Deconstruir al Hacker

Ignacio Pérez Crisafulli

QuintaDisciplina Consultores
by DOMUS GLOBAL

Primero vamos a visualizar el presente

Atalayar.
ENTRE DOS ORILLAS
LAS CLAVES DEL MUNDO EN TUS MANOS

El cibercrimen supera en cifras al tráfico de armas, drogas y personas juntos

El cibercrimen supera ya el 1,5% del PIB mundial. Ha llegado al billón de dólares, hasta alcanzar un volumen que suma la de los otros tres grandes "motores" económicos en el mundo del crimen: el tráfico ilegal de armas, la trata de seres humanos y el mercado ilegal de drogas. En cuanto a sus objetivos, se dirige a todos los mercados, pero, principalmente, a empresas, gobiernos y administraciones. Y lo que es peor, las víctimas solo toman conciencia cuando ya poco pueden hacer.

CROWDSTRIKE

2025 LATAM THREAT REPORT

- 15% de aumento en incidentes de ransomware en LATAM (2024 vs. 2023)
- Más de mil millones de credenciales expuestas en Latinoamérica
- 428 organizaciones latinoamericanas listas para la venta de acceso inicial en la dark web

“El negocio de vender accesos robados es más lucratívo y extendido que nunca: nadie necesita ser hacker para hackear

—CrowdStrike LATAM Report 2025

Top five risks for organizations in the future.

Short-term: over the next 12 months (2024)	Mid to long-term: over the next 5 to 10 years (2029-2034)
1 Cyber-attacks	1 Cyber-attack
2 Extreme weather events	2 Climate risk
3 IT or telecom outage	3 Supply chain issues
4 Increased cost of living	4 Technology or telecoms outage
5 Interruption to energy supply	5 Geopolitical changes

Horizon Scan Report 2023 BCI

The top five risks for organizations in the future.

Short-term: next 12 months	**Medium term:** 5 to 10 years
1 Cyber-attacks	1 Cyber security
2 Extreme weather events (e.g. floods, storms, freeze, etc.)	2 Climate risk
3 Data breaches	3 Technology/ telecoms failure
4 IT and telecom outage	4 Supply chain issues
5 Critical Infrastructure failure	5 Introduction of emerging technologies

Horizon Scan Report 2024 BCI

Riesgos globales para los próximo 2 años, por impacto

		Tipo de riesgo
1º	Desinformación	Tecnológico
2º	Fenómenos climáticos extremos	Ambiental
3º	Polarización de la sociedad	Social
4º	Inseguridad cibernética	Tecnológico
5º	Conflicto armado interestatal	Geopolítico
6º	Falta de oportunidades económicas	Social
7º	Inflación	Económico
8º	Migración involuntaria	Social
9º	Recesión económica	Económico
10º	Contaminación	Ambiental

Fuente: Encuesta de percepción de riesgos globales del Foro Económico Mundial 2023-2024
https://www.zurich.es/notas-prensa/informe-riesgos-globales-2024

Foro Económico Global, Riesgos 2023-2024

¿Cuál es el cóctel letal para que los ciberataques sean un problema mayúsculo?

Séptimo regimiento

1. Vermut: Dark Web
2. Gin: Criptomonedas
3. Bitter: RaaS + IAB *
4. Soda: falta de conciencia y sistemas vulnerables

(*) Initial Access Broker´s, son los servicios encargados que, a través de recolección de credenciales con infostealers, le dan el punto de acceso al RaaS.

Los pagos de rescates por criptomonedas alcanzaron un récord de mil millones de dólares en 2023 - Chainalysis

Por **Medha Singh**

7 de febrero de 2024, 18:18 GMT-3 · Actualizado el 7 de febrero de 2024

En esta ilustración tomada el 24 de octubre de 2023 se ven representaciones físicas de la criptomoneda bitcoin. REUTERS/Dado Ruvic/Ilustración/Foto de archivo. Derechos de licencia de compra.

La moneda de la Dark Web: ¿cuánto vale su información personal?

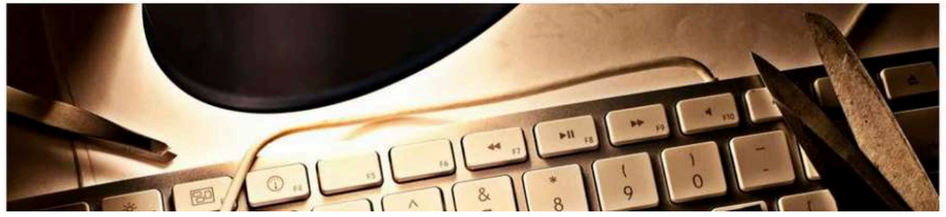
Datos financieros, como números de tarjetas de crédito o cuentas bancarias, se pagan entre 6 y 100 dólares; credenciales de acceso hasta US$75 y un historial médico puede llegar a los US$30. ¿Cómo protegerse?

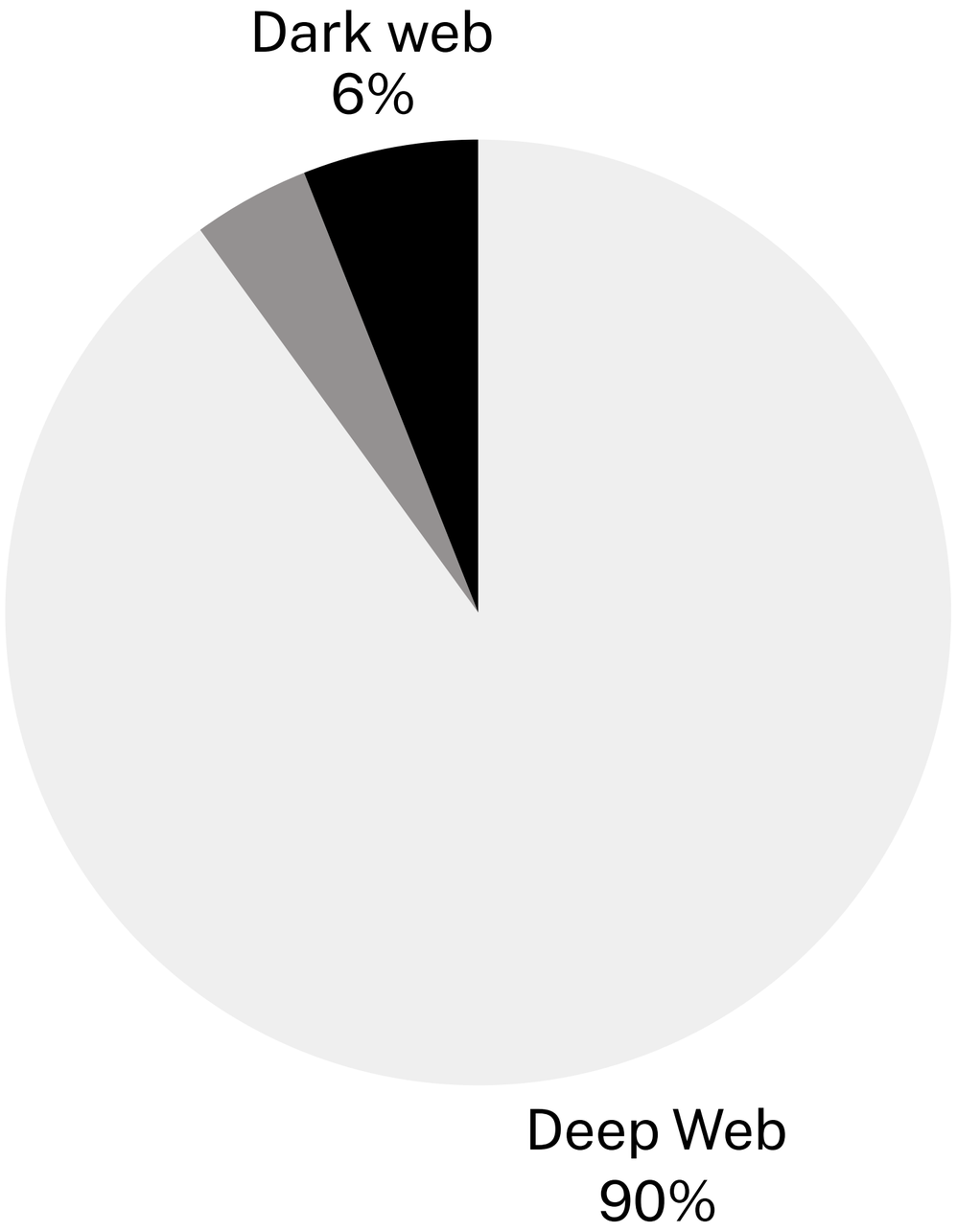
The Rise Of Ransomware As A Service (RaaS) And Implications For Business Security

Janos Konetschni Forbes Councils Member
Forbes Business Council
COUNCIL POST | Membership (Fee-Based)

Dec 18, 2023, 09:30am EST

Founder, BeforeCrypt Ltd – A Leading Ransomware Expert In Europe.




Dark web
6%
Deep Web
90%

Dark Web

World / Asia

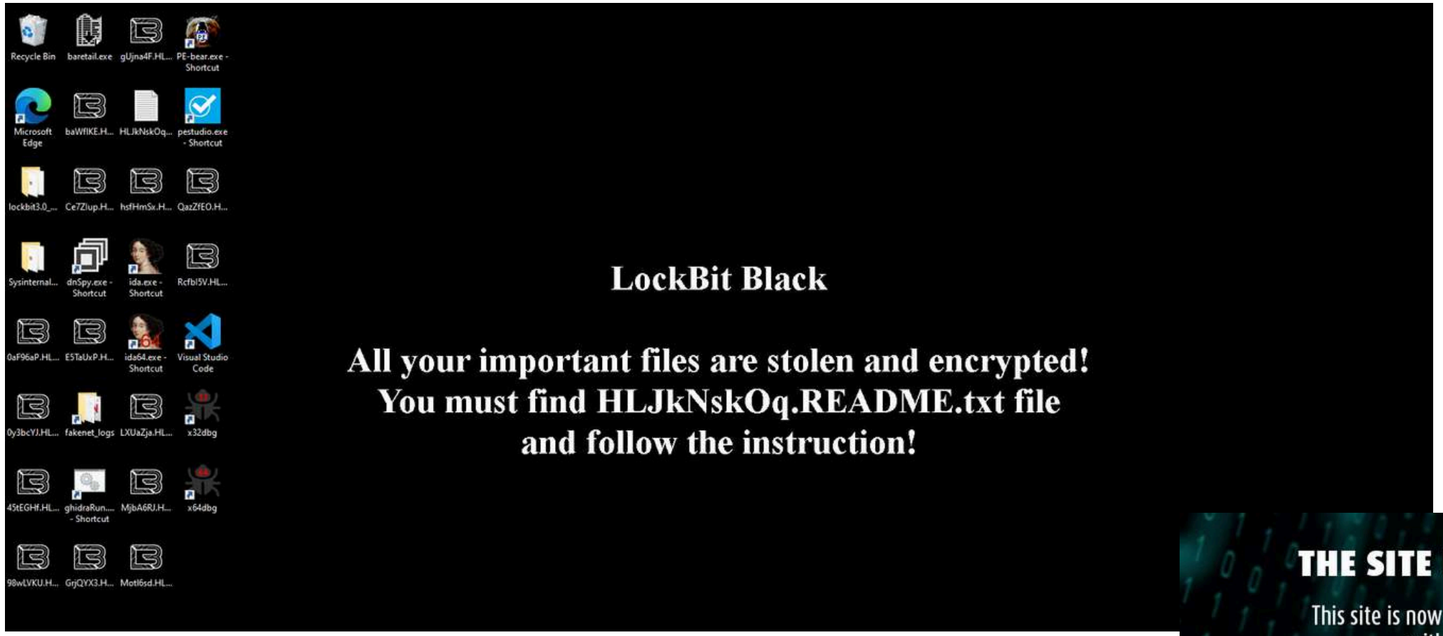
Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

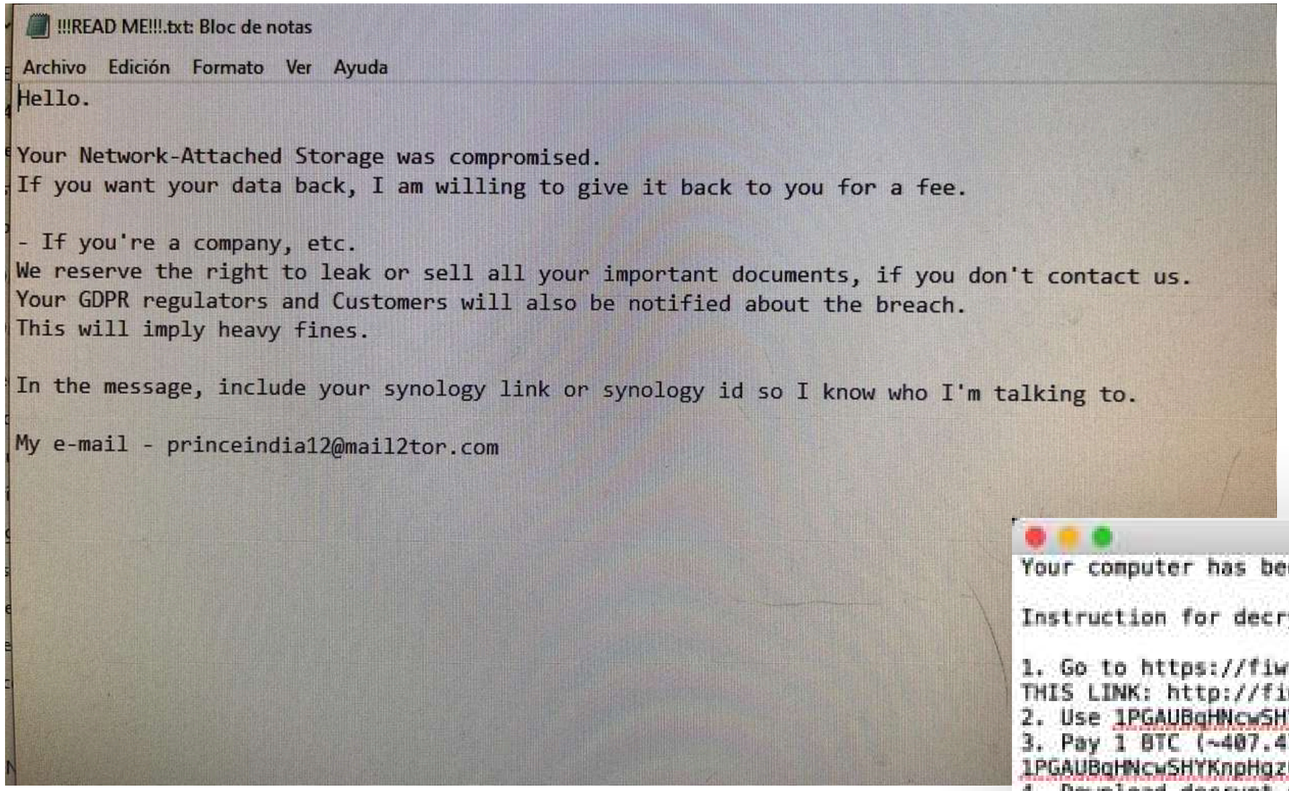
¿Quiénes se dedican a todo esto?

Hacker vs Hackactivista


Recycle Bin
baretail.exe
gUjna4F.HL...
PE-bear.exe - Shortcut
Microsoft Edge
baWfIKE.H...
HLJkNskOq...
pestudio.exe - Shortcut
lockbit3.0_...
Ce7Ziup.H...
hsfHmSx.H...
QazZfEO.H...
Sysinternal...
dnSpy.exe - Shortcut
ida.exe - Shortcut
RcfbI5V.HL...
0aF96aP.HL...
E5TaUxP.H...
ida64.exe - Shortcut
Visual Studio Code
0y3bcYJ.HL...
fakenet_logs
LXUaZja.HL...
x32dbg
45tEGHf.HL...
ghidraRun.... - Shortcut
MjbA6RJ.H...
x64dbg
98wLVKU.H...
GrjQYX3.H...
Motl6sd.HL...
LockBit Black
All your important files are stolen and encrypted!
You must find HLJkNskOq.README.txt file
and follow the instruction!


THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT
This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.
LOCKBIT
NCA
National Crime Agency
EUROPOL
POLITIE
Kanton Zürich
SH
Schleswig-Holstein
POLIISI

Pago de ataque... ¿sí o no? ¿Plan comunicación?



!!!READ ME!!!.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
Hello.

Your Network-Attached Storage was compromised.
If you want your data back, I am willing to give it back to you for a fee.

- If you're a company, etc.
We reserve the right to leak or sell all your important documents, if you don't contact us.
Your GDPR regulators and Customers will also be notified about the breach.
This will imply heavy fines.

In the message, include your synology link or synology id so I know who I'm talking to.

My e-mail - princeindia12@mail2tor.com
```

README_FOR_DECRYPT.txt — Edited

```
Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to https://fiwf4kwysm4dpw5l.onion.to ( IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN
THIS LINK: http://fiwf4kwysm4dpw5l.onion )
2. Use 1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof as your ID for authentication
3. Pay 1 BTC (~407.47$) for decryption pack using bitcoins (wallet is your ID for authentication -
1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof)
4. Download decrypt pack and run


---> Also at https://fiwf4kwysm4dpw5l.onion.to  you can decrypt 1 file for FREE to make sure
decryption is working.


Also we have ticket system inside, so if you have any questions - you are  welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```

El costo real de un ciberataque

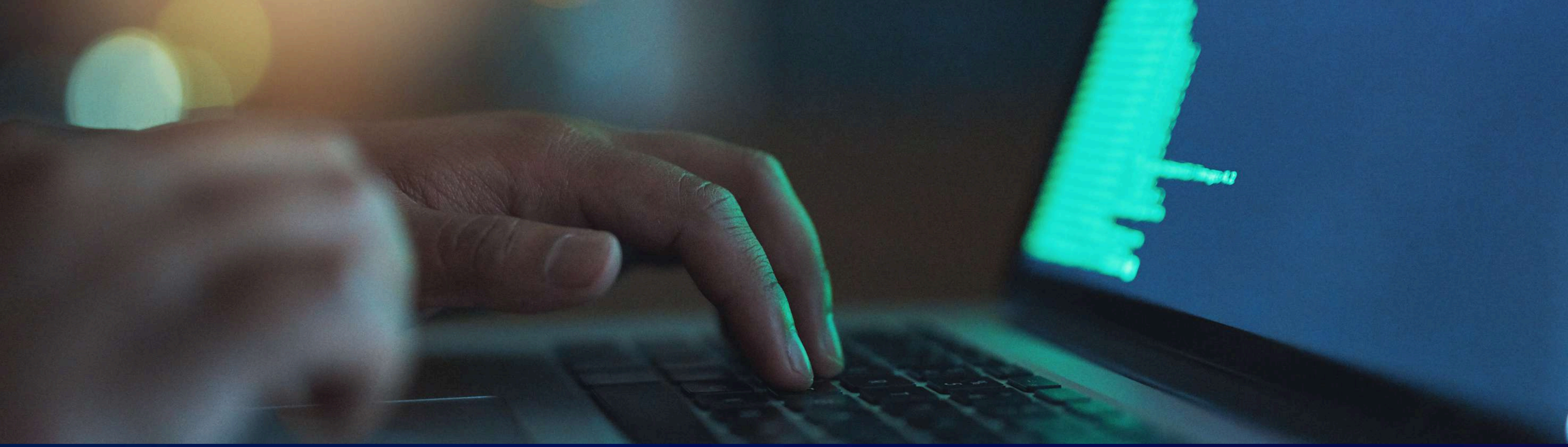
- Financiero
- Operacional
- Legal
- Reputacional

¿Cuento con análisis de riesgo que incluya perspectiva de seguridad de la información?

¿Qué nivel de reportería tengo a nivel de la Dirección?

¿Existe algún procedimiento para gestionar ataques/incidentes?

¿Plan de continuidad de negocio?



Principales causas de un ciberataque

1. Falta de concientización

2. Falta monitoreo comportamiento usuarios (UEBA)

3. Falta de doble factor de autenticación y contraseñas débiles

4. Vulnerabilidades no parcheadas

5. Débil detección de amenazas avanzadas

Tips personales

- Doble factor de autenticación en todas las redes sociales y sistemas que me lo permitan.
- Utilizar preferentemente dobles factores de autenticación en aplicaciones destinadas para tal fin (Google Authenticator, Microsoft Authenticator, etc) o con biometría.
- Activación de OTP (contraseña de un único uso) en las Tarjetas de Crédito que me lo permitan.
- Utilizar un gestor de contraseñas (Keepass, Dashlane, etc).
- Proteger con antivirus la computadora personal. Muchas ya lo traen, es simplemente activarlo.

Tips personales

- Verificar en haveibeenpwnd si mi correo personal fue vulnerado en alguna base de datos y no usar esa contraseña en otros sitios.
- Ten cuidado con los correos o enlaces sospechoso en donde pongas datos personales.
- Haz las actualizaciones que te solicitan los sistemas.
- Ten respaldada tu información personal relevante.

Tips empresariales

- Contar con un diagnóstico de situación actual y mapa de riesgos empresarial actualizado regularmente.
- Sensibilización a los empleados. Campañas de phishing ético.
- Uso de herramienta de seguridad avanzadas (próxima generación) en firewalls, antivirus, detección y prevención de intrusiones.
- Servicio interno/externo de monitoreo y respuesta de incidentes.
- Gestión regular de parches y actualizaciones.

Tips empresariales

- Auditorías internas y pruebas de penetración/hacking ético/pentesting.
- Respaldos y pruebas de respaldos.
- Plan de continuidad de negocio (BIA/BCP/DRP).

CONCIENTIZAR? SI

FORMAR CERRAJEROS? NO

Mover el foco en el usuario a la identidad del usuario

y aunque la tecnología avance...

¿Dónde está el punto más debil?


ALL YOUR CYBER SECURITY EFFORTS


THAT ONE EMPLOYEE CLICKING A PHISHING LINK

QuintaDisciplina

Consultores

by DOMUS GLOBAL