Junio 2024

CiberPulso

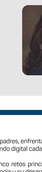
Boletín del Comité de Ciberseguridad

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
Impulsamos la transformación digital

LÍDER COMITÉ DE CIBERSEGURIDAD

Bienvenidos a la edición de junio de Ciberpulso. En este mes reflexionamos sobre los retos adicionales que enfrentamos como padres en el ámbito de la ciberseguridad. Es esencial proteger a nuestros jóvenes navegantes de las amenazas digitales que crecen en complejidad. A lo largo de esta edición, no solo destacaremos las últimas tendencias y desafíos en ciberseguridad, sino que también ofreceremos recursos valiosos para educar y equipar mejor a nuestros niños contra los riesgos cibernéticos.



Ana Cecilia Pérez

Líder del Comité de Ciberseguridad ALETI

¿Qué tan fácil es ser padres de familia cuando nuestros niños son nativos digitales?

Como padres, enfrentamos el desafío constante de mantener a nuestros hijos seguros en un mundo digital cada vez más complejo.

Los cinco retos principales que enfrentan hoy los padres de familia en relación con la tecnología y su desarrollo incluyen:

1. Manejo del tiempo de pantalla: Equilibrar el tiempo que los niños pasan frente a dispositivos electrónicos con actividades fuera de línea.
2. Acceso a contenido inapropiado: Proteger a los niños de contenido dañino o inapropiado mientras navegan en internet.
3. Ciberacoso: Prevenir y manejar situaciones donde los niños pueden ser acosados o acosar a otros en línea.
4. Seguridad de la información personal: Enseñar a los niños a proteger su información personal y entender la importancia de la privacidad en línea.
5. Dependencia tecnológica: Lidiar con la dependencia excesiva de los dispositivos tecnológicos que puede afectar el desarrollo social y emocional de los niños.

Aquí hay algunas reflexiones y estrategias para *ayudar a proteger a los más jóvenes:*

Educación continua
Es fundamental enseñar a los niños sobre los riesgos en línea desde una edad temprana, adaptando las lecciones a su nivel de comprensión.

Uso supervisado
Participar activamente en el uso de tecnologías digitales de nuestros hijos puede ayudar a monitorear y guiar su comportamiento en línea.

Configuraciones de privacidad
Asegurarnos de que las configuraciones de privacidad en dispositivos y aplicaciones estén adecuadamente ajustadas para proteger la información personal de los niños.

Fomentar la comunicación
Crear un ambiente en el que los niños se sientan cómodos compartiendo sus experiencias y preocupaciones en línea con los adultos.

Herramientas de control parental
Utilizar herramientas y aplicaciones de control parental para ayudar a limitar y gestionar el acceso de los niños a contenido inapropiado

Estas estrategias no solo ayudan a proteger a los niños, sino que también promueven un entendimiento más profundo de la tecnología y sus impactos, preparándolos para un futuro digital seguro y responsable.

A continuación te compartimos algunas recomendaciones que te pueden ser útiles para educar a los niños sobre los riesgos cibernéticos, incluyendo un plan especializado:

1. **Plan de Bienestar Digital de Escuelas Ciberseguras**: Un programa estructurado para implementar prácticas seguras en el uso de tecnologías en el entorno educativo.
2. **NetSmartz Workshop**: Ofrece recursos educativos interactivos diseñados por la National Center for Missing & Exploited Children para enseñar a los niños sobre seguridad en línea.
3. **Common Sense Media**: Proporciona guías y actividades para padres y educadores sobre cómo mantener seguros a los niños en internet.
4. **CyberSmart**: Un conjunto de lecciones y actividades gratuitas que fomentan habilidades de navegación segura entre los estudiantes.

RECOMENDACIÓN DE RECURSOS

Con el fin de proveerles de recursos que puedan ser de utilidad les recomendamos:

Kaspersky Cybersecurity Training

Plataforma de formación que ofrece cursos sobre diferentes aspectos de la ciberseguridad, desde conceptos básicos hasta temas avanzados adecuado para mejorar las habilidades de seguridad digital de empleados en cualquier organización.

SANS Cyber Aces Online

Un curso en línea gratuito diseñado para enseñar los conceptos esenciales de ciberseguridad, cubriendo áreas como sistemas operativos, redes y sistemas de control. Es una excelente introducción al mundo de la ciberseguridad para estudiantes y profesionales.

RECOMENDACIÓN DE CURSOS

En nuestro compromiso por fortalecer la seguridad digital y promover el desarrollo profesional continuo, incluimos en nuestro boletín recomendaciones de cursos de ciberseguridad. Estas selecciones abarcan desde fundamentos hasta técnicas avanzadas, adaptándose a las necesidades de profesionales y entusiastas por igual. La formación en ciberseguridad no solo enriquece el conocimiento y las habilidades necesarias para enfrentar las amenazas digitales actuales, sino que también contribuye a la creación de un entorno digital más seguro para todos. Con estas recomendaciones, esperamos brindarte las herramientas necesarias para avanzar en tu carrera y responder eficazmente a los retos de seguridad en este mundo interconectado.

Gestión de Identidades y Accesos [IAM] (LinkedIn Learning)

Aborda los desafíos y soluciones relacionadas con la gestión de identidades y el control de accesos, un área crítica para proteger los recursos de la organización contra accesos no autorizados

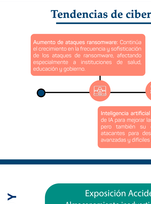
Fuente recomendada: LinkedIn Learning

Protección de Infraestructuras Críticas contra Ciberamenazas [SANS Institute]

Este curso avanzado se enfoca en la protección de infraestructuras críticas, como redes eléctricas y sistemas de agua, contra ciberataques. Es vital para profesionales que trabajan en la seguridad de sectores esenciales.

Fuente recomendada: SANS Institute

NOTICIAS DESTACADAS



Ciberterrorismo y Ciberespionaje: Los conflictos geopolíticos continúan integrando elementos cibernéticos, aumentando el ciberespionaje y los ataques patrocinados por estados. Las tensiones geopolíticas pueden dar lugar a un incremento de los ciberataques, afectando a infraestructuras críticas, sectores gubernamentales y empresas de defensa a nivel mundial.

Retos para el Foro Económico Mundial en 2024: Los desafíos clave identificados por el Foro Económico Mundial incluyen la gestión de la creciente sofisticación de los ataques cibernéticos y la necesidad de una colaboración más fuerte entre el sector público y privado para mejorar la ciberresiliencia. La adopción de nuevas tecnologías y el manejo de la inequidad cibernética son también áreas críticas de enfoque para este año.

Estrategias clave para reforzar la ciberresiliencia en 2024.

Tendencias de ciberseguridad en 2024

Aumento de ataques ransomware: Continua el crecimiento en la frecuencia y sofisticación de los ataques de ransomware, afectando especialmente a instituciones de salud, educación y gobierno.

Seguridad en la nube: Con más empresas migrando a soluciones en la nube, se intensifica la necesidad de proteger datos e infraestructuras en estos entornos frente a violaciones y fugas de información.

2024

Inteligencia artificial en ciberseguridad: Uso de IA para mejorar las defensas cibernéticas, pero también su empleo por parte de atacantes para desarrollar amenazas más avanzadas y difíciles de detectar.

INFOGRAFÍAS INFORMATIVAS

CAUSAS DE BRECHAS DE SEGURIDAD Y FILTRACIÓN DE DATOS

Exposición Accidental en Internet
Almacenamiento inadvertido de datos confidenciales en ubicaciones públicas, como carpetas compartidas en la nube.

Transferencia de Datos Insegura
Falta de control sobre la seguridad de los datos en tránsito, usando protocolos no seguros.

Piratería / Intrusión
Ataques de hackers, incluyendo phishing, malware, y ransomware.

Amenazas Internas
Empleados que abusan de sus permisos o cuentas internas comprometidas sin su conocimiento.

Descubre la infografía completa aquí

Agradecemos la información de esta infografía a Diego González, CEO de Štit Cybersecurity

COMITÉ DE CIBERSEGURIDAD PARA LA REGIÓN

aleti
Impulsamos la transformación digital

Štit Cybersecurity

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

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