Diciembre 2024

CiberPulso

Boletín del Comité de Ciberseguridad

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
impulsamos la transformación digital

LÍDER COMITÉ DE CIBERSEGURIDAD

A medida que el 2024 llega a su fin, reflexionamos sobre los desafíos y avances en ciberseguridad. Este año se ha visto un aumento en la sofisticación de los ciberataques, impulsando a las organizaciones a fortalecer sus defensas y adaptarse rápidamente. La seguridad de la información se ha convertido en una prioridad, especialmente con la adopción del trabajo remoto y la protección de infraestructuras críticas. En 2025, debemos seguir fomentando una cultura de seguridad proactiva, colaborando entre industrias y educándonos constantemente para anticipar y prevenir riesgos cibernéticos.

Ana Cecilia Pérez

Líder del Comité de Ciberseguridad ALETI

Tema del Mes:
Ciberseguridad y trabajo remoto

En la era del trabajo remoto, la seguridad de la información se ha convertido en un componente esencial para las operaciones diarias de cualquier organización. A medida que más empleados operan fuera de las oficinas tradicionales, las prácticas de ciberseguridad robustas son más cruciales que nunca para proteger tanto a las empresas como a sus empleados de ciberataques potencialmente devastadores.

Uso seguro de conexiones a Internet:

VPN Segura: Asegúrate de que todos los empleados utilicen una conexión VPNcifrada cuando accedan a la red corporativa. Esto crea un canal seguro que encripta los datos antes de que viajen por internet.

Wi-Fi Protegido: Instruye a los empleados para que eviten el uso de redes Wi-Fi públicas sin protección. Si es necesario, deben utilizar una VPN o un dispositivo hotspot personal para una capa adicional de seguridad.

Gestión de dispositivos y accesos:

Autenticación multifactor (MFA): Implementa MFA para todas las cuentas corporativas, proporcionando una capa adicional de seguridad que requiere múltiples formas de verificación antes de conceder acceso.

Política de BYOD (Bring Your Own Device): Establece y haz cumplir políticas de BYOD que definan claramente qué medidas de seguridad deben tener los dispositivos personales antes de ser utilizados para el trabajo.

Educación y capacitación continua:

Formación regular: Realiza sesiones de capacitación regularmente sobre los últimos riesgos de ciberseguridad y las mejores prácticas para mitigarlos. Esto incluye formación sobre phishing, manejo seguro de datos y protocolos de seguridad.

Simulaciones de phishing: Organiza pruebas de phishing simuladas para educar a los empleados sobre cómo identificar y manejar intentos de phishing de manera efectiva.

Actualizaciones y mantenimiento de Software:

Parches y actualizaciones: Asegura que todos los sistemas y aplicaciones estén al día con los últimos parches de seguridad. Automatiza las actualizaciones siempre que sea posible para reducir la posibilidad de errores humanos.

Antivirus y Antimalware: Equipa cada dispositivo con soluciones robustas de antivirus y antimalware que se actualicen automáticamente para proteger contra software malicioso.

Respuesta ante incidentes y recuperación:

Plan de respuesta a incidentes: Desarrolla y prueba un plan de respuesta a incidentes ciberseguros que incluya procedimientos específicos para incidentes remotos.

Copias de seguridad automatizadas: Implementa una estrategia de copias de seguridad automáticas para todos los datos críticos. Esto no solo protege la información importante, sino que también facilita la recuperación en caso de un ataque cibernético o pérdida de datos.

Implementar estas mejores prácticas no solo fortalecerá la infraestructura de ciberseguridad de tu organización sino que también fomentará una cultura de seguridad consciente y preparada. A medida que el trabajo remoto sigue siendo una norma, es esencial mantener una postura proactiva en ciberseguridad para proteger los activos digitales y la integridad de la información corporativa.

Actualizaciones en legislación de ciberseguridad

Mantenerse al día con las últimas actualizaciones en la legislación de ciberseguridad es crucial para las organizaciones que operan en un entorno global interconectado. A medida que los gobiernos de todo el mundo buscan abordar las nuevas amenazas digitales, las normativas cambian frecuentemente, impactando cómo las empresas deben proteger tanto sus datos como los de sus clientes.

Estados Unidos:

Se ha introducido nueva regulación por parte del Departamento de Servicios Financieros de Nueva York (NYDFS), ampliando los requisitos de notificación de incidentes de ransomware. Esta regulación está aumentando la responsabilidad de las organizaciones en hacer evaluaciones de vulnerabilidad más rigurosas y mejora los requerimientos para la respuesta y recuperación de incidentes y desastres. **ConnectWise**

Unión Europea:

La Directiva de Seguridad de Redes y Sistemas de Información (NIS2) ha sidoexpandida, comenzando a afectar a las empresas en cuanto a la gobernanza global de IA y haciendo de la ciberseguridad un tema obligatorio a nivel de dirección para prácticamente todos los sectores industriales. **ConnectWise**

Regulación General de Protección de Datos (GDPR):

Se están proponiendo ajustes a la GDPR para fortalecer la cooperación entre las autoridades de protección de datos en casos transfronterizos. Esto incluye esfuerzos para armonizar las reglas procesales y acelerar la resolución de casos.
Baker McKenzie

ATAQUE CIBERNÉTICO A INSTITUCIÓN FINANCIERA EN COLOMBIA

Ataque de ransomware que paralizó los sistemas operativos y transacciones de una importante institución financiera.

MÉTODO DE ATAQUE:

Infiltración a través de técnicas de **phishing** que comprometieron las redes internas de la institución, seguido de la implantación de **ransomware** que cifró los datos críticos, inutilizando los sistemas operativos y de transacciones.

DEMANDA DE LOS ATACANTES:

Exigencia de un rescate en criptomonedas para desbloquear los sistemas afectados y evitar la divulgación de datos confidenciales robados.

DETALLES DEL CASO

- Sector Financiero
- Noviembre 2024
- Colombia

¿CUÁL ES LA LECCIÓN APRENDIDA?

IMPORTANCIA DE LA RESPUESTA RÁPIDA:

La necesidad de una respuesta inmediata y efectiva a los incidentes para minimizar daños y restaurar operaciones.

INVERSIÓN EN CIBERSEGURIDAD:

Destacar la importancia de invertir en soluciones avanzadas de ciberseguridad y entrenamiento continuo para los empleados en técnicas de detección de phishing y otras amenazas.

PLANES DE CONTINUIDAD DEL NEGOCIO:

El desarrollo y la implementación de planes de continuidad de negocio y recuperación de desastres robustos son cruciales para la resiliencia organizacional.

COLABORACIÓN SECTORIAL:

Fomentar una mayor colaboración entre instituciones financieras y agencias gubernamentales para mejorar las defensas colectivas contra ciberataques.

RESPUESTA Y PREVENCIÓN

Innovaciones en ciberseguridad: Cifrado Homomórfico

En el panorama actual de la ciberseguridad, proteger la confidencialidad y la integridad de los datos mientras se mantienen accesibles y funcionales es un desafío considerable. El cifrado homomórfico, una de las tecnologías emergentes más prometedoras, ofrece una solución a este dilema permitiendo que los datos permanezcan cifrados durante el procesamiento.

El cifrado homomórfico es una forma avanzada de cifrado que permite realizar cálculos complejos directamente sobre datos cifrados sin necesidad de descifrarlos. Esta capacidad es revolucionaria porque asegura que la información sensible permanezca segura y protegida incluso durante el análisis.

Funcionamiento técnico:

La técnica utiliza algoritmos matemáticos que aplican operaciones aritméticas a los datos cifrados. Esto resulta en un conjunto de datos cifrados que, una vez descifrados, revelan el resultado correcto de las operaciones como si se hubieran realizado sobre los datos originales en claro. El proceso asegura que la información sensible nunca esté expuesta, ni siquiera durante el procesamiento por aplicaciones o servicios en la nube.

Aplicaciones y beneficios:

Seguridad en la nube: El cifrado homomórfico es ideal para entornos de nube, donde las organizaciones pueden procesar o analizar datos confidenciales en la nube pública sin comprometer su seguridad.

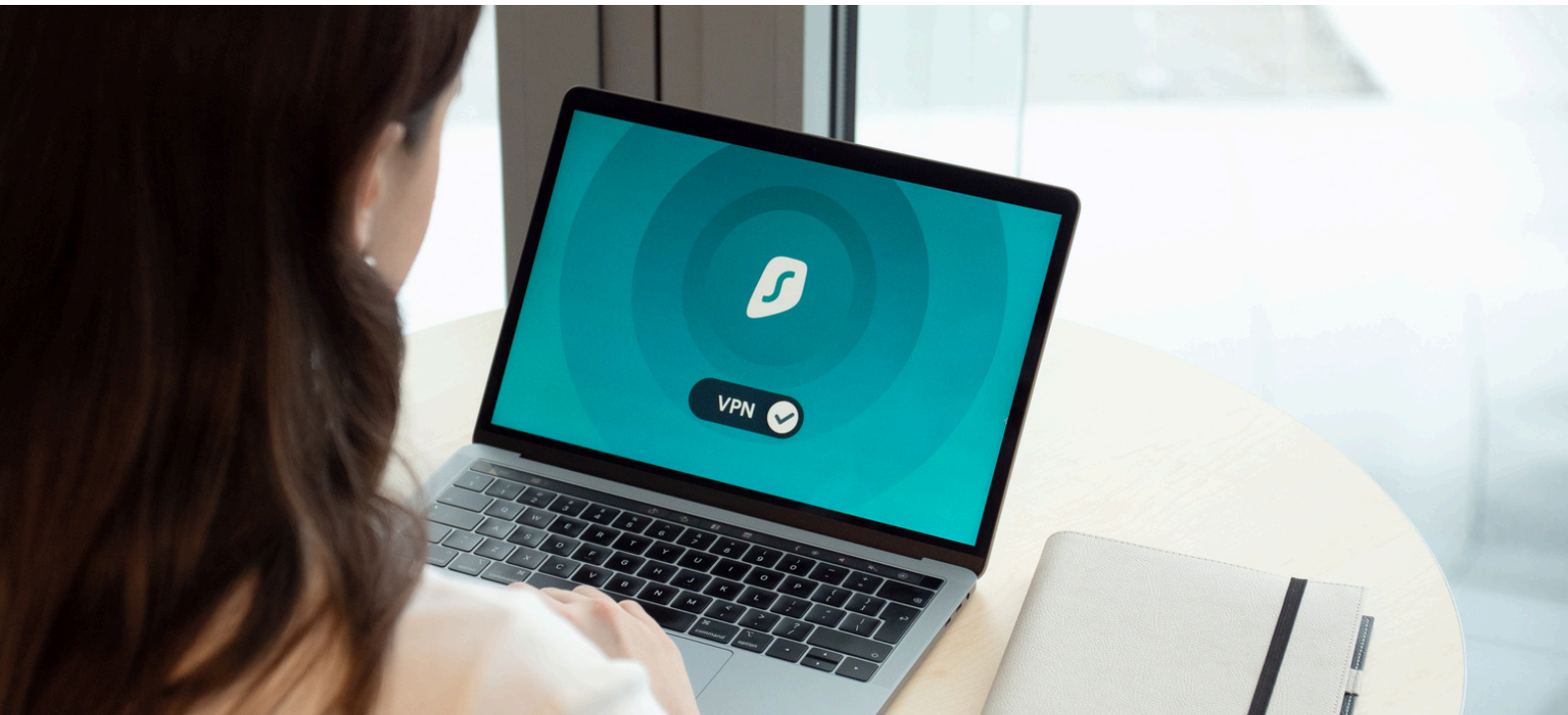
Cumplimiento regulatorio: Ayuda a las empresas a cumplir con regulaciones estrictas de protección de datos, como la GDPR, ya que los datos pueden procesarse sin revelar información sensible a terceros, incluidos los proveedores de servicios en la nube.

Investigación colaborativa: En campos como la medicina y la financiación, donde la privacidad de los datos es crucial, el cifrado homomórfico permite a los investigadores colaborar en conjuntos de datos sensibles sin exponer la información subyacente.

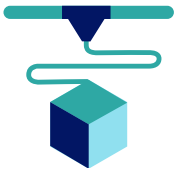
Desafíos y limitaciones:

A pesar de sus ventajas, el cifrado homomórfico todavía enfrenta desafíos significativos en términos de eficiencia y velocidad de computación. Los algoritmos actuales requieren una gran cantidad de recursos computacionales, lo que puede resultar en tiempos de procesamiento más lentos en comparación con métodos no cifrados. Sin embargo, la investigación continua y los avances en hardware especializado están comenzando a superar estas barreras.

El cifrado homomórfico representa un avance significativo en el campo de la ciberseguridad, ofreciendo nuevas posibilidades para la protección de datos en la era digital. A medida que la tecnología madura y se vuelve más accesible, es probable que su adopción se expanda, transformando la manera en que protegemos y procesamos la información más valiosa.

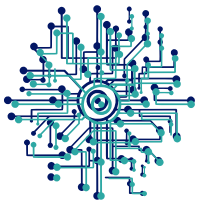


Problemáticas adicionales y urgentes:



El Uso de Impresoras 3D para la Creación de Armas

El avance en la tecnología de impresión 3D ha traído consigo numerosas innovaciones en campos que van desde la medicina hasta la ingeniería. Sin embargo, esta tecnología también presenta desafíos significativos para la seguridad pública, especialmente en su capacidad para fabricar armas de fuego. Informes recientes indican un aumento en la utilización de impresoras 3D para crear armas, una tendencia preocupante que plantea preguntas sobre cómo las leyes actuales pueden abordar la regulación de esta práctica. Este fenómeno no solo subraya la necesidad de una legislación actualizada que pueda mantenerse al ritmo de la tecnología, sino también destaca las brechas en la capacidad de los gobiernos para prevenir la manufactura ilícita y la distribución de armas fabricadas en casa.



El Reporte sobre el Algoritmo de la Anorexia de YouTube

Un estudio reciente emitido por el "**Centro para Contrarrestar el Odio Digital**" (**Center for Countering Digital Hate, CCDH**) ha arrojado luz sobre una problemática creciente en plataformas de video como YouTube. Titulado "El Algoritmo de la Anorexia de YouTube: Cómo YouTube recomienda videos sobre trastornos alimentarios a adolescentes", el informe detalla cómo los algoritmos de recomendación de la plataforma pueden llevar a jóvenes vulnerables hacia un ciclo perjudicial de contenido que glorifica los trastornos alimentarios.

Este hallazgo es alarmante, considerando el aumento global en casos de trastornos alimentarios entre adolescentes. El informe insta a YouTube y otras plataformas a tomar medidas más rigurosas para filtrar y controlar los contenidos que pueden tener consecuencias devastadoras para la salud mental de los usuarios, especialmente los más jóvenes.

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
impulsamos la transformación digital

Mientras cerramos otro mes en ciberseguridad, la innovación sigue siendo clave contra las amenazas. Tecnologías emergentes como la inteligencia artificial adaptativa y el cifrado homomórfico nos preparan mejor para el futuro.

En "Ciberpulso", seguiremos compartiendo los desarrollos más recientes para mantener a nuestra comunidad informada. Agradecemos a nuestros lectores por su interés y participación. Recuerden, en ciberseguridad, el conocimiento es poder y protección.

CONTÁCTANOS:

comunicaciones@aleti.org

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