Marzo 2025

CiberPulso

Boletín del Comité de Ciberseguridad

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
impulsamos la transformación digital

LÍDER COMITÉ DE CIBERSEGURIDAD

Ana Cecilia Pérez
Líder del Comité de Ciberseguridad ALETI

A medida que entramos en el tercer mes del año, el paisaje de la ciberseguridad sigue mostrándose tanto dinámico como desafiante. En esta edición de **Ciberpulso**, exploramos una serie de temas críticos que son fundamentales para comprender y enfrentar los retos actuales y futuros en seguridad digital. Desde incidentes de gran impacto que ponen a prueba nuestra resiliencia, hasta iniciativas estratégicas que buscan fortalecer nuestra postura de seguridad a nivel regional e internacional.

Este mes destacamos el reciente apagón en Chile causado por un ataque cibernético, un recordatorio potente de la vulnerabilidad de nuestras infraestructuras críticas. También analizamos las últimas estadísticas de ciberseguridad de 2024, que reflejan una escalada en la sofisticación y frecuencia de los ataques, especialmente en formas de ransomware de doble y triple extorsión que amenazan no solo a las empresas, sino también a la infraestructura nacional.

Además, celebramos la creación de la Dirección General de Ciberseguridad en México, una medida esperanzadora hacia una gestión más eficaz y unificada de las amenazas cibernéticas.

Esperamos que los temas tratados en esta edición les proporcionen perspectivas valiosas y les ayuden a fortalecer sus estrategias de ciberseguridad. Estamos comprometidos a mantenerlos informados y preparados para enfrentar los desafíos que nos depara el futuro digital.

Noticias

Incidente de ciberseguridad en Chile: Apagón nacional y sus consecuencias

Este mes, Chile experimentó un apagón masivo resultado de un ataque cibernético dirigido a su infraestructura eléctrica nacional, destacando la vulnerabilidad de sistemas críticos a amenazas digitales:

- **Impacto inmediato:** La interrupción afectó a gran parte del país, paralizando servicios esenciales y causando una significativa disrupción económica.
- **Respuesta de emergencia:** Hospitales, servicios de emergencia y transporte público se vieron obligados a activar protocolos de crisis, demostrando la importancia de tener planes de contingencia robustos.
- **Acciones gubernamentales:** La rápida intervención de la Dirección General de Ciberseguridad ayudó a mitigar los efectos del ataque y a iniciar una investigación exhaustiva para prevenir futuros incidentes.

- **Lecciones aprendidas:** El evento reafirmó la necesidad de fortalecer las medidas de seguridad cibernética a nivel nacional e internacional, impulsando la cooperación entre gobiernos y el sector privado.

Se crea la Dirección General de Ciberseguridad en México:

La creación de la Dirección General de Ciberseguridad en México es un paso significativo en el fortalecimiento de las capacidades nacionales para enfrentar los desafíos de ciberseguridad. Este organismo no solo centraliza la gestión y coordinación de las estrategias de ciberseguridad, sino que también establece un marco claro para la respuesta a incidentes y la colaboración entre sectores públicos y privados.

Importancia de la Dirección General de Ciberseguridad:

Coordinación mejorada: Antes de su establecimiento, la respuesta a los incidentes de ciberseguridad en México era fragmentada, lo que a menudo llevaba a respuestas lentas y descoordinadas. La Dirección General de Ciberseguridad deberá de unificar estas respuestas, permitiendo una acción más rápida y cohesiva en situaciones críticas.

Política integral de ciberseguridad: Esta entidad debiera ser la responsable de desarrollar y ejecutar una política de ciberseguridad nacional que no solo aborde la defensa contra ataques cibernéticos, sino que también promueva la resiliencia cibernética a través de regulaciones, normativas y mejores prácticas que estén alineadas con estándares internacionales.

Educación y concientización: La Dirección tiene un papel crucial en la educación y concientización sobre ciberseguridad a todos los niveles de la sociedad. Esto incluye programas de formación para empleados del gobierno y colaboraciones con instituciones educativas para incorporar la ciberseguridad en el currículo académico.

Importancia de la Dirección General de Ciberseguridad:

- **Recursos y capacitación:** Uno de los mayores retos es asegurar que la Dirección esté adecuadamente equipada con los recursos y las herramientas necesarias para combatir amenazas avanzadas. Esto incluye la capacitación continua de su personal en las últimas tecnologías y estrategias de defensa.
- **Colaboración intersectorial:** Aunque es fundamental, la colaboración entre el gobierno, la industria y la academia presenta desafíos, especialmente en términos de compartir información sensible y coordinar respuestas a incidentes de manera efectiva y segura.
- **Adaptación a nuevas amenazas:** El panorama de amenazas cibernéticas está en constante evolución, lo que requiere que la Dirección General de Ciberseguridad sea ágil y adaptable en sus estrategias para mantenerse al día con las nuevas tácticas y técnicas de los ciberdelincuentes.
- **Balance entre seguridad y privacidad:** Mantener un equilibrio entre fortalecer la seguridad cibernética y proteger los derechos de privacidad de los ciudadanos es otro desafío significativo. La Dirección debe asegurarse de que las medidas implementadas no infrinjan indebidamente las libertades individuales**.**

En resumen, la Dirección General de Ciberseguridad desempeña un papel vital en la protección de la infraestructura nacional y la información crítica de México contra las crecientes amenazas cibernéticas. Su éxito dependerá de la capacidad para superar estos retos y de su efectividad en implementar una estrategia que fortalezca la seguridad de toda la nación de manera sostenible y respetuosa con los derechos de los ciudadanos.

Estadísticas de ciberseguridad de 2024

Aumento de ataques de ransomware:

En 2024, los ataques de ransomware en Iberoamérica siguieron siendo una de las mayores amenazas. La región experimentó un aumento significativo en ataques de doble y triple extorsión, que no solo buscan el pago de rescates por el descifrado de datos, sino también amenazan con la publicación de datos robados si no se cumplen las demandas económicas. Este tipo de ataque refleja una evolución en la sofisticación y la audacia de los ciberdelincuentes.

Phishing y BEC (Compromiso de Email Empresarial):

El phishing continúa siendo el método principal de ataque, particularmente a través de correos electrónicos que se utilizan para entregar malware. Además, los ataques BEC, donde los atacantes usurpan la identidad de ejecutivos para solicitar transferencias de fondos fraudulentas, siguen causando pérdidas significativas en las empresas. La falta de autenticación multifactor en muchas organizaciones ha exacerbado este problema.

Inversión en seguridad de la información:

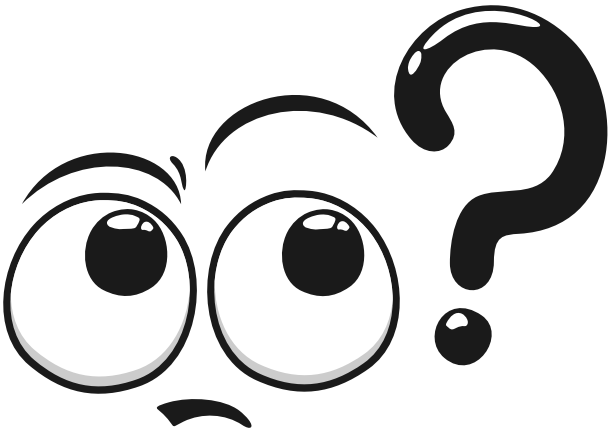
La inversión en productos y servicios de seguridad de la información ha crecido considerablemente, con una previsión de alcanzar más de $215 mil millones en 2024. Este incremento refleja la creciente reocupación por proteger infraestructuras críticas y datos corporativos frente a amenazas cada vez más complejas y costosas. La necesidad de adaptarse a las regulaciones globales sobre privacidad y protección de datos también ha impulsado este aumento en la inversión.

Impacto en industrias específicas:

Sectores como el de la salud y las telecomunicaciones fueron especialmente vulnerables y, por tanto, objetivos primarios de ciberataques en 2024. En el sector salud, por ejemplo, los ataques no solo buscaron robar datos, sino también interrumpir servicios, forzando a las instituciones a pagar rescates para recuperar el acceso a sistemas críticos.

Estas tendencias reflejan un panorama de ciberseguridad en el que los riesgos están escalando y la necesidad de soluciones avanzadas de seguridad es más crítica que nunca. La respuesta adecuada implica tanto la adopción de tecnología de punta como la formación y la concienciación continua entre los empleados sobre las mejores prácticas de seguridad.

¿A qué le debemos poner atención?



A los ataques de ransomware: Este vector de ataque representan una forma de malware que cifra los archivos de la víctima, impidiendo el acceso a sus datos o sistemas hasta que se pague un rescate.

Preguntas con respuestas...

Los atacantes generalmente exigen el pago en criptomonedas para evitar ser rastreados. Este tipo de malware puede entrar en los sistemas a través de correos electrónicos de phishing, descargas maliciosas o explotando vulnerabilidades en el software.

¿Por qué nos deben de interesar los ataques de ransomware?

Los ataques de ransomware son críticos por varias razones:

- **Impacto financiero significativo:** Además del pago del rescate, las organizaciones pueden sufrir pérdidas operativas, daños a la reputación y costos legales significativos.
- **Interrupción de operaciones críticas:** En sectores como la salud y la infraestructura crítica, un ataque de ransomware puede paralizar operaciones esenciales, poniendo vidas en riesgo.
- **Pérdida de datos sensibles:** Muchos ataques de ransomware ahora incluyen el robo de datos, lo que puede exponer información sensible de clientes o interna.

¿Qué tan preparadas y conscientes están las organizaciones para ser víctimas de doble y triple extorsión?

La preparación varía ampliamente entre las organizaciones, pero muchos aún luchan por mantenerse al día con estas amenazas cada vez más sofisticadas:

- **Doble extorsión:** Implica no solo el cifrado de datos sino también su robo, amenazando con liberar la información en línea si no se paga el rescate. Las empresas a menudo no están preparadas para este escenario, careciendo de medidas de detección y respuesta adecuadas.
- **Triple extorsión:** Añade una capa adicional al atacar o extorsionar a clientes o socios de la víctima, aumentando la presión para pagar el rescate. Esto requiere un nivel aún más sofisticado de preparación en términos de seguridad cibernética y gestión de crisis.

Preparación y conciencia:

- **Inversiones en ciberseguridad:** Aunque las organizaciones están aumentando sus inversiones en ciberseguridad, muchas aún carecen de las capacidades para detectar y responder rápidamente a los ataques complejos de ransomware.

- **Educación y entrenamiento:** La formación continua en ciberseguridad es crucial, pero no todas las organizaciones tienen programas establecidos para educar a sus empleados sobre las últimas tácticas de amenazas, incluidos los ataques de ransomware.
- **Planes de respuesta a incidentes:** Tener un plan de respuesta a incidentes que incluya escenarios de doble y triple extorsión es fundamental, pero no todas las empresas cuentan con estos planes detallados y probados.

En conclusión, aunque la conciencia sobre el ransomware está aumentando, muchas organizaciones todavía necesitan mejorar significativamente en términos de preparación técnica y estratégica para enfrentar estos ataques avanzados. La inversión en medidas proactivas de ciberseguridad, junto con la educación y la formación continua, son esenciales para mitigar el riesgo y el impacto de los ataques de ransomware de doble y triple extorsión.

Conclusión:

Los eventos de este mes nos recuerdan la importancia de la vigilancia y la adaptación continua en el campo de la ciberseguridad. La colaboración y el intercambio de conocimientos entre países y sectores son fundamentales para desarrollar una defensa efectiva que pueda hacer frente a las dinámicas amenazas cibernéticas. **Ciberpulso** se compromete a mantener a nuestra comunidad informada y preparada para enfrentar estos desafíos.

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
impulsamos la transformación digital

Reflexionamos sobre la importancia de estar siempre un paso adelante en ciberseguridad, tanto en la tecnología que utilizamos como en la educación que proporcionamos a las próximas generaciones. En “Ciberpulso”, continuaremos brindándote las últimas noticias, análisis en profundidad y recursos educativos para asegurar que estés bien equipado para enfrentar los desafíos del mañana en el mundo digital.

CONTÁCTANOS:

comunicaciones@aleti.org

¡Únete aquí al comité de trabajo que promueve la ciberseguridad en la región!