¿TU ORGANIZACION ESTA LISTA PARA UN INCIDENTE?

Computer Security Incident Response Team (CSIRT)

LAC Digital Academy

LAC Digital Academy

¿Qué harían si...

mañana a las 7 AM les cifran todos los archivos y les piden 2 bitcoins?

Incidente Coppel

En abril de 2024 Grupo Coppel sufrió uno de los incidentes de ciberseguridad más grandes en la historia del sector retail en México.

El grupo LockBit 3.0 aprovechó una brecha de seguridad para infiltrarse en la red, cifrar la información de los servidores y exigir el pago de un rescate, esto terminó afectando 9500 servicios y las operaciones de 1800 tiendas físicas.

Coppel tardó 3 meses completos en restaurar el 100% de la operatividad del negocio. Tras la recuperación, la empresa sometió su infraestructura a auditorías, reforzó sus controles de acceso y actualizó sus protocolos de seguridad.

https://www.incibe.es/incibe-cert/blog/lockbit-acciones-de-respuesta-y-recuperacion

https://vanguardia.com.mx/noticias/coppel-acepta-fallas-de-ciberseguridad-en-su-sistema-se-trato-de-un-hackeo-EA11778084

https://www.eleconomista.com.mx/finanzaspersonales/Por-falla-en-sistemas-Coppel-perdonara-intereses-moratorios-a-sus-clientes-20240418-0126.html

LAC Digital Academy

Coppel
14 de abril de 2024 ·

A nuestros clientes, muy pronto podrán disfrutar de nuestros servicios.

Atento aviso

Hemos identificado fallas en nuestros sistemas.
Nuestro equipo se encuentra trabajando para su restablecimiento.
Lamentamos las molestias ocasionadas.

Coppel

Coppel
20 de abril de 2024 ·

Actualización para nuestros clientes.

20 de abril, 2024

Tiendas Coppel informa

En días pasados identificamos una falla en algunos de nuestros sistemas, por lo que de inmediato se activaron los procedimientos de respuesta, protección y análisis para estos casos. Tras un proceso de investigación exhaustivo, hemos determinado que se trató de un incidente de ciberseguridad, por lo que reforzamos nuestras medidas y controles.

Las **Tiendas Coppel** están abiertas al público en el horario normal y atendiendo a los clientes para diversos servicios.

Reiteramos nuestro compromiso con nuestros clientes, colaboradores y proveedores. Seguiremos trabajando para restablecer la totalidad de nuestros servicios, y canales de atención y venta.

En caso de dudas solicitamos a nuestros clientes comunicarse al teléfono **800 220 7735**, al correo **atencion@coppel.com** o acudir a cualquiera de nuestras tiendas para solicitar información.

Coppel

Sala de prensa | Comunicados nacionales |

Pemex opera con normalidad

11/11/2019 | 48

- **El funcionamiento de los sistemas de operación y producción operan con normalidad**
- **El inventario y abasto de combustibles está garantizado**
- **Se invita a la comunidad petrolera y a la sociedad, evitar rumores que dañan la imagen de la empresa.**

Ante la ola de rumores y comunicados apócrifos, notas y comentarios en redes sociales sobre un ataque a los sistemas informáticos internos de Petróleos Mexicanos, se informa lo siguiente:

Petróleos Mexicanos opera con normalidad. El funcionamiento de los sistemas de operación y producción de la empresa no están comprometidos, además de que se encuentran blindados.

El día de ayer domingo 10 de noviembre, la empresa productiva del Estado recibió intentos de ataques cibernéticos que fueron neutralizados oportunamente, afectando el funcionamiento a menos del 5% de los equipos personales de cómputo.

https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx

LAC Digital Academy

HACKEO A LA SEDENA

El 29 de septiembre de 2022, el grupo *hacktivista* Guacamaya ingresó a los sistemas de la Secretaría de la Defensa Nacional (SEDENA) y obtuvo 6 terabytes[32] de información. Entre los documentos filtrados, se encontraban comunicaciones, fotografías y documentos de diversos temas, como contratos de obra pública, seguridad, contratos del ejército, correos, el estado de salud del Presidente López Obrador, **informes de inteligencia sobre líderes** criminales y **políticos**,[33] **transcripciones de intervenciones telefónicas, directorios y reportes sobre seguimiento a persones, como el Embajador de**

[31] *Ibid.*

[32] Abi-Habib, M. (2022). "El hackeo del ejército mexicano expone secretos de la institución más poderosa del país". The New York Times. Recuperado 8 de octubre de 2023. Disponible en: https://www.nytimes.com/es/2022/10/06/espanol/mexico-sedena-guacamaya-hackeo.html

[33] BBC News Mundo. (2022). "Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México". Recuperado 8 de octubre de 2023. Di
latina-63167331

UNCATEGORIZED **Loret Capítulo 96**

Foto: Latinus

Por Carlos Loret de Mola Escrito en UNCATEGORIZED el 29/9/2022 · 19:59 hs

En el capítulo de hoy, el ciberataque más grave que haya sufrido el **gobierno de México** en su historia dejó al descubierto decenas de miles de correos alojados en los servidores de la **Secretaría de la Defensa Nacional**, que datan de 2016 hasta septiembre de este año.

Detalles sobre el verdadero estado de salud del presidente Andrés Manuel López Obrador o las disputas entre los titulares de la **Sedena** y de la **Secretaría de la Marina**, la versión completa del "**Culiacanazo**", así como la débil seguridad de las aduanas, son algunos de los hallazgos que presentamos en esta primera entrega sobre la información obtenida en los seis terabytes de material expuesto por el grupo internacional de hackers autodenominado "**Guacamaya**", que también vulneró la seguridad virtual de otros cuatro países en **Latinoamérica**.

Esta intromisión a los sistemas de cómputo de la **Sedena** muestra además una radiografía del enorme poderío y mando que tiene el **Ejército** en la actual administración.

Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México

Redacción
BBC News Mundo

6 octubre 2022

Son millones de correos electrónicos y documentos militares de México los que han quedado expuestos.

El grupo de hackers autodenominado Guacamaya asegura que se infiltró en un servidor de la Secretaría de la Defensa Nacional (Sedena) y extrajo 6 terabytes de información interna y confidencial.

Eso es aproximadamente **el triple de información** que la divulgada en los Pandora Papers que expusieron secretos financieros mundiales en 2021.

CÁMARA DE DIPUTADOS
LXV LEGISLATURA

https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx
https://www.bbc.com/mundo/noticias-america-latina-63167331
https://gaceta.diputados.gob.mx/PDF/65/2023/dic/20231206-II-6-1.pdf

LAC Digital Academy

País más atacado en America Latina

En Latinoamerica ocurren 1600 ciberataques por segundo, y cada brecha exitosa puede llegar a costar en promedio $4.65 Millones de USD a las organizaciones.

Brasil, México y Colombia figuran como las naciones más impactadas de la región. En el caso de México, este concentra el 23% de los incidentes regionales (equivalente a 58.1 billones anuales), lo que se traduce en pérdidas estimadas de hasta 137 mil millones de pesos mexicanos al año.

https://latam.newsroom.ibm.com/

https://latam.kaspersky.com/

Organizaciones que han sido blanco de ciberataques:
Mercado Libre, Ticketmaster, PEMEX, SEDENA, Coppel, Lajas Renner, EPM.

LAC Digital Academy

Definición de un CSIRT

- Un CSIRT (Computer Security Incident Response Team) ejecuta, coordina y asiste en la respuesta a incidentes de seguridad que involucren sistemas informáticos.
- Atiende a una comunidad predefinida con un conjunto de servicios acordados.
- No solo responde a incidentes: también toma medidas preventivas para evitar o mitigar su ocurrencia.

LAC Digital Academy

Tipos de CSIRT

Tipo	Comunidad objetivo	Ejemplos
Nacional	Todo el país; rol coordinador	CERT-MX, ColCERT, EcuCERT
Sector Público	Entidades gubernamentales	CSIRT de un ministerio, gobierno municipal
Interno	Personal interno de una organización	CSIRT de empresa, universidad, hospital
Académico	Comunidad universitaria / investigadores	UNAM-CERT
Comercial (MSSP)	Clientes de pago	Empresas de seguridad gestionada
Infraestructura crítica	Energía, agua, transporte	CSIRT de operadores de red eléctrica
PSIRT	Usuarios de un producto específico	Cisco PSIRT, Microsoft MSRC
PyMES	Grupo de organizaciones pequeñas	CSIRT sectorial compartido

En que tipo cae SU organizacion?

Es la primera decision que se toma al crear un CSIRT. Y define todo lo demas: a quien atiende, que servicios ofrece y que autoridad tiene.

LAC Digital Academy

Miércoles, 7:00 AM

Un empleado de finanzas reporta que no puede abrir sus archivos.
En pantalla aparece una nota:

“Sus datos han sido cifrados. Tiene 48 horas para pagar 2 BTC.”

- Soporte de TI sugiere formatear y reinstalar Windows
- Comunicación pregunta si hay que publicar algo
- El Director General pregunta si se paga.

LAC Digital Academy

Lo que un CSIRT entrenado pregunta:

1. Es un incidente?
2. A quien avisamos?
3. Apagamos el equipo?
4. Se paga el rescate?
5. Que le decimos a la prensa?
6. Quien documenta?

LAC Digital Academy

Lo que un CSIRT entrenado pregunta:

1	Es un incidente?	Si. Cifrado + rescate = ransomware.
2	A quien avisamos?	Al coordinador del CSIRT. No al periodico ni al proveedor. El proveedor solo se contacta según el protocolo.
3	Apagamos el equipo?	NO. Se pierde evidencia forense. Se aisla de la red, no se apaga.
4	Se paga el rescate?	NO. No garantiza recuperacion y financia al atacante.
5	Que le decimos a la prensa?	Nada por el momento. Solo hechos verificados según el plan de crisis de comunicación. Cero especulación
6	Quien documenta?	Se documenta todo desde el minuto 1, por todo el equipo.

La diferencia:

Sin CSIRT

- x Nadie sabe a quien llamar
- x Se apaga el equipo, se pierde evidencia
- x TI reinstala sin investigar la causa
- x No se documenta nada
- x Se repite el mismo incidente
- x La direccion se entera por el periodico

Con CSIRT

- Coordinador activado en minutos
- Se aisla de la red, se preserva evidencia
- Triage con protocolo, ticket y clasificacion
- Todo documentado desde el minuto 1
- Leccion aprendida, defensa actualizada
- Comunicacion controlada y verificada

LAC Digital Academy

Beneficios de contar con un CSIRT

01

Especialización

El personal de la organización cuenta con especialistas en distintas tecnologías, listos para asistir ante incidentes.

02

Confianza

Genera mayor confianza en la comunidad atendida, agilizando la resolución de incidentes y reduciendo su impacto.

03

Punto de contacto único

Canal centralizado para recibir alertas, reportar incidentes y obtener asesoría y asistencia en tiempo real.

04

Cultura de seguridad

Mejora la percepción y práctica de la seguridad a través de difusión de buenas prácticas y concientización continua.

¿Cuánto cuesta NO tener un CSIRT?

No es cuanto cuesta tener uno.

Es cuanto cuesta NO tenerlo.