POLITICA 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 a que se contacten con nosotros y nos informen sobre ello de manera responsable.

El objeto de esta Política es fomentar los reportes que nos ayuden a proteger la infraestructura, sistemas y datos, ayudando a evitar la afectación de la Confidencialidad, Integridad y/o Disponibilidad de la información de nuestros Clientes, Proveedores, o de IPLAN en general.

Por ello, en caso de que hayas descubierto alguna potencial vulnerabilidad, te invitamos a que nos reportes la misma respetando los lineamientos que detallamos a continuación:

- Antes de hacer público tu descubrimiento, es importante que te comuniques con nosotros para darnos la oportunidad de analizarlo y en el caso que sea posible, solucionar o parchear el problema.

- Para comunicarte con nosotros envíanos un correo electrónico a **csirt@iplan.com.ar** y 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.

- Por favor, incluí tus datos para que podamos contactarnos con vos en caso de necesitar realizar alguna consulta extra y/o para enviarte un correo oficial y formal reconociendo tu aporte.

Adicionalmente, te dejamos una serie de **recomendaciones prácticas para poder reportar tu hallazgo** de la mejor forma:

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

- No expongas nunca la privacidad de otras personas, por ejemplo, difundiendo datos personales como correos electrónicos, teléfonos, etc.

- En el caso que por el descubrimiento realizado, te hayas encontrado con información confidencial, evita nuevos accesos y no modifiques ni descargues información.

- Evita aprovecharte de la brecha de seguridad para demostrar posibles nuevos problemas adicionales (que son consecuencia del problema original)

- Recuerda que hay acciones que no están dentro del alcance de nuestra Política de Divulgación Responsable ya que pueden afectar de forma perjudicial a IPLAN.

Algunas de las **acciones prohibidas** para el descubrimiento de vulnerabilidades, son:

- Spam o técnicas de ingeniería social.

- Ataques por denegación de servicio.
- Inyección de código o contenido.
- Ataques por fuerza bruta.
- Las investigaciones llevadas a cabo por menores, personas en listas de sanciones o personas en países con listas de sanciones.
- Acciones deliberadas que impliquen la utilización de malware, virus o software similares dañinos.

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:

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

Por último, recuerda que 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.

VIGENCIA

La presente política se encuentra vigente a partir de la fecha de su publicación.

Última actualización: 26/07/2021.