SECTOR-7

Securing the Truth. Protecting You.

Directrices de seguridad de la plataforma de denuncia de irregularidades del Sector-7

Versión: 1.0

Fecha: 28 de marzo de 2025

Clasificación: PÚBLICA

Tabla de contenido

---

1. Introducción

Descripción general:

Sector-7 se compromete a mantener los más altos estándares de seguridad, confidencialidad y transparencia para cualquier persona que denuncie prácticas poco éticas o ilegales. Nuestra plataforma de denuncia garantiza que todas las denuncias se gestionen con una sólida protección de datos y procedimientos claros de respuesta a incidentes.

Objetivo:
Este documento describe las pautas de seguridad que rigen el envío de informes, la gestión y privacidad de los datos recopilados, los protocolos de respuesta a incidentes (tanto internos como externos) y las mejores prácticas para mantener el anonimato al presentar informes.

Alcance y audiencia:
Estas directrices se aplican a todos los empleados, contratistas y partes interesadas externas que utilizan la plataforma Sector-7. El documento está dirigido tanto a los usuarios que presentan denuncias como a los equipos internos responsables de la gestión e investigación de denuncias.

---

2. Directrices para la presentación de informes

Descripción general

Denunciar conductas indebidas de forma rápida y segura es esencial para un entorno transparente y ético. Sector-7 ofrece canales seguros que garantizan la confidencialidad y la tramitación rápida de las denuncias.

Canales de denuncia

- Portal web seguro: utilice nuestro formulario de envío en línea encriptado.
- Correo electrónico seguro: informes por correo electrónico a [redacted] utilizando encriptación PGP.

Pasos para presentar un informe

1. Acceda a la Plataforma: Inicie sesión en su cuenta utilizando la autenticación multifactor.
2. Complete el formulario de informe: proporcione una descripción detallada del incidente, incluyendo fecha, hora, lugar y cualquier evidencia de respaldo.
3. Elija el modo de informe: seleccione si desea informar de forma anónima o con su identidad adjunta.
4. Envíe de forma segura: confirme el envío y reciba un número de seguimiento único.

Mejores prácticas

- Verifique sus datos dos veces: asegúrese de que toda la información sea precisa antes del envío.
- Utilice canales cifrados: utilice siempre las opciones seguras designadas para evitar fugas de datos
- Informar oportunamente: Informar tan pronto como tenga conocimiento de cualquier posible marcha mala.

Preguntas frecuentes

- P: ¿Cómo se protege mi identidad?
  R: Los informes se pueden enviar de forma anónima, e incluso si decide revelar su identidad, se aplican estrictas medidas de confidencialidad.
- P: ¿Puedo adjuntar documentos de forma segura?
  R: Sí, el portal admite cargas de archivos encriptados.

---

3. Tratamiento de datos y privacidad

Descripción general

Sector-7 se compromete a proteger todos los datos proporcionados por los denunciantes. Cumplimos con los estándares globales de protección de datos (incluidos el RGPD y la norma ISO 27001) para garantizar la confidencialidad, integridad y disponibilidad de la información sensible.

Recopilación de datos

- Lo que recopilamos: identificadores personales (si se proporcionan), detalles del incidente y cualquier evidencia adjunta.
- Propósito: Verificar e investigar la mala conducta denunciada, protegiendo al mismo tiempo la derechos de todos los involucrados.

Almacenamiento y cifrado de datos

- Almacenamiento: Todos los datos se almacenan en servidores seguros y encriptados.
- Cifrado: Los datos se cifran en reposo y en tránsito utilizando el estándar de la industria. protocolos.

Control de acceso

- Acceso restringido: Solo el personal autorizado con necesidad de saber puede acceder a los datos.
- Registros de auditoría: todos los accesos a los datos se registran y se revisan periódicamente.

Retención y eliminación de datos

- Periodo de conservación: Los datos se conservan solo el tiempo necesario para completar investigaciones y cumplir con los requisitos legales.
- Eliminación segura: una vez que los datos ya no son necesarios, se eliminan de forma segura mediante protocolos de eliminación certificados.

Cumplimiento y auditorías

- Auditorías periódicas: Realizadas internamente y por terceros para garantizar el cumplimiento. con las leyes de protección de datos.
- Revisiones de incidentes: Los procesos de manejo de datos se revisan periódicamente para mejorar Nuestra postura de seguridad.

---

4. Directrices de respuesta a incidentes

Descripción general

Sector-7 mantiene protocolos sólidos para abordar incidentes de seguridad. Ya sea que el incidente sea interno (que afecte a nuestros sistemas) o externo (relacionado con la denuncia de un denunciante), se implementan medidas rápidas y eficaces.

Identificación de incidentes

- Herramientas de detección: Los sistemas de monitoreo automatizados alertan a nuestro equipo de seguridad sobre cualquier actividades anómalas
- Canales de denuncia: Se anima a los usuarios a denunciar incidentes sospechosos a través de los canales seguros proporcionados.

Procedimientos de respuesta

1. Evaluación inicial: El equipo de seguridad verifica el incidente y evalúa su gravedad.
2. Contención: Se toman acciones inmediatas para aislar los sistemas afectados y evitar una mayor pérdida de datos.
3. Investigación: Se lleva a cabo una investigación exhaustiva para determinar la causa raíz y el alcance de la infracción.
4. Remediación: Se implementan medidas para mitigar los daños y restablecer la normalidad. operaciones.
5. Documentación: Cada paso se registra en un informe de respuesta a incidentes para rendición de cuentas y referencia futura.

Incidentes internos vs. externos

- Incidentes internos: Manejado por nuestros equipos dedicados de TI y ciberseguridad con controles internos estrictos.
- Incidentes externos: Se coordina con las autoridades policiales y los organismos reguladores según sea necesario, con protocolos de comunicación claros para las partes interesadas.

Plan de comunicación

- Notificaciones internas: Se envían alertas inmediatas al personal clave.
- Comunicación externa: Se emite un comunicado predefinido si es necesario, garantizar que los detalles sensibles permanezcan confidenciales.

Análisis posterior al incidente

- Lecciones aprendidas: Se lleva a cabo una reunión de revisión para analizar el incidente y Actualizar las políticas en consecuencia.
- Medidas preventivas: Se recomiendan prácticas de seguridad mejoradas. implementado para prevenir la recurrencia.

---

5. Cómo permanecer anónimo

Descripción general

Mantener el anonimato es fundamental para proteger la identidad de los denunciantes. Sector-7 emplea medidas de seguridad tecnológicas y procedimentales para garantizar que los usuarios puedan denunciar.
Sin miedo.

Herramientas y tecnologías

- VPN y Tor: se recomienda a los usuarios utilizar una VPN o acceder a la plataforma a través de la red Tor para obtener mayor anonimato.
- Comunicaciones cifradas: todos los intercambios de datos están protegidos de extremo a extremo. cifrado.
- Navegadores seguros: recomendamos utilizar navegadores centrados en la privacidad (por ejemplo, Firefox con complementos de privacidad).

Mejores prácticas para el anonimato

- Evite los identificadores personales: cuando sea posible, no incluya identificadores personales. Detalles en su informe.
- Use seudónimos: elija un alias al enviar informes si lo prefiere. conservar el anónimo.

- Proteja sus dispositivos: asegúrese de que su dispositivo esté actualizado con los últimos parches de seguridad y software antivirus.
- Cuentas separadas: utilice un correo electrónico o una cuenta separada y anónima únicamente para fines de denuncia de irregularidades.

Características de la plataforma

- Opción de envío anónimo: Nuestra plataforma le permite elegir opciones completas anonimato.
- Cifrado y enmascaramiento: todos los datos enviados están cifrados y los metadatos que Podría revelar que su identidad se elimina automáticamente.
- Guía del usuario: Se proporcionan instrucciones paso a paso sobre cómo maximizar el anonimato al utilizar la plataforma.

---

6. Aplicación de políticas y capacitación

Descripción general

Para garantizar el cumplimiento de estas directrices, el Sector-7 implementa estrictas medidas de cumplimiento y capacitación continua para todo el personal.

Roles y responsabilidades

- Responsable de Protección de Datos (OPD): supervisa todos los aspectos de la seguridad de los datos y privacidad.
- Equipo de respuesta a incidentes: responsable de gestionar y resolver problemas de seguridad. incidentes.
- Equipo de Cumplimiento: Garantiza que todos los procesos cumplan con los estándares regulatorios.

Programas de formación

- Capacitación periódica en seguridad: Todos los empleados reciben capacitación periódica sobre seguridad de datos. Seguridad y respuesta a incidentes.
- Talleres de denuncia de irregularidades: sesiones especializadas para educar a los usuarios sobre cómo Informar de forma segura y mantener el anonimato.
- Actualizaciones de políticas: Las actualizaciones se comunican rápidamente para garantizar que todos estén informados. consciente de nuevos protocolos o cambios.

Consecuencias por incumplimiento

- Medidas disciplinarias internas: Las violaciones de estas pautas pueden resultar en acción disciplinaria, que puede incluir hasta el despido.

- Repercusiones legales: Las infracciones también pueden dar lugar a consecuencias legales en virtud de leyes de protección de datos pertinentes.

---

7. Conclusión

Sector-7 mantiene su compromiso de fomentar un entorno seguro, transparente y ético. Al cumplir con estas directrices, garantizamos que todas las denuncias se gestionen con el máximo cuidado, protegiendo tanto a quienes denuncian conductas indebidas como la integridad de nuestra organización. Se proporcionarán actualizaciones según sea necesario, y nuestro equipo de soporte está siempre disponible para cualquier consulta o asistencia adicional.

---

8. Apéndices

Glosario de términos

- Denuncia de irregularidades: El acto de denunciar actividades poco éticas o ilegales dentro de una organización. organización.
- Cifrado: El proceso de codificar información para protegerla del acceso no autorizado. acceso.
- VPN: Red Privada Virtual, una herramienta utilizada para asegurar las conexiones a Internet.
- DPO: Responsable de Protección de Datos, responsable de supervisar la protección de datos. estrategias.

Referencias legales y regulatorias

- Reglamento General de Protección de Datos (RGPD)
- Norma de Seguridad de la Información ISO 27001
- Leyes de protección de datos nacionales y locales pertinentes

Hay recursos y plantillas adicionales disponibles en la página de Recursos.
