1. Propósito

El presente Procedimiento de Canal de Denuncias establece los lineamientos para recibir, registrar, analizar, investigar y cerrar denuncias relacionadas con conductas irregulares, incumplimientos normativos, riesgos de ciberseguridad, uso indebido de activos tecnológicos, afectación de información confidencial, vulneración de controles internos o cualquier hecho que pueda comprometer la integridad, continuidad, reputación o cumplimiento de NOVARED.

Este procedimiento busca asegurar un tratamiento objetivo, confidencial, trazable y oportuno de las denuncias, manteniendo estándares de legalidad, probidad, ética profesional, protección de datos, seguridad de la información y cumplimiento corporativo.

2. Objetivo

NOVARED pone a disposición de sus colaboradores, proveedores, clientes, partners, contratistas y terceros relacionados un Canal de Denuncias destinado a informar, de manera segura y responsable, situaciones que puedan implicar fraude, corrupción, robo, uso no autorizado de información, acceso indebido a sistemas, fuga de datos, abuso de privilegios, manipulación de evidencias digitales, conflicto de interés, incumplimiento contractual, incumplimiento de políticas de seguridad o infracciones asociadas a la Ley N° 20.393 y demás normativa aplicable.

El canal permite contar con un mecanismo confiable para reportar hechos que requieran análisis interno, investigación, preservación de evidencia, escalamiento legal, adopción de medidas correctivas o activación de protocolos de respuesta ante incidentes.

3. Alcance

Este procedimiento aplica a todos los trabajadores de NOVARED, cualquiera sea su modalidad de contratación, así como a proveedores, clientes, practicantes profesionales, consultores, subcontratistas, partners tecnológicos, terceros con acceso a infraestructura, plataformas, información, servicios gestionados, ambientes de cliente o sistemas internos.

También aplica a hechos relacionados con servicios de monitoreo de seguridad, SOC, CSOC, respuesta a incidentes, threat intelligence, consultoría, auditoría, ethical hacking, gestión de vulnerabilidades, administración de plataformas de seguridad, soporte, desarrollo, automatización, operación cloud, redes, endpoints, SIEM, SOAR, EDR, XDR, firewalls, IPS, WAF, antispam, antimalware, bases de datos, repositorios de código y cualquier activo tecnológico administrado por NOVARED.

4. Principios rectores

Confidencialidad: La identidad del denunciante y los antecedentes entregados se protegerán conforme a la normativa vigente, políticas internas y necesidad de conocimiento.

No represalia: NOVARED no tolerará represalias contra personas que presenten denuncias de buena fe o colaboren en una investigación.

Trazabilidad: Toda denuncia deberá contar con registro, clasificación, responsables, plazos, evidencias relevantes, decisiones adoptadas y resultado documentado.

Imparcialidad: Las investigaciones deberán realizarse con objetividad, respeto a la presunción de inocencia y separación de funciones cuando exista conflicto de interés.

Integridad de evidencia: La información técnica, correos, logs, artefactos, capturas, indicadores de compromiso o registros de sistemas deberán preservarse evitando alteraciones.

Proporcionalidad: Las medidas adoptadas deberán ser razonables, fundadas y proporcionales al riesgo, impacto y gravedad de los hechos.

5. Responsables

El Encargado de Prevención de Delitos, Oficial de Cumplimiento o la función que NOVARED designe será responsable de administrar el Canal de Denuncias, recibir los reportes, coordinar su análisis, determinar su admisibilidad y activar las investigaciones que correspondan.

Cuando la denuncia tenga componente tecnológico o de ciberseguridad, podrá requerirse apoyo del área de Seguridad de la Información, SOC/CSOC, Legal, Recursos Humanos, Auditoría, Riesgo, Continuidad Operacional, Protección de Datos o del equipo técnico especializado que corresponda.

Cuando el hecho denunciado involucre infraestructura, información o servicios de clientes, el tratamiento deberá considerar las obligaciones contractuales, acuerdos de confidencialidad, acuerdos de nivel de servicio, normativa de protección de datos y procedimientos de notificación aplicables.

6. Materias denunciables

Las denuncias podrán referirse, entre otras, a las siguientes situaciones:

- Fraude, cohecho, corrupción entre particulares, negociación incompatible, administración desleal, lavado de activos, financiamiento del terrorismo, receptación u otros delitos contemplados en la Ley N° 20.393.
- Acceso no autorizado a sistemas, credenciales, consolas, plataformas de cliente, repositorios, bases de datos, herramientas SOC, SIEM, SOAR, EDR, XDR, firewalls, plataformas cloud o ambientes productivos.
- Exfiltración, divulgación, copia, retención, destrucción o uso indebido de información confidencial, datos personales, datos de cliente, documentación técnica, reportes de incidentes, inteligencia de amenazas o evidencias digitales.
- Uso indebido de privilegios, cuentas compartidas, credenciales administrativas, llaves API, tokens, certificados, secretos, claves de cifrado o accesos temporales.
- Manipulación, eliminación o alteración de logs, bitácoras, artefactos, indicadores de compromiso, evidencias forenses, tickets, casos, informes técnicos o registros de auditoría.
- Incumplimiento de políticas de seguridad, hardening, segregación de funciones, gestión de cambios, respuesta a incidentes, clasificación de información, continuidad operacional, desarrollo seguro o control de accesos.
- Conflictos de interés, regalos indebidos, relaciones comerciales no transparentes o favorecimiento irregular de proveedores, clientes, candidatos, partners o terceros.
- Robo, hurto, pérdida o uso no autorizado de equipos, notebooks, dispositivos móviles, tokens físicos, medios extraíbles, documentos, licencias o servicios de NOVARED.
- Conductas que afecten el ambiente laboral, acoso, discriminación, hostigamiento, abuso de autoridad o incumplimiento del Código de Conducta.
- Cualquier otra situación irregular que pueda comprometer la ética, seguridad, reputación, cumplimiento, continuidad o confianza de NOVARED y sus clientes.

7. Antecedentes recomendados para una denuncia

Para facilitar el análisis, el denunciante deberá aportar, en la medida de lo posible, antecedentes claros, verificables y ordenados. La falta de identificación del denunciante no impedirá el análisis de una denuncia anónima, siempre que existan antecedentes suficientes para iniciar la revisión.

- Identificación del denunciante, cuando desee entregarla: nombre, correo electrónico, teléfono o área de pertenencia.
- Fecha, hora, lugar, sistema, plataforma, cliente, servicio o activo afectado.
- Descripción clara de los hechos y forma en que tomó conocimiento de ellos.
- Personas, áreas, proveedores, cuentas, sistemas o terceros presuntamente involucrados.
- Evidencias disponibles: correos, capturas, tickets, logs, alertas SIEM, hashes, URLs, IPs, dominios, archivos, reportes, contratos, órdenes de compra, comunicaciones o registros de acceso.
- Impacto observado o potencial: pérdida de confidencialidad, indisponibilidad, afectación de integridad, incumplimiento contractual, daño reputacional, impacto legal o riesgo para clientes.

8. Canales de recepción

Las denuncias podrán recibirse por los canales formales que NOVARED defina y comunique internamente, incluyendo formulario web corporativo, correo electrónico habilitado para denuncias, comunicación escrita confidencial o los medios establecidos por la compañía para cumplimiento, ética, seguridad y gestión de incidentes.

Cuando el reporte corresponda a un incidente de ciberseguridad activo o con riesgo operacional inmediato, deberá activarse además el procedimiento de respuesta a incidentes, sin perjuicio del registro de la denuncia en este canal.

9. Procedimiento de gestión de denuncias

El flujo de gestión considera las siguientes etapas:

Etapa	Descripción
Recepción y registro	La denuncia se registra con fecha, hora, canal de ingreso, clasificación preliminar, criticidad inicial y responsable asignado. Si existe riesgo inmediato de ciberseguridad, se activa el escalamiento técnico correspondiente.
Análisis de admisibilidad	Se revisa si los antecedentes permiten iniciar investigación, si corresponde derivación operativa o si se requieren antecedentes adicionales. Las denuncias de alto riesgo deberán priorizarse.
Investigación	Se recopilan antecedentes, se preserva evidencia, se entrevista a las personas necesarias, se revisan registros técnicos y se documentan hallazgos. La investigación deberá ejecutarse con confidencialidad, imparcialidad y respeto a los derechos de las partes.

Etapa	Descripción
Comunicación a persona denunciada	Cuando proceda y sin comprometer la investigación, se informarán los hechos investigados a la persona denunciada, otorgándole oportunidad razonable para presentar antecedentes, descargos o evidencias.
Resolución	Se emite una conclusión fundada y se definen medidas correctivas, preventivas, disciplinarias, legales o de fortalecimiento de controles.
Seguimiento	Se verifica el cumplimiento de las medidas definidas, se actualiza el registro y se integran aprendizajes al sistema de gestión de seguridad, cumplimiento y mejora continua.

10. Protección de denunciantes y personas involucradas

NOVARED resguardará la identidad del denunciante y de las personas involucradas, salvo obligación legal, requerimiento de autoridad competente o necesidad estrictamente justificada para el desarrollo de la investigación.

Se prohíbe cualquier represalia, amenaza, presión, discriminación o consecuencia laboral adversa contra quien formule una denuncia de buena fe, aporte antecedentes o colabore en una investigación.

La presentación deliberada de denuncias falsas, maliciosas o destinadas a perjudicar a otra persona, cliente, proveedor o a la reputación de NOVARED podrá ser considerada una falta grave y dar lugar a las medidas disciplinarias o legales que correspondan.

11. Tratamiento de evidencia digital

Cuando la denuncia incluya evidencia técnica, deberán aplicarse criterios de preservación, trazabilidad y cadena de custodia adecuados al caso. Esto puede incluir respaldo de logs, exportación de eventos SIEM, hash de archivos, conservación de correos, snapshots, tickets, registros de acceso, capturas, indicadores de compromiso, reportes de herramientas de seguridad y documentación de las acciones ejecutadas.

La evidencia deberá almacenarse en repositorios autorizados, con control de acceso, registro de modificaciones y protección contra alteración, eliminación o divulgación no autorizada.

12. Cierre, resolución y medidas correctivas

Concluida la investigación, el responsable deberá emitir una resolución fundada que indique los hechos analizados, antecedentes revisados, resultados, conclusiones, medidas correctivas, acciones preventivas y responsables de seguimiento.

Cuando corresponda, las medidas podrán incluir ajustes de control, bloqueo o rotación de credenciales, cambios de configuración, refuerzo de monitoreo, capacitación, acciones disciplinarias, comunicaciones a clientes, denuncias ante autoridad competente, acciones legales, mejora de procedimientos, actualización de políticas o fortalecimiento de controles de ciberseguridad.

Toda denuncia deberá contar con estado final documentado: válida, no válida, no concluyente, derivada, cerrada por insuficiencia de antecedentes o cerrada por otra causal fundada.

13. Registro, indicadores y mejora continua

El responsable del canal mantendrá un registro centralizado de denuncias, con acceso restringido, que permita seguimiento, auditoría, generación de indicadores y control de plazos.

El registro deberá considerar, a lo menos: fecha de recepción, tipo de denunciante, área involucrada, clasificación del hecho, criticidad, responsable asignado, estado, fechas relevantes, evidencia asociada, resultado, medidas adoptadas y fecha de cierre.

Los aprendizajes derivados de denuncias confirmadas deberán incorporarse al ciclo de mejora continua de NOVARED, incluyendo revisiones de riesgos, controles, concientización, procedimientos de respuesta, hardening, automatizaciones, monitoreo y controles de cumplimiento.

14. Conocimiento y cumplimiento

Todo colaborador de NOVARED deberá conocer, respetar y aplicar este procedimiento. Las jefaturas y responsables de área deberán promover su difusión, asegurar la colaboración con las investigaciones y reforzar la importancia de reportar oportunamente cualquier situación irregular.

El incumplimiento de este procedimiento, de las políticas de seguridad, del Código de Conducta o de las normas internas aplicables podrá dar lugar a medidas disciplinarias, contractuales o legales, según la gravedad del hecho y la normativa vigente.