BOLETÍN DE CIBERSEGURIDAD EDICIÓN ENERO 2026

REGRESO A CLASES SEGURO

TUS DISPOSITIVOS, TU RED, TU FUTURO

BOLETÍN DE CIBERSEGURIDAD, ENERO DE 2026

“APRENDER ES IMPORTANTE: HACERLO DE FORMA SEGURA, INDISPENSABLE.”

Recomendaciones clave para el inicio de clases:

- Usar contraseñas seguras y únicas para plataformas educativas y correos (evitar repetir contraseñas).
- Desconfiar de correos o mensajes sospechosos que pidan datos personales, contraseñas o enlaces “urgentes”.
- Evitar conectarse a redes Wi-Fi públicas sin protección; si es necesario, no ingresar datos sensibles.
- Mantener actualizados los dispositivos (sistema operativo, antivirus y aplicaciones).
- Padres y docentes: acompañar y orientar a niños y jóvenes sobre el uso responsable y seguro de la tecnología.

FUENTE: SUBDIRECCIÓN DE EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS.

COMPROMISO DE DATOS Y RIESGO DE IDENTIDAD

Exfiltración en Entidades Públicas: Se confirmó la filtración de bases de datos de la Defensoría del Pueblo en la Dark Web. El vector de ataque aprovechó vulnerabilidades en infraestructura heredada (Legacy), comprometiendo Información de Identificación Personal (PII) de funcionarios.

• Comercialización de Datos Ciudadanos: En foros clandestinos se identificó la venta masiva de registros que afectan a 7.1 millones de ciudadanos colombianos, elevando el riesgo de campañas de suplantación y fraude a nivel nacional.

• Fugas de Información por IA Generativa: Se ha detectado que analistas de defensa y contratistas exponen involuntariamente material clasificado, llaves API, tokens de sesión y código fuente al interactuar con plataformas públicas de IA generativa sin los debidos controles de seguridad.

FUENTE: BOLETÍN INFORMATIVO CSIRT AMÉRICAS

EVOLUCIÓN EN LA DISTRIBUCIÓN DE MALWARE

Los adversarios han sofisticado sus tácticas de evasión mediante el uso de técnicas de Geofencing (Geocercado) para evitar el análisis técnico:

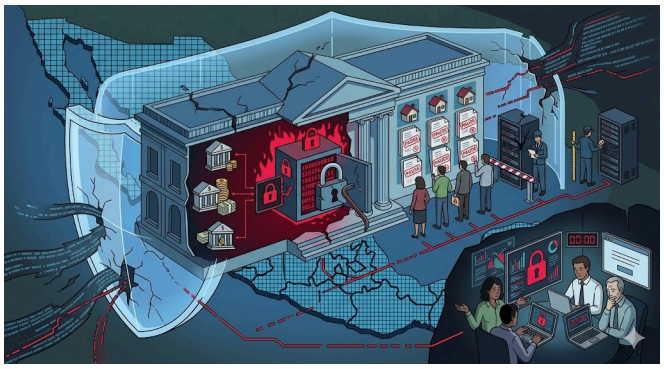
• Campaña "DeepSeek" bajo demanda: Se identificó la distribución de instaladores falsos del modelo de IA DeepSeek. La amenaza utiliza un filtrado por dirección IP: si la petición se origina fuera de Colombia o Latinoamérica, el servidor entrega un archivo benigno.

• Evasión de Sandboxing: Esta táctica de geolocalización permite que el malware evite ser detectado por sistemas de análisis automático y sandboxing ubicados usualmente en Estados Unidos y Europa, asegurando que el payload malicioso solo se ejecute en el objetivo geográfico previsto.

CSIRT DEFENSA

FUENTE: BOLETÍN INFORMATIVO CSIRT AMÉRICAS

ATAQUE CIBERNÉTICO A LA SOCIEDAD HIPOTECARIA FEDERAL PARALIZA TRÁMITES DE AVALÚOS



El sitio de la Sociedad Hipotecaria Federal habría sufrido un hackeo. De momento, los procesos están en pausa ante un posible secuestro de información.
Esta dependencia regula los créditos hipotecarios en el país, para los bancos "es el banco de los bancos".

Diego Martín González Almanza, presidente del Clúster de Tecnologías de la Información de Guanajuato (CLUTIG), explicó que la página aparece como activa, pero es una carátula, ya que las bases de datos y la información de la dependencia está encriptada.

El presidente del Clutig reconoció que si bien no ha habido un posicionamiento oficial, el sitio está caído. "Lo que hicieron fue desconectar los equipos y están trabajando con laptops, mientras deciden si pagan o no".

FUENTE: AM.COM.MX

BARÓMETRO DE RIESGOS DE ALLIANZ 2026: EL CIBERESPACIO SIGUE SIENDO EL PRINCIPAL RIESGO EMPRESARIAL, PERO LA IA ASCIENDE MÁS RÁPIDO AL SEGUNDO PUESTO

- Los ataques cibernéticos, especialmente los de ransomware, se clasifican como el riesgo número uno por quinta vez consecutiva para empresas de todos los tamaños (42 % de las respuestas a nivel mundial).
- La inteligencia artificial (IA) es la que más sube y pasa del puesto 10 al 2 (32%), lo que pone de relieve los riesgos emergentes para las empresas de casi todos los sectores industriales.
- La agitación geopolítica y la incertidumbre empujan los riesgos políticos y la violencia a su posición más alta hasta la fecha, en el puesto número 7.

FUENTE: ALLIANZ.COM

MARTES DE PARCHES DE MICROSOFT DE ENERO DE 2026: 115 VULNERABILIDADES CORREGIDAS

Microsoft lanzó su primer Martes de Parches de 2026 , con una gran cantidad de correcciones de seguridad para proteger a los usuarios de diversas amenazas digitales. Este mes, el gigante tecnológico abordó 115 vulnerabilidades, de las cuales ocho se consideran críticas (el nivel de riesgo más alto), mientras que 106 se consideran importantes.

Para quienes no estén familiarizados con el término, el Martes de Parches es el día en que Microsoft publica actualizaciones regularmente para corregir vulnerabilidades de seguridad. Este enero, las actualizaciones abarcan todo, desde Windows 11 y Microsoft Office hasta el navegador Edge.

FUENTE: HACKREAD.COM