POLÍTICA DE DIVULGACIÓN RESPONSABLE

En IPLAN, creemos que la seguridad de los datos de nuestros usuarios es muy importante, y por eso alentamos a aquellas personas que hayan descubierto potenciales vulnerabilidades de seguridad que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información de nuestros Clientes o de IPLAN en general, a que se contacten con nosotros y nos informen sobre ello de manera responsable.

Antes de reportar un error o hallazgo, te pedimos que cumplas con la política de divulgación responsable que detallamos a continuación:

- Antes de hacer pública o compartir la información del reporte, es importante que te comuniques con nosotros siguiendo los 3 pasos que detallamos a continuación:

1. Envianos un correo electrónico a csirt@iplan.com.ar e incluí "Divulgación Responsable" en el asunto.
2. En el cuerpo del correo electrónico, describí la naturaleza del error o hallazgo, identificá los pasos requeridos para replicarlo, las aplicaciones, programas o herramientas que utilizaste para detectar la vulnerabilidad y la fecha y hora en que realizaste las pruebas. De ser posible, adjuntá imágenes y/o videos de lo detectado.
3. Por favor, incluí tus datos para que podamos contactarnos con vos.

- No expongas la privacidad de otras personas (físicas o jurídicas), por ejemplo, mediante el acceso no autorizado a datos y/o su destrucción, y/o la interrupción y/o degradación de nuestros servicios.

- No accedas y/o modifiques cuentas sin el consentimiento del propietario.

- No te aproveches del problema de seguridad intentando demostrar que existen riesgos adicionales para descubrir más problemas.

- No accedas a nuestra información sensible, por ejemplo, datos de Clientes, Proveedores y/o de IPLAN, ya que no estás autorizado a hacerlo.

Si consideras que descubriste una vulnerabilidad de seguridad en el sitio de IPLAN (u otros sitios relacionados a IPLAN), comunicate con nosotros, así de esta manera podemos investigar lo que reportes y resolver el problema rápidamente.

Las siguientes acciones no están dentro del alcance de nuestra política de divulgación responsable ya que pueden afectar de forma perjudicial a IPLAN:

- Spam o técnicas de ingeniería social.
- Ataques por denegación de servicio.
- Inyección de código o contenido.
- Ataques por fuerza bruta.

- Escaneos de vulnerabilidad manuales o automatizados.
- Las investigaciones llevadas a cabo por menores, personas en listas de sanciones o personas en países con listas de sanciones.
- Publicar, actualizar, vincular, enviar o almacenar deliberadamente malware, virus o software similares dañinos

IPLAN no recompensa económicamente a las personas u organizaciones por identificar vulnerabilidades potenciales o confirmadas. Las solicitudes de remuneración monetaria serán consideradas una violación de esta Política de divulgación responsable.

En IPLAN tenemos un fuerte compromiso con la seguridad y agradecemos tus aportes de divulgación responsable, es por ello que a todos los investigadores de seguridad que cumplen esta Política de divulgación responsable, IPLAN se compromete a:

- agradecerles la recepción de su informe de forma oportuna;
- brindarles un marco de tiempo estimado para contemplar la vulnerabilidad;
- notificarles cuando se soluciona la vulnerabilidad;
- reconocer públicamente su revelación responsable, si así lo desean.