

POLÍTICA DE DIVULGACIÓN RESPONSABLE DE VULNERABILIDADES

REVISIONES DE LA POLÍTICA

Nº Revisión	Fecha	Motivo de la revisión
01	Octubre 2026	Creación de la política para establecer el canal público de reporte de vulnerabilidades y el proceso de gestión de dichos reportes.

I.- OBJETIVO

GrupoExpro reconoce el valor de la colaboración de investigadores de seguridad, clientes, proveedores y público en general para identificar vulnerabilidades en sus sistemas. La presente política establece el canal oficial para reportarlas, las reglas que deben respetar quienes las reporten y el proceso mediante el cual GrupoExpro las recibe, evalúa, corrige y comunica.

Esta política complementa la Política de Gestión de Incidentes de Seguridad de la Información (0087) y el Anexo de Gestión de Vulnerabilidades y Pentesting (018).

II.- ALCANCE

Esta política aplica a los sistemas, aplicaciones y servicios de información de propiedad de GrupoExpro o administrados por ella, incluidos sus sitios web y las aplicaciones expuestas a internet.

Quedan fuera del alcance:

- Sistemas de proveedores externos (por ejemplo, plataformas SaaS utilizadas por GrupoExpro). Las vulnerabilidades en estos sistemas deben reportarse directamente al proveedor correspondiente.
- Sistemas de clientes, incluso cuando el personal de GrupoExpro opere en ellos. Si un colaborador de GrupoExpro detecta una vulnerabilidad en sistemas de un cliente, la reportará por el canal interno de incidentes (Política 0087) y GrupoExpro la comunicará al cliente conforme a los acuerdos contractuales vigentes.
- Ataques de ingeniería social o phishing dirigidos a colaboradores, y pruebas sobre la seguridad física de las instalaciones.

III.- CANAL DE REPORTE

Las vulnerabilidades deben reportarse al correo electrónico ciberseguridad@grupoexpro.com. Este canal también se publica en el archivo security.txt del sitio web corporativo, conforme al estándar RFC 9116.

Para facilitar la evaluación, el reporte debería incluir:

- Descripción de la vulnerabilidad y del sistema, URL o componente afectado.
- Pasos para reproducirla y, si corresponde, una prueba de concepto.
- Impacto potencial estimado.
- Datos de contacto para el seguimiento (opcional; se aceptan reportes anónimos).

El reporte no debe incluir datos personales ni información confidencial de terceros más allá de lo estrictamente necesario para demostrar la vulnerabilidad.

IV.- REGLAS PARA QUIENES REPORTAN

Quien investigue y reporte una vulnerabilidad debe actuar de buena fe y limitarse a lo necesario para demostrar su existencia. En particular, no está permitido:

- Acceder, modificar, copiar o eliminar datos que no le pertenezcan. Si accede accidentalmente a datos personales o confidenciales, debe detenerse, reportarlo y no conservar copia alguna.
- Realizar ataques de denegación de servicio o acciones que degraden la disponibilidad de los sistemas.
- Ejecutar escaneos automatizados de alto volumen.
- Instalar puertas traseras, mantener accesos persistentes o explotar la vulnerabilidad más allá de lo necesario para demostrarla.
- Divulgar públicamente la vulnerabilidad antes de lo previsto en la sección VII.
- Exigir pagos o beneficios a cambio de la información.

V.- COMPROMISOS DE GRUPOEXPRO

Ante un reporte recibido por el canal oficial, GrupoExpro se compromete a:

- **Acuse de recibo:** acusar recibo en un plazo máximo de 5 días hábiles;
- **Evaluación:** realizar una evaluación inicial y clasificar la criticidad de la vulnerabilidad en un plazo máximo de 10 días hábiles desde su recepción;
- **Seguimiento:** informar al reportante sobre el avance y el cierre de la gestión;
- **Confidencialidad:** mantener reservada la identidad del reportante, salvo que autorice lo contrario o que la ley lo exija;
- **Reconocimiento:** con autorización del reportante, reconocer públicamente su contribución.

GrupoExpro no ofrece recompensas económicas por los reportes recibidos.

Las vulnerabilidades confirmadas se corregirán según su criticidad, con los siguientes plazos objetivo desde su confirmación:

Criticidad	Plazo objetivo de corrección o mitigación
Crítica	15 días corridos
Alta	30 días corridos
Media	90 días corridos
Baja	Próximo ciclo de mantenimiento planificado

Cuando la corrección definitiva no sea factible en el plazo objetivo, se aplicarán controles compensatorios y se documentará el plan de corrección.

VI.- PUERTO SEGURO

GrupoExpro no iniciará acciones legales contra quien investigue y reporte una vulnerabilidad de buena fe y en cumplimiento de esta política, en la medida en que la

legislación aplicable lo permita. Esta protección no se extiende a sistemas de terceros ni a conductas que infrinjan las reglas de la sección IV.

VII.- DIVULGACIÓN COORDINADA

El reportante se compromete a no divulgar públicamente la vulnerabilidad hasta que haya sido corregida o hasta que transcurran 90 días corridos desde su reporte, lo que ocurra primero, salvo que se acuerde otro plazo con GrupoExpro.

Si la vulnerabilidad afecta o pudo afectar información de clientes, GrupoExpro la tratará como un incidente de seguridad conforme a la Política 0087 y notificará a los clientes afectados en los plazos y por los canales establecidos en los respectivos contratos.

VIII.- GESTIÓN INTERNA DE LOS REPORTE

- **Responsable:** El Encargado de Ciberseguridad recibe los reportes, los registra en el sistema de tickets definido en la Política 0087 y es responsable de su gestión hasta el cierre.
- **Evaluación y asignación:** se valida la vulnerabilidad, se clasifica su criticidad y se asigna su corrección al responsable del sistema afectado.
- **Verificación:** una vez aplicada la corrección, el Encargado de Ciberseguridad verifica su eficacia antes de cerrar el reporte.
- **Escalamiento:** si existen indicios de que la vulnerabilidad fue explotada, se activa de inmediato el procedimiento de la Política 0087.
- **Registro y mejora:** se mantiene un registro de cada reporte con su fecha de recepción, criticidad, acciones realizadas y fecha de cierre. Las causas recurrentes se incorporan al proceso de gestión de vulnerabilidades (Anexo 018).

IX.- PUBLICACIÓN Y REVISIÓN

Esta política se publica en el sitio web corporativo de GrupoExpro, y su canal de reporte se publica además en el archivo /.well-known/security.txt del mismo sitio. Se revisará al menos una vez al año o ante cambios significativos en los sistemas o en el canal de reporte.