GUÍA DE CYBER-SEGURIDAD

APOYO UNNIO EN CASO DE EMERGENCIAS – Tenemos una red de expertos para responder a usted en caso de incidentes.
En caso de un incidente en su seguridad, por favor comuníquese con nuestra línea de Emergencias Cibernéticas disponible 24/7: **+56 2 2483 8910**

ADVERTENCIA: Este documento es un conjunto de buenas prácticas y debe ser considerado como recomendaciones generales de seguridad. Unnio no asume ninguna responsabilidad en cuanto a estas recomendaciones, solo los términos y las condiciones de los servicios y el Seguro pactados son obligatorios. Contacte a Unnio o a su corredor de seguros en caso de consultas sobre su contrato y al equipo de apoyo cibernético en caso de un incidente.

LO QUE SE DEBE Y NO SE DEBE HACER EN CYBER-SEGURIDAD

- ✓ Mantenga sus sistemas y software actualizados (especialmente sus sistemas operativos) idealmente permitiendo actualizaciones automáticas.
- ✓ Mantenga un firewall configurado correctamente para proteger su red de internet, así como de sus Wi-Fi de visita.
- ✓ Ejecute una aplicación de protección de malware (por ejemplo aplicación de antivirus) en todos sus equipos y sistemas de correo electrónico y habilite las actualizaciones automáticas de firmas.
- ✓ Prepare regularmente una copia de seguridad (diaria, semanal, mensualmente) de todos sus datos críticos e importantes. Almacene las copias de seguridad en un edificio separado o nube desconectada de toda su red. También, de vez en cuando compruebe si puede restaurar los datos de las copias de seguridad.

- ✗ No confíe en nadie. Siempre piense antes de actuar, por ejemplo antes de copiar, almacenar o abrir documentos o enviar datos confidenciales o fondos.
- ✗ No abra ningún adjunto sospechoso.
- ✗ No comparta claves con otras cuentas o personas.
- ✗ No almacene o transfiera información encriptada confidencial
- ✗ No conecte dispositivos USB, tarjetas SD u otros dispositivos a su computador sin verificar de donde proviene el dispositivo y si su fuente es confiable.

LO QUE SE DEBE Y NO SE DEBE HACER EN RESPUESTA DE INCIDENTE DE CYBER-SEGURIDAD

EXTORCIÓN (Ej. Ransomware)

- ✓ Tome una foto del correo / nota de rescate con un teléfono inteligente o una cámara.
- ✓ Desconecte los sistemas infectados de cada red (por ejemplo la red Wi-Fi, Bluetooth y LAN).
- ✓ Llame la Línea de Emergencia cibernética de Unnio
- ✗ No pague ningún dinero o monedas digitales
- ✗ No responde a ningún correo electrónico.

INFECCIÓN POR MALWARE (Ej. Troyano o virus)

- ✓ Aísle la red o el sistema infectado del resto de la red.
- ✓ Escanee el sistema infectado con una aplicación antivirus con firmas actualizadas.
- ✓ Llame la Línea de Emergencia cibernética de Unnio.
- ✗ No apague el sistema infectado.
- ✗ No conecte un dispositivo USB desde el sistema infectado a un sistema no infectado.

VIOLACIÓN DE DATOS (Ej. Cuando datos de tarjeta de crédito o nombres de usuario / contraseñas son robadas)

- ✓ Inmediatamente llame la Línea de Emergencia cibernética de Unnio
- ✓ Sea transparente y cooperativo.

CIBER-CRIMEN (Ej. Transacción no autorizada)

- ✓ Informe a su banco, compañía de pago o empresa de e-wallet y bloquee / cancele los datos de la tarjeta a través de una llamada telefónica a su banco o a través del portal de banca en línea.
- ✓ Bloquee / cambie las credenciales para su aplicación bancaria y otra información de cuenta relacionada con transacciones financieras.
- ✓ Reporte el caso a la policía.
- ✓ Llame la Línea de Emergencia cibernética de Unnio.
- ✗ No comparta con nadie su PIN/TAN, datos de tarjeta de crédito u otra información confidencial.