Ingeniería
en Desarrollo de Software

Actividad | 2 | Privacidad por Diseño

Ética y Sustentabilidad

Ingeniería en Desarrollo de Software

TUTOR: Francisco Ortega Rivera

ALUMNO: Carlos Fco Estrada Salazar

FECHA: 18/Jul/2025

ÍNDICE

GitHub Link:

INTRODUCCIÓN

En la actualidad, la privacidad de los datos personales se ha convertido en un aspecto fundamental en el diseño de cualquier sistema que maneje información sensible. Esta situación cobra especial relevancia en entornos organizacionales donde los colaboradores requieren canales seguros y confidenciales para reportar irregularidades, malas prácticas o situaciones contrarias a la ética y a la sustentabilidad. Por ello, en esta segunda etapa de la actividad, se abordará el concepto de "Privacidad por Diseño", un enfoque preventivo que busca integrar la protección de datos desde la fase inicial de construcción del sistema de denuncias.

Partiendo de los elementos definidos en la Actividad 1 *como los medios de comunicación, los protocolos de gestión y los reportes generados por el sistema*, se presentarán recomendaciones específicas orientadas a fortalecer la privacidad desde su concepción. Esto incluye asegurar que los datos personales estén protegidos por defecto, garantizar el anonimato cuando sea solicitado, y limitar el acceso solo a personal autorizado.

El objetivo es no solo mejorar la eficiencia y funcionalidad del sistema, sino también asegurar que su diseño cumpla con los principios éticos, legales y técnicos que rigen la protección de la información. De este modo, se promoverá una cultura organizacional basada en la confianza, el respeto y la responsabilidad hacia la privacidad de todos los miembros de la empresa.

DESCRIPCIÓN

La Actividad 2 se enfoca en reforzar la *protección de la privacidad* dentro del sistema de denuncias diseñado en la etapa anterior. En el contexto actual, donde los datos personales y confidenciales son vulnerables a múltiples riesgos, resulta fundamental que cualquier sistema que administre información delicada; *como denuncias anónimas o reportes internos*; sea concebido desde su diseño con mecanismos que aseguren su *privacidad y resguardo ético*.

La premisa de "Privacidad por Diseño" no implica únicamente implementar soluciones de seguridad técnica al final del desarrollo, sino integrar prácticas preventivas desde la planificación del sistema. Esto incluye el análisis de los posibles riesgos, la identificación de puntos críticos de exposición de datos y la creación de estructuras que eviten accesos indebidos, garantizando siempre el anonimato del denunciante, si así lo desea.

En este sentido, lo solicitado en la actividad busca que se revisen funciones clave del sistema, como los medios de comunicación, los protocolos de gestión y la generación de reportes, para proponer *tres recomendaciones concretas por función*. Estas recomendaciones deben garantizar que la privacidad sea una prioridad y que el sistema genere confianza en todos los niveles organizacionales. Esta actividad cobra aún más relevancia en una empresa con múltiples niveles jerárquicos y presencia nacional, ya que el adecuado manejo de información sensible es esencial para mantener una cultura organizacional ética, segura y respetuosa de los derechos de los colaboradores.

JUSTIFICACIÓN

El diseño de sistemas de denuncias debe incorporar desde su origen el principio de "Privacidad por Diseño" como una medida fundamental para proteger la integridad y confidencialidad de las personas involucradas. En la actualidad, donde la información es uno de los activos más valiosos y vulnerables, garantizar la privacidad de los datos no solo es una buena práctica, sino una *obligación ética y legal*. Esto es especialmente importante en sistemas que gestionan información sensible como denuncias sobre malas prácticas, conflictos éticos o problemas relacionados con la sustentabilidad.

La aplicación de este enfoque en la actividad resulta clave para fomentar la confianza entre los colaboradores de la organización. Cuando los empleados saben que su identidad será resguardada y que sus datos personales estarán protegidos desde el diseño del sistema, se sienten más seguros de reportar irregularidades sin temor a represalias. Esto promueve una cultura organizacional basada en la integridad, la justicia y la rendición de cuentas.

Al integrar la privacidad desde el diseño, se previenen filtraciones de información, se reduce el riesgo reputacional y se garantiza el cumplimiento de normativas de protección de datos. Por estas razones, implementar esta solución no solo es pertinente, sino esencial para fortalecer los procesos internos de ética y sustentabilidad dentro de la empresa.

DESARROLLO

MEDIOS DE COMUNICACIÓN PARA GESTIONAR LAS DENUNCIAS

1. **Implementar canales cifrados de extremo a extremo:**

Todo medio de comunicación digital, como plataformas web, aplicaciones móviles, correos electrónicos o líneas telefónicas virtuales, debe contar con protocolos de cifrado robustos (por ejemplo, HTTPS, TLS o cifrado de voz) que garanticen que la información transmitida no pueda ser interceptada ni modificada por terceros no autorizados. Esto protege tanto el contenido de la denuncia como la identidad del denunciante.

2. **Ofrecer opciones de anonimato sin recopilación de datos personales por defecto:**

Los medios de comunicación deben estar configurados por diseño para no exigir datos personales obligatorios al momento de realizar una denuncia. Se debe permitir al usuario mantener el anonimato completo, y cualquier campo opcional (como correo para seguimiento) debe aclarar su uso y requerir consentimiento explícito. Esto previene la reidentificación innecesaria del denunciante.

3. **Minimizar la exposición del canal físico o digital ante terceros:**

Los buzones físicos deben ubicarse en lugares seguros y privados, y las plataformas digitales no deben requerir credenciales vinculadas a la identidad del denunciante (como cuentas institucionales). Además, los accesos a las denuncias deben ser limitados por rol y registrados para auditoría, asegurando que solo personal autorizado pueda acceder a la información.

PROTOCOLOS DE COMUNICACIÓN PARA GESTIONAR LAS DENUNCIAS

1. **Establecer un flujo de gestión con roles limitados y claramente definidos:**

Los protocolos deben contemplar niveles de acceso restringidos según la función del personal involucrado en la atención de denuncias. Solo el personal estrictamente necesario (por ejemplo, del comité de ética o del área de cumplimiento) debe tener acceso a la información, evitando la circulación innecesaria de datos sensibles. Este principio de mínimo privilegio reduce el riesgo de exposición.

2. **Incorporar trazabilidad y registro de acceso a la información:**

Todos los protocolos deben incluir mecanismos de auditoría interna, es decir, mantener un registro seguro (logs) de quién accede a las denuncias, cuándo y con qué propósito. Esta medida no solo refuerza la responsabilidad de los gestores, sino que también permite detectar cualquier intento de mal uso o vulneración de la privacidad.

3. **Incluir procedimientos para preservar el anonimato durante todo el proceso:**

Desde la recepción hasta la resolución del caso, los protocolos deben estar diseñados para evitar la revelación de identidad, incluso en etapas de análisis, entrevistas o comunicación con otros involucrados. Si el denunciante decide mantenerse en el anonimato, el sistema debe garantizar que ningún paso del protocolo lo exponga directa o indirectamente.

GESTIÓN DE REPORTES

1. **Generar reportes anonimizados por defecto:**

Los reportes generados por el sistema deben excluir cualquier dato personal o identificador directo del denunciante o denunciado, a menos que sea estrictamente necesario. La información debe presentarse de forma estadística, agregada o codificada, permitiendo análisis y toma de decisiones sin comprometer la privacidad de los involucrados.

2. **Restringir la distribución de los reportes a perfiles autorizados:**

El sistema debe incluir controles que permitan definir quiénes pueden acceder, visualizar o exportar los reportes. Solo personal con funciones estratégicas (por ejemplo, alta dirección, comité de ética o auditores internos) debe recibir reportes sensibles. Además, debe configurarse la opción de autodestrucción o expiración de acceso a ciertos documentos según su nivel de sensibilidad.

3. **Proteger los reportes mediante cifrado y autenticación robusta:**

Todos los documentos generados deben estar protegidos con contraseñas seguras o claves de acceso únicas, y almacenarse en entornos cifrados (por ejemplo, almacenamiento seguro en la nube con autenticación multifactor). De esta forma, se reduce el riesgo de filtraciones accidentales o accesos no autorizados a la información contenida en los reportes.

CONCLUSIÓN

La implementación del enfoque de Privacidad por Diseño dentro de un sistema de denuncias representa una medida crucial tanto en el ámbito laboral como en la vida cotidiana, especialmente en una era donde la protección de los datos personales es una prioridad ética y legal. Esta actividad permite reconocer que no basta con identificar malas prácticas o disponer de canales de comunicación; es necesario rediseñar procesos y herramientas con una visión proactiva hacia la privacidad desde el inicio.

En el campo laboral, este tipo de soluciones favorece la confianza organizacional y el cumplimiento de normativas como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México o el RGPD en Europa. Un sistema que garantiza confidencialidad, anonimato y seguridad en la gestión de denuncias promueve una cultura ética, reduce la corrupción interna y protege tanto al denunciante como a la reputación institucional.

En la vida cotidiana, esta perspectiva ayuda a generar una mayor conciencia sobre el uso responsable de la información personal. Como ciudadanos y profesionales, comprender y aplicar estos principios nos permite prevenir vulneraciones, exigir transparencia en el manejo de nuestros datos y actuar con responsabilidad cuando trabajamos con la información de otros.

Adoptar el enfoque de privacidad desde el diseño no solo mejora sistemas, sino también transforma culturas organizacionales hacia entornos más seguros, éticos y sostenibles.

REFERENCIAS

- Martínez, V. (2024, 29 abril). *Cómo diseñar e implementar un canal de denuncias efectivo*. https://www.auditool.org/blog/fraude/como-disenar-e-implementar-un-canal-de-denuncias-efectivo

- Valentina. (2023, 8 febrero). *13 MEJORES PRÁCTICAS PARA IMPLEMENTAR UN CANAL DE DENUNCIAS SÓLIDO – BH Compliance*. BH Compliance. https://bh-compliance.com/es/blog/mejores-practicas-canal-de-denuncias/

- Ático34 Protección de datos para empresas y autónomos. (2024, 18 diciembre). *Protocolo canal de denuncias 2025 | Grupo Atico34*. Grupo Atico34. https://protecciondatos-lopd.com/empresas/compliance/canal-denuncias/protocolo/

- Martínez, V. (2024b, abril 29). *Cómo diseñar e implementar un canal de denuncias efectivo*. https://www.auditool.org/blog/fraude/como-disenar-e-implementar-un-canal-de-denuncias-efectivo

- Romero, V. M. (2025, 3 abril). *Ejemplos de canales de denuncias efectivos en empresas*. Factorial. https://factorial.es/blog/ejemplos-canales-denuncia/

- MyWeb TNUniversity. (s. f.). *ISO 37301: Estándares globales para el Compliance Empresarial*. TN University. https://www.tnuniversity.edu.mx/editorial/articulo/iso-37301-estandares-globales-para-el-compliance-empresarial/

- *Reportes de gestión de cumplimiento*. (s. f.). Blog | Central CRM Panamá. https://blog.central-crm.com/2019/08/reportes-de-gestion-de-cumplimiento.html