



CiberPulso

Boletín del Comité de Ciberseguridad



COMITÉ DE CIBERSEGURIDAD
PARA LA REGIÓN

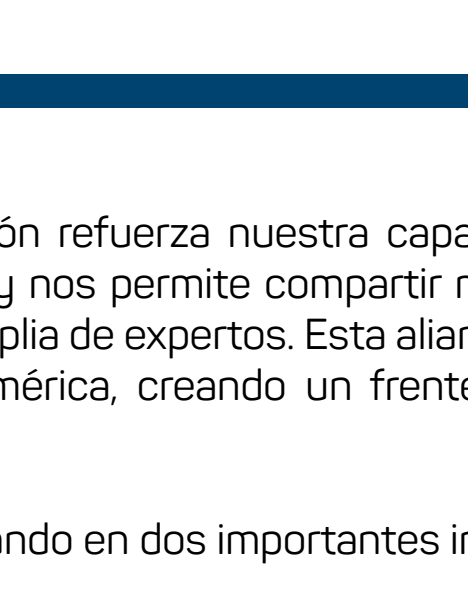


aleti

impulsamos la transformación digital

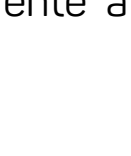
LÍDER COMITÉ DE CIBERSEGURIDAD

Bienvenidos a la edición de septiembre de Ciberpulso. Este mes, celebramos la integración estratégica de nuestro Comité de Ciberseguridad de ALETI con el Comité de Ciberseguridad de AMITI, una alianza que nos permitirá enfrentar de manera conjunta los crecientes desafíos en el ámbito de la ciberseguridad en toda Iberoamérica. Además, profundizaremos en iniciativas clave como el Reporte de Visión Cibersegura de Iberoamérica y la Colaboración Regional para el Intercambio de Información de Inteligencia de Amenazas, que buscan fortalecer la cooperación y mejorar nuestras capacidades de respuesta ante las amenazas cibernéticas.



Ana Cecilia Pérez

Líder del Comité de
Ciberseguridad ALETI



INICIATIVAS

Esta colaboración refuerza nuestra capacidad para enfrentar desafíos comunes en la ciberseguridad y nos permite compartir mejores prácticas, experiencias y recursos con una red más amplia de expertos. Esta alianza fortalecerá el ecosistema de ciberseguridad en toda Iberoamérica, creando un frente unificado frente a las crecientes amenazas cibernéticas.

Estamos trabajando en dos importantes iniciativas:

- Reporte de Visión Cibersegura de Iberoamérica:** A finales de este mes, iniciaremos las mesas de trabajo con las principales organizaciones de la región para definir una estrategia conjunta que impulse la ciberseguridad en todos los sectores. Esta iniciativa busca no solo diagnosticar el estado actual de la seguridad informática, sino también generar recomendaciones accionables que apoyen a los gobiernos y

- Iniciativa de Colaboración Regional para el Intercambio de Información de Inteligencia de Amenazas:** Esta plataforma de colaboración regional permitirá el intercambio rápido y seguro de información sobre amenazas cibernéticas entre nuestros países miembros. El objetivo es aumentar la capacidad de respuesta ante

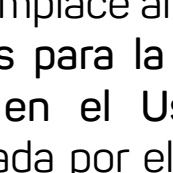
Beneficios



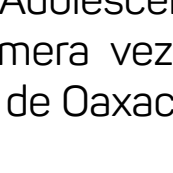
Fortalecimiento de la cooperación entre los países de Iberoamérica, creando una red más robusta de colaboración y respuesta rápida ante ciberamenazas.



Acceso a mejores prácticas compartidas por expertos de AMITI y ALETI, lo que permitirá a las empresas y gobiernos reforzar sus estrategias de ciberseguridad.



Aumento en la capacidad de respuesta ante amenazas cibernéticas gracias a la colaboración regional para la inteligencia de amenazas.



Creación de políticas más efectivas en ciberseguridad, basadas en un diagnóstico regional profundo y recomendaciones claras obtenidas a través del reporte de visión cibersegura.

NOTICIAS DESTACADAS

Implementación de RIAMUSI en Oaxaca, México

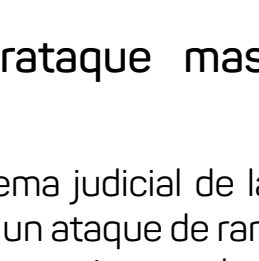
Nos complace anunciar que la Red Iberoamericana de Actores para la Protección de los Derechos de los Niños en el Uso Seguro de Internet (RIAMUSI), impulsada por el Instituto Interamericano del Niño, la Niña y Adolescentes (IIN) de la OEA, se implementará por primera vez en México, específicamente en el estado de Oaxaca.



¿De qué se trata la RIAMUSI?

La RIAMUSI es una iniciativa que busca proteger a la niñez y adolescencia en el entorno digital, promoviendo un uso seguro y responsable de las tecnologías en Iberoamérica. Esta red facilita la colaboración entre diversas organizaciones para educar y concientizar a jóvenes y familias sobre los riesgos en línea y cómo enfrentarlos de manera efectiva. Además, fomenta la creación de políticas públicas que resguarden a las personas menores de edad frente a las ciberamenazas.

Organizaciones participantes:



Estas organizaciones colaborarán en la implementación de RIAMUSI, desarrollando actividades que incluirán capacitaciones, campañas educativas y mesas de diálogo con familias y comunidades en Oaxaca.

Beneficios

Protección de los derechos digitales

La red busca garantizar que niñas, niños y adolescentes puedan navegar de manera segura, protegiendo su privacidad y su bienestar digital.

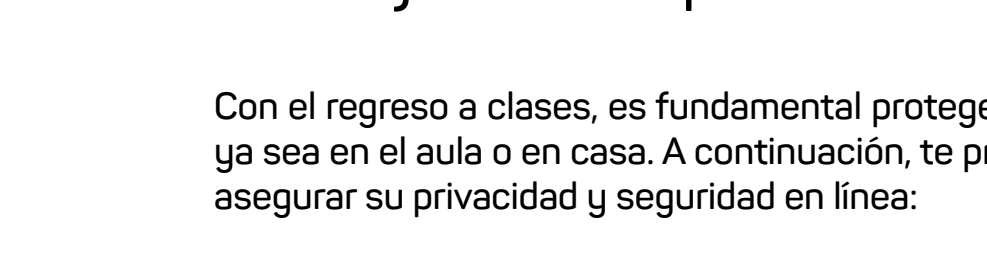
Prevención de riesgos

A través de la educación y concienciación, se enseña a las familias a identificar y prevenir riesgos como el ciberacoso, grooming, y exposición a contenido inapropiado.

Fortalecimiento de políticas públicas

La colaboración entre organizaciones y autoridades locales ayuda a establecer marcos legales y políticas públicas que protejan a los menores en el entorno digital.

Este es un paso fundamental hacia la creación de un entorno digital más seguro para las niñas, niños y adolescentes en México, y refuerza la importancia de la colaboración regional en temas de ciberseguridad y protección digital.



Ransomware: cómo actuar frente a un ciberataque de este tipo.

En los últimos años, los ataques de ransomware crecieron considerablemente a nivel global, transformándose en una de las principales ciberamenazas para los Estados y todo tipo de organización pública o privada, que no posee un plan adecuado de seguridad para proteger sus activos de información.

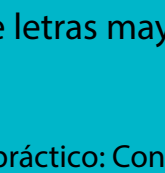
Tal aumento de los ataques ha llevado a la creación de equipos de respuesta en los medios de comunicación, así como también en distintos sitios web especializados en el tema y en las cuentas de redes sociales de las víctimas y de profesionales vinculados con la ciberseguridad, la seguridad de la información o la seguridad informática.

Otras fuentes de divulgación fueron las empresas privadas que ofrecen servicios y/o productos de protección para software. Estas realizaron también informes destacando el crecimiento del uso de este malware, que a fin de evitar el riesgo de vulneración para que luego quien lo usó envíe un pago para quitar esa restricción de acceso.

Argentina sufre ciberataque masivo contra sistema judicial

En agosto de 2024, el sistema judicial de la provincia de Buenos Aires fue víctima de un ataque de ransomware que afectó gravemente las operaciones de tribunales y oficinas judiciales. Los atacantes lograron cifrar información sensible y exigieron un rescate en criptomonedas para liberar los datos.

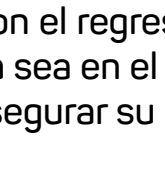
Este incidente dejó paralizadas varias funciones del sistema judicial durante más de una semana, impactando en procesos legales en curso. Las autoridades han respondido implementando medidas de emergencia para mitigar el impacto, mientras continúan investigando la naturaleza y el alcance del ataque.



Lección clave: Este ataque subraya la importancia de proteger los sistemas críticos en las administraciones públicas y la necesidad de mantener actualizados los protocolos de seguridad para mitigar ataques de ransomware.

Chile refuerza su ciberseguridad tras filtración de datos personales

En agosto de 2024, el gobierno de Chile anunció nuevas regulaciones para reforzar la protección de datos personales, tras la filtración masiva de información confidencial de más de 1 millón de ciudadanos. La filtración, que se debió a la vulnerabilidad de una base de datos de un proveedor de servicios de salud, expuso nombres, números de identificación y direcciones de los afectados. Esta violación de datos generó preocupación a nivel nacional sobre la seguridad de las plataformas digitales del sector público y privado.

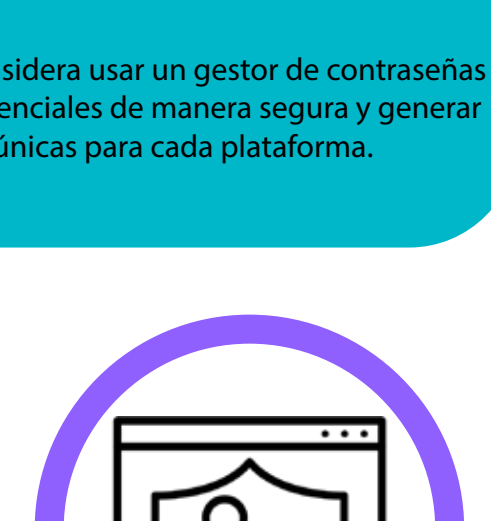


Medidas implementadas: El gobierno chileno introdujo un conjunto de reformas para mejorar la protección de datos, exigiendo estándares más altos de encriptación y controles de acceso en las bases de datos que manejan

RECOMENDACIONES

5 Consejos Claves para la Ciberseguridad en el Regreso a Clases

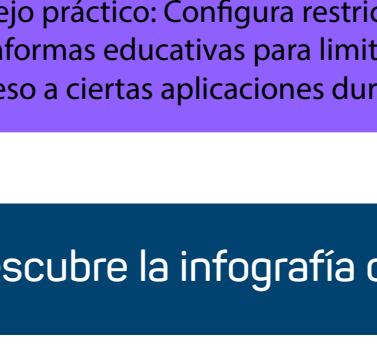
Con el regreso a clases, es fundamental proteger a los niños mientras navegan en el entorno digital, ya sea en el aula o en casa. A continuación, te presentamos cinco recomendaciones esenciales para asegurar su privacidad y seguridad en línea:



Educar sobre el uso seguro de internet

Es crucial que los niños comprendan los riesgos asociados con compartir información personal en línea. Enséñales a no divulgar datos sensibles, como direcciones, números de teléfono o nombres completos, en redes sociales o plataformas de aprendizaje.

Consejo práctico: Recuérdales que no deben aceptar solicitudes de amistad de personas desconocidas y que deben hablar con un adulto antes de descargar aplicaciones o juegos.



Utilizar herramientas de control parental web

El uso de herramientas de control parental permite a los padres y tutores monitorear la actividad en línea de los niños y bloquear el acceso a sitios web inapropiados o peligrosos. Muchos dispositivos y plataformas ofrecen opciones de control parental personalizables que pueden ayudar a proteger a los niños de contenido no deseado.

Consejo práctico: Configura restricciones en dispositivos y plataformas educativas para limitar el tiempo de uso y el acceso a ciertas aplicaciones durante el horario escolar.

Descubre la infografía completa aquí

CÓMO PROTEGERSE ANTE EL PHISHING



El phishing sigue siendo una de las amenazas más comunes y efectivas en el ámbito de la ciberseguridad. Los atacantes envían correos electrónicos fraudulentos que parecen provenir de fuentes confiables, con el objetivo de engañar a los destinatarios para que revelen



La ciberseguridad es un esfuerzo conjunto que requiere la colaboración de todos los miembros de nuestra comunidad. Las amenazas son constantes y evolucionan rápidamente, pero juntos podemos crear un entorno más seguro para nuestras organizaciones y nuestros datos. Continuemos trabajando unidos y compartiendo conocimientos y experiencias para

Agradecemos la información de esta infografía a Juan Pablo Carsi, Socio Director de Capa8



COMITÉ DE CIBERSEGURIDAD
PARA LA REGIÓN



aleti
impulsamos la transformación digital

Estamos comprometidos con fortalecer nuestra comunidad y garantizar que contamos con las herramientas y conocimientos necesarios para enfrentar y prevenir amenazas cibernéticas.

Agradecemos su confianza y participación activa en este esfuerzo conjunto.

CONTÁCTANOS AQUÍ:

seguridaddigital@aleti.org

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

