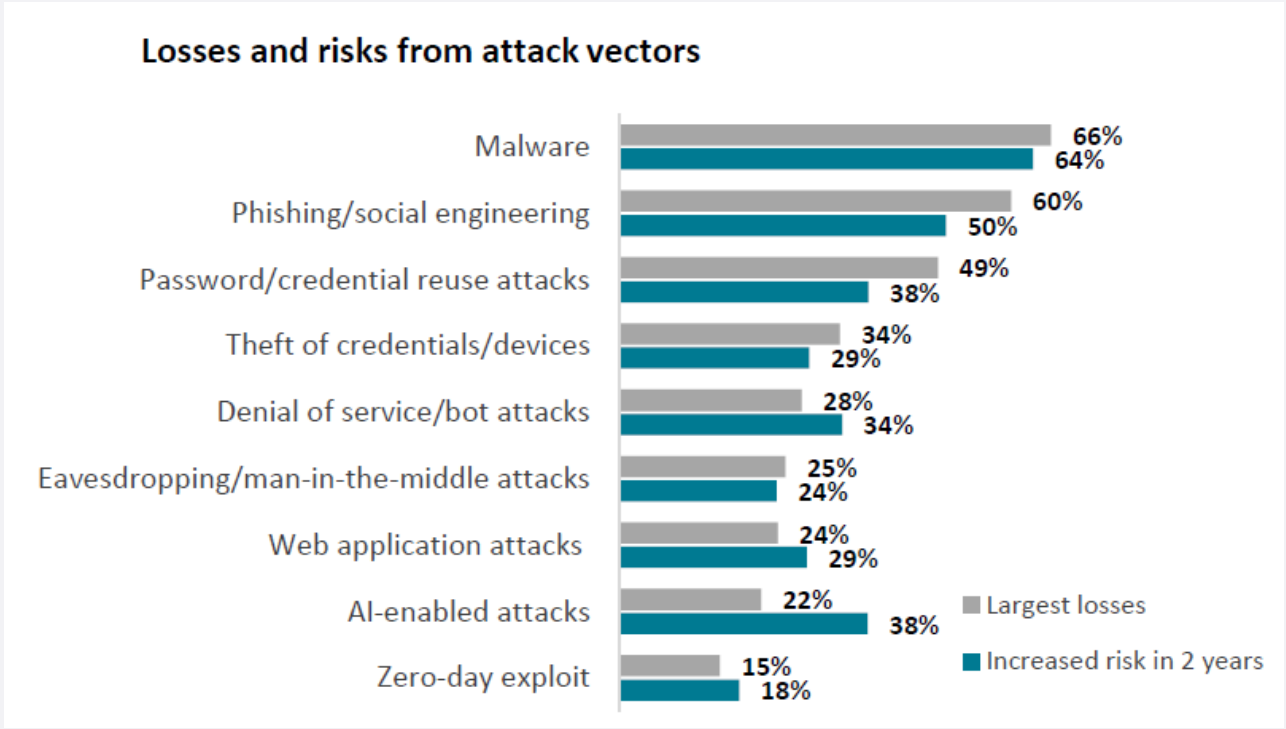
El Estado de la Ciberseguridad

Dónde?
Quién?
Qué?
Cuales?

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

De **Dónde** viene el riesgo?

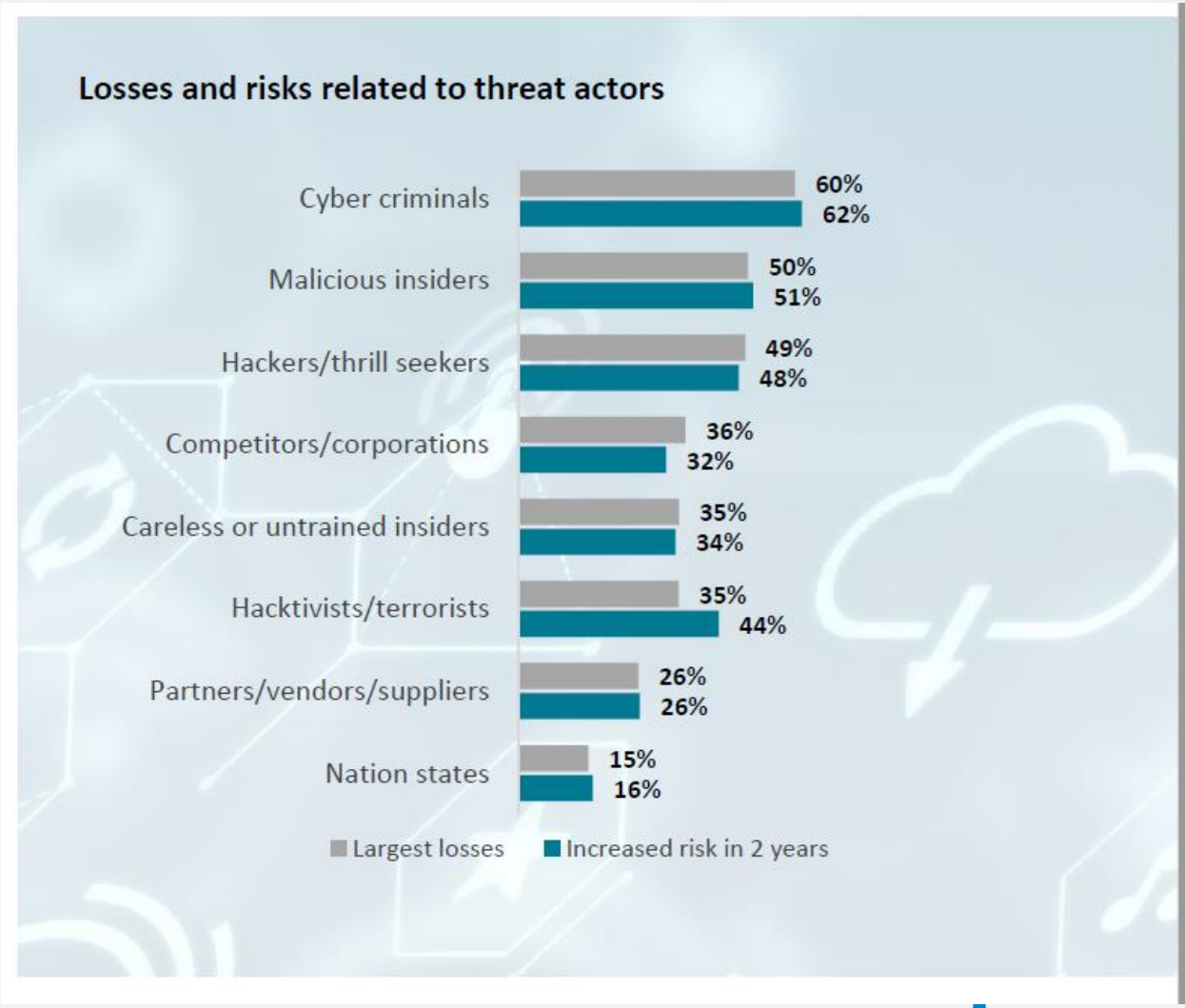
- Malware y Phishing son los responsables de los mayores daños en ciberataques
  - Antes de la Pandemia, igual eran los mayores riesgos
  - La Pandemia exacerbó los riesgos y aumento su potencial impacto
- El aumento en el uso de la tecnología trae consecuencias
  - Ejecutivos esperan un aumento en ataques por DDoS y aplicaciones web
  - El mayor aumento vendrá de ataques basados en inteligencia artificial



SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

De **Quién** viene el riesgo?

- Cibercriminales continuarán causando mayores pérdidas
  - Están mejorando en seleccionar y atacar empresas selectivamente
  - Teletrabajo trae nuevas vulnerabilidades
  - Permite atacar Wifi inseguro y dispositivos personales
- Usuarios internos también pueden causar pérdidas grandes
  - Personas sin entrenamiento son un riesgo alto, aunque en algunas empresas ha disminuido



SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Qué Tecnologías generan el riesgo?

- Plataformas de Código Abierto
- Endpoints (Computadoras y Móviles) propios y empresariales
- Sistemas mal configurados
- Sistemas sin parchar

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Cuales inversiones en tecnología son más efectivas?

- Detección y Protección en el Endpoint
- Tecnología de Decepción
- Protección de la Data
- Securidad de Trabajos en la Nube (Iaas, PaaS)
- Filtrado y monitoreo de Email
- Firewall y Web Filtering

Most effective cybersecurity technology investments

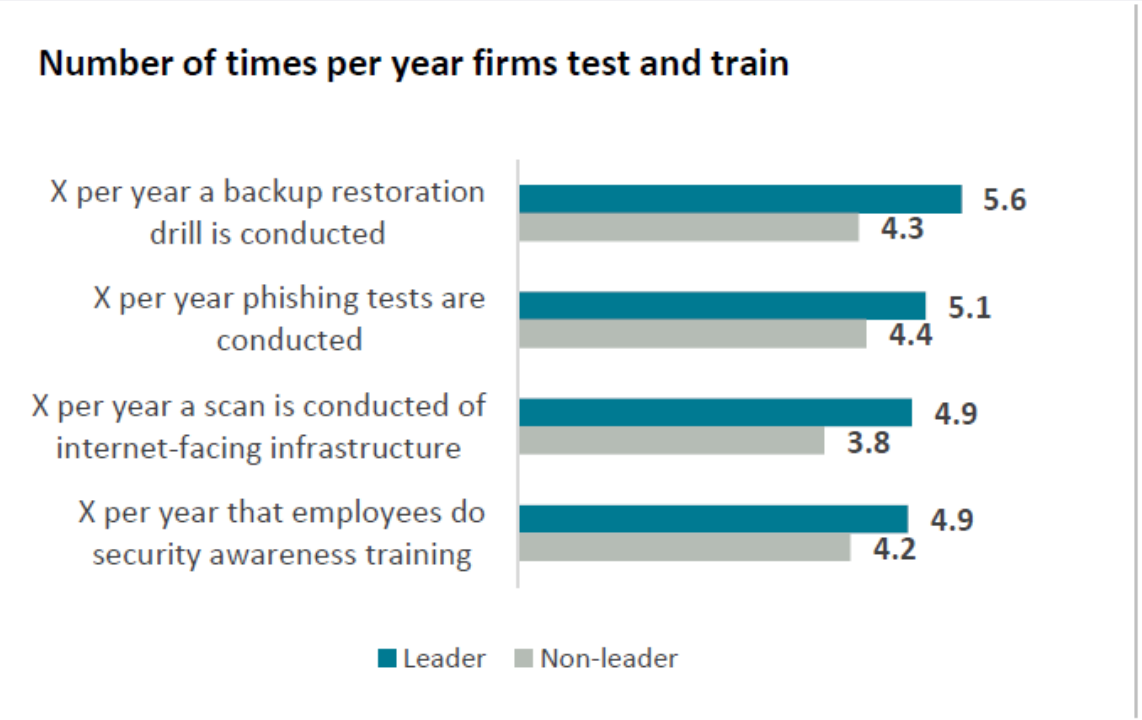
	Leader	Non-leader	Difference
Endpoint detection and protection	83%	59%	24%
Deception technology	82%	59%	23%
Data protection	75%	71%	4%
Security orchestration and automation*	71%	53%	18%
Cloud workload (Iaas, PaaS) security*	70%	46%	24%
Email filtering and monitoring software	69%	57%	12%
Firewalls and web filtering	69%	51%	18%
Mobile device management*	68%	56%	12%
Privileged access management*	68%	48%	20%
Encryption and tokenization*	66%	55%	11%

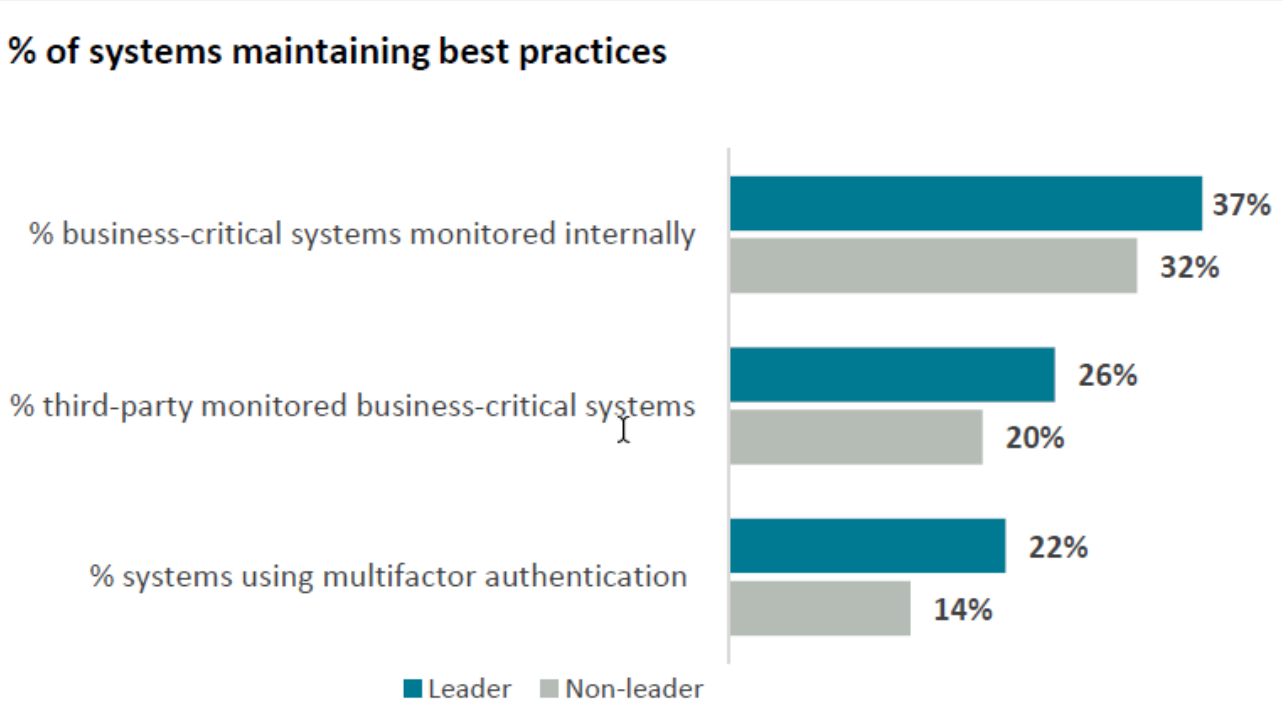
* Technology areas where only 1 in 5 firms are investing significantly

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Ciber Higiene es clave para Disminuir el Riesgo

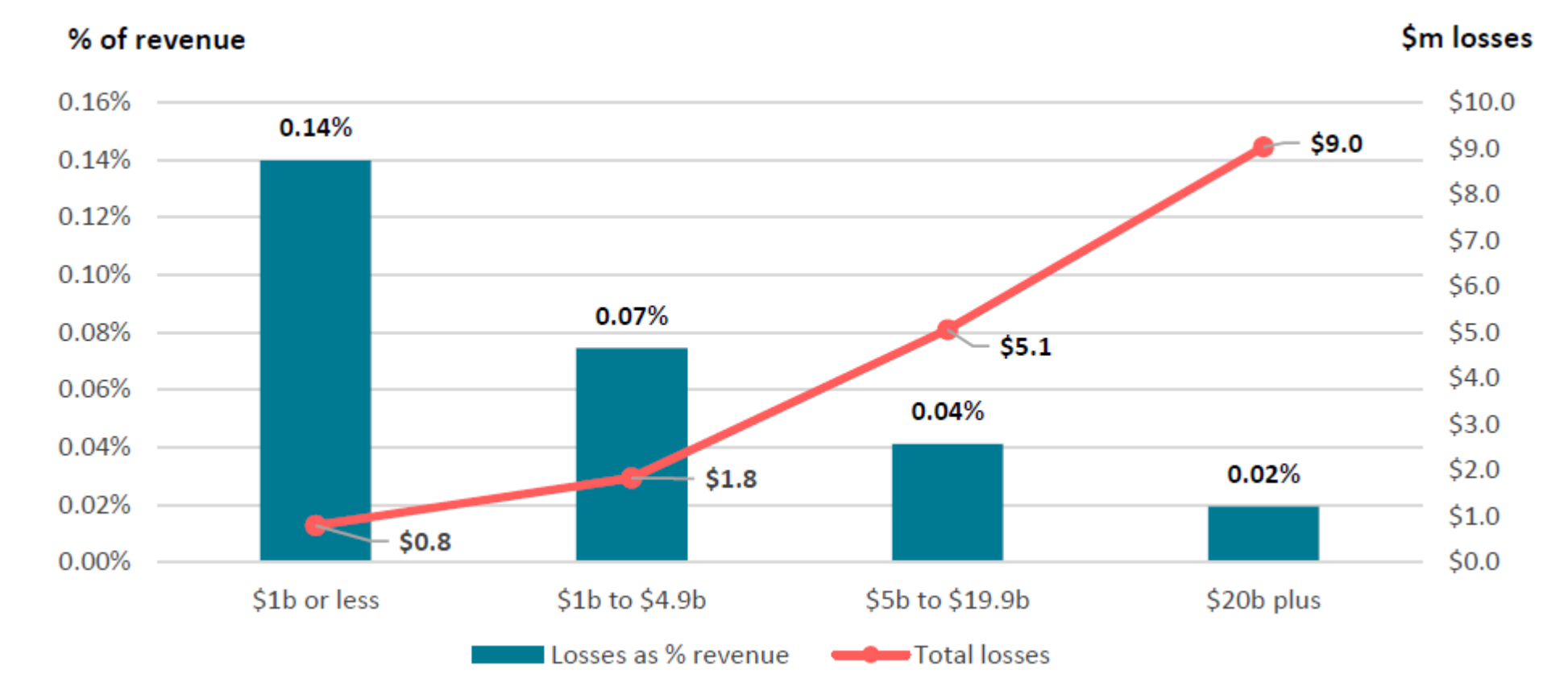
- Restauración de backups
- Pruebas de Phishing
- Scans de Perímetro
- Entrenamiento de Seguridad





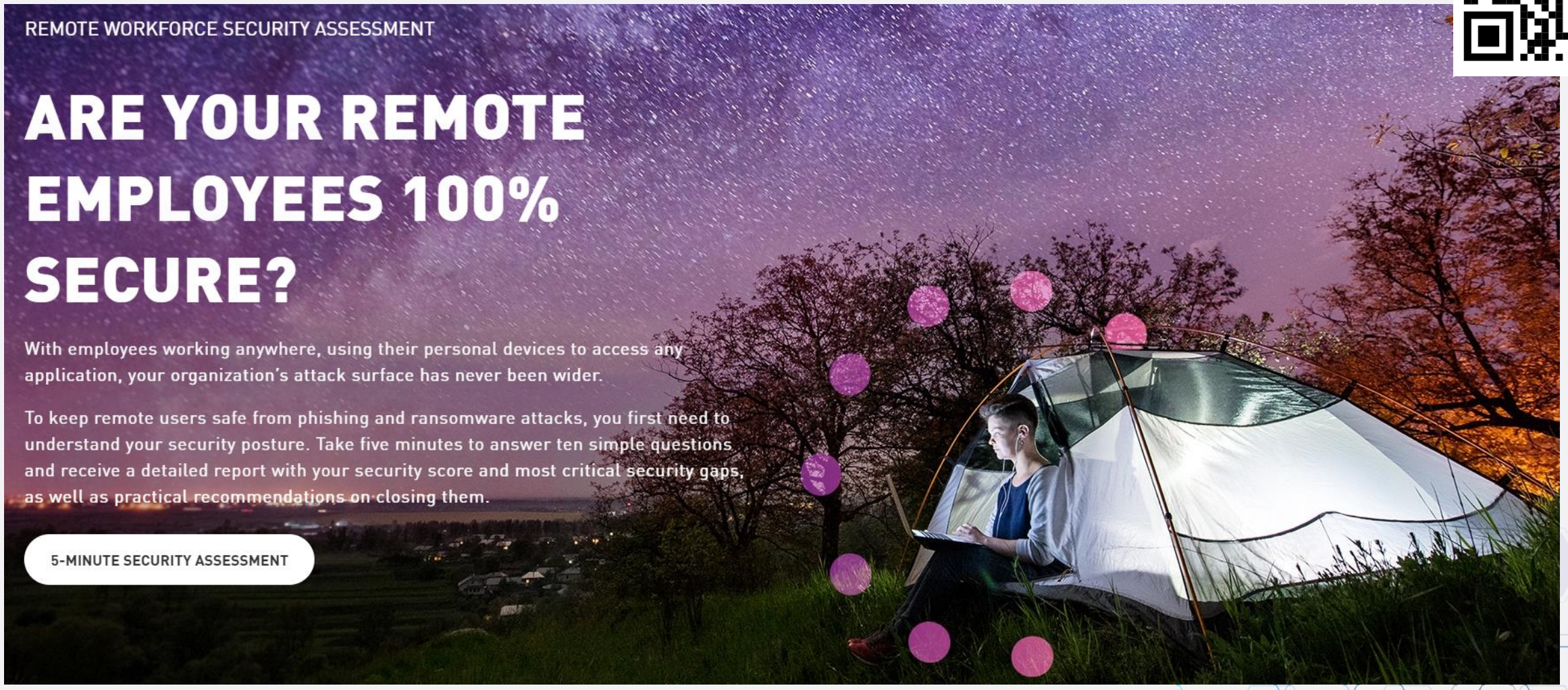
Cual es el daño de un ataque?

- En empresas con ventas de menos de $1 Billón, tiene un promedio de pérdida por incidente de más de $100,000.



SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Asegurando el Teletrabajo



Cómo se permite el acceso a a

Your organization's security policy allows remote access to corporate applications...

choose all that apply

- ☐  From personal mobile devices
- ☐  From personal laptops
- ☐  By third parties (contractors, consultants or partners)
- ☐  From company-managed laptops
- ☐  We do not allow any remote access

Cuales aplicaciones usa su personal?

Pick the applications your company's employees use for corporate email and collaboration

choose all that apply

- ☐ On-prem email (Microsoft Exchange)
- ☐ Office365
- ☐ Gmail
- ☐ Office apps like Teams, SharePoint and OneDrive
- ☐ Google apps like Drive, Docs, Sheets and Meet
- ☐ Other apps like Zoom, Slack and Dropbox

En un ataque de ransomware, puedo:

In the case of a ransomware attack, my organization's endpoint protection can:

choose all that apply

- ☐  Automatically detect and stop the attack
- ☐  Quarantine the infected endpoint
- ☐  Recover ransomware-encrypted files
- ☐  None of the above

Cuantos fabricantes de ciberseguridad us

How many security vendors do you use to secure remote internet access, corporate access, email, endpoint and mobile devices?

- ○  1-3
- ○  4-6
- ○  7-9
- ○  10 and over

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Busque un diagnóstico rápido

Overall security score

Secure	47%
Vulnerable	53%

Email & Office Security

Secure	30%
Vulnerable	70%

Endpoint Security

Secure	30%
Vulnerable	70%

Mobile Security

Secure	100%
Vulnerable	0%

Secure Internet Access

Secure	59%
Vulnerable	41%

Remote Corporate Access

Secure	37%
Vulnerable	63%

Consolidation

Secure	50%
Vulnerable	50%

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Proteger la ‘Oficina’ Remota

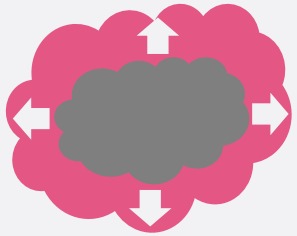
SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Analice la Adopción acelerada de la Nube

- Más servidores están en la nube
  - Mas Proyectos están migrándose a la nube
- Más servicios están en la nube (365, G-Suite, etc.)
  - No se le puede dar Seguridad en premisas a servicios en la nube
- Homologación de Tecnologías
- Defina cuales Proyectos ameritan estar en la nube
- Tenga cuidado con Shadow IT
- Recuerde que casi nunca es un ahorro económico

Consideraciones para la Seguridad de la Nube

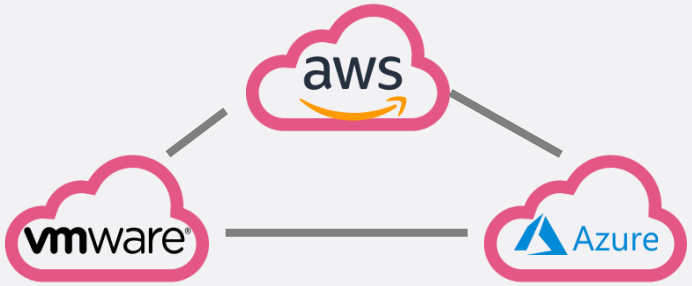
Ambientes en la Nube son Dinámicos



La Seguridad Nube debe...

Dar visibilidad y control para administrar la Seguridad en ambientes dinámicos

La Nube está en Todo Lugar



La Seguridad Nube debe...

Proteger las cargas de trabajo en ambientes híbridos y multi-nube

Desarrollo e implementación ágil de aplicaciones

La Seguridad Nube debe...

Estar al día con la agilidad y elasticidad que trae DevOps y desarrollo moderno

La Nube requiere administración inteligente

Administración de Postura

Visibilidad granular a todos los activos, redes y grupos en la nube

Cumplimiento y Gobernanza

Cumplir automáticamente con requerimientos regulatorios y mejores prácticas

Protección de Identidad

Usar acceso just-in-time basado en los usuarios y sus roles para las operaciones sensitivas

Cloud Security Posture Management

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

Comience Ejercicios de Ciberseguridad Ahora Mismo

- Que harían en caso de
  - Ataque a la página web
  - Ransomware en un equipo de un usuario remoto? O en premisas?
  - Wiper en un equipo en premisas o de un usuario remoto?
  - Robo de credenciales de sus usuarios? De sus clientes?
  - Pérdida de su datacenter?
  - Equipo clave inaccessible?
- Publique internamente expectativas claras y logrables
  - Comunicación esperada
  - Tiempo de recuperación
  - Modo de operación

Resumen / Prioridades

- Asegurar los Endpoints
- Habilitar doble factor de autenticación
- Permitir el acceso solamente a los recursos que se necesitan
- Soluciones de SASE para optimizar la conectividad
- Asegurar la Nube y su Postura
- Asegurar Servicios SaaS
- Monitoreo de las herramientas
- Hacer ejercicios y definiciones de continuidad de negocios

¡gracias!