Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |2| Privacidad por Diseño.

Ética y Sustentabilidad.

Ingeniería en Desarrollo de Software.

TUTOR: Urbano Francisco Ortega Rivera.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 11/11/2025.

Introducción.

En esta segunda actividad de la materia Ética y sustentabilidad, nos enfocamos en la gestión de denuncias que exige ir más allá de la mera identificación de malas prácticas, medios de comunicación o protocolos deficientes. La seguridad, privacidad e integridad del proceso son fundamentales, especialmente en un entorno donde la filtración o mal uso de la información puede tener graves consecuencias legales y de confianza.

Este trabajo se centra en promover cambios de seguridad que garanticen el mejoramiento integral de estos aspectos. Tomando como base la Actividad 1, desarrollaremos tres recomendaciones clave para cada función esencial del sistema de denuncias: medios de comunicación, protocolos de gestión y manejo de reportes. El enfoque principal de estas propuestas será asegurar que el sistema promueva la privacidad de los datos desde su diseño, adoptando un enfoque de Privacy by Design. El objetivo es transformar el sistema en uno robusto, ético y plenamente conforme con las normativas de protección de datos.

Descripción.

En esta segunda actividad de la materia Ética y la Sustentabilidad, está enfocado en el análisis fundamental de la información obtenida en la Actividad 1, la cual reveló debilidades críticas en las malas prácticas, medios de comunicación y protocolos utilizados en el sistema de denuncias. El objetivo central de este documento es pasar de la simple identificación a la acción proactiva, proponiendo cambios de seguridad concretos que optimicen estos procesos.

El núcleo de la actividad consiste en formular tres recomendaciones específicas para cada una de las tres funciones esenciales de un sistema de denuncias: medios de comunicación, protocolos de comunicación para la gestión, y la gestión de reportes. Cada recomendación está diseñada bajo la filosofía de Privacidad desde el Diseño (Privacy by Design). Esto asegura que la protección de los datos personales, la identidad de los denunciantes y denunciados se integren como un componente

fundamental del sistema, y no como un añadido posterior. Este enfoque garantizará un sistema más seguro, ético y legalmente robusto.

Justificación.

La justificación de este trabajo radica en que la mera identificación de fallas, como se hizo en la Actividad 1, no garantiza un sistema de denuncias funcional ni ético. Es imperativo pasar a la fase de promoción e implementación de cambios de seguridad que corrijan las malas prácticas y fortalezcan la confianza en el proceso.

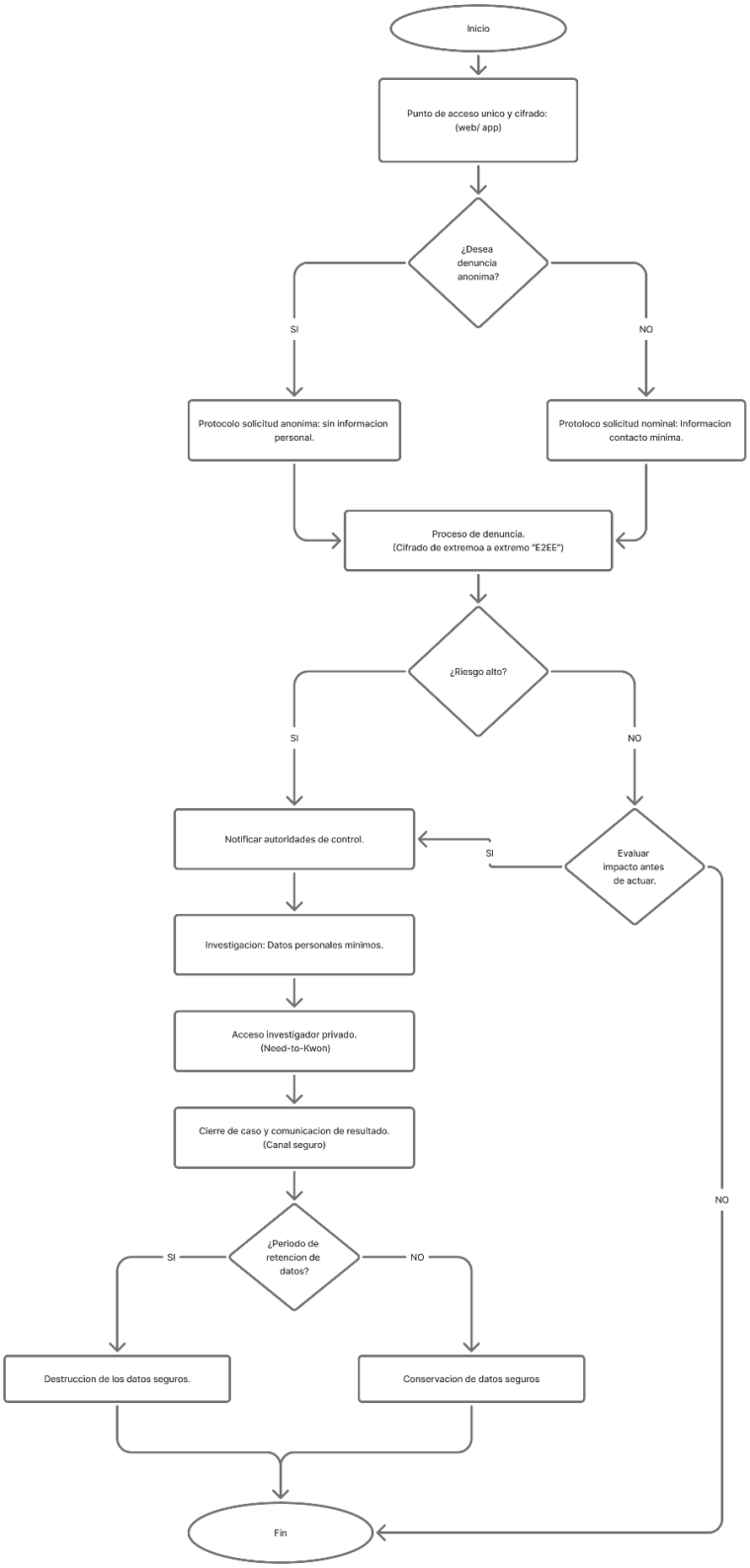
La justificación fundamental es que un sistema de denuncias sólo es efectivo si garantiza la seguridad y la privacidad de sus usuarios. Al enfocar las tres recomendaciones para cada función del sistema "medios, protocolos y gestión de reportes" en la Privacidad desde el Diseño (Privacy by Design), se garantiza que la protección de datos no sea una medida superficial, sino un componente intrínseco y prioritario. Esto no solo protege la identidad del denunciante y cumple con las normativas legales, sino que también fomenta la cultura de la denuncia, asegurando que los usuarios se sientan seguros al reportar irregularidades.

Desarrollo.

En esta parte de la actividad nos enfocaremos a realizar la documentación de la materia Ética y sustentabilidad donde dicha documentación nos indica la realización de un diagrama de un sistema de denuncias anónimas que cumpla con privacidad desde el diseño el cual se anexara como evidencia dando una breve explicación. Adicional dar 3 ejemplos de cada una de las funciones del sistema "medios, protocolos y gestión de reportes".

Link: GitHub.

Diagrama de sistema de denuncias anónimas.



Medios de comunicación para gestionar las denuncias.

Un sistema de denuncias para una empresa departamental con presencia nacional y una estructura compleja, los medios de comunicación deben garantizar el anonimato y la seguridad desde el primer contacto, cumpliendo rigurosamente con los principios de Privacidad por Diseño.

1. Medios Digitales (Online):

- Buzón de Correo Electrónico: Debe ser una cuenta dedicada con cifrado de extremo a extremo (E2EE) utilizando PGP y un servicio de correo que garantice la residencia de datos en jurisdicciones seguras.
- Chat/Mensajería Instantánea: Si se usa para la comunicación de seguimiento, debe ser una herramienta corporativa que permite el cifrado E2EE y tenga políticas estrictas de retención y borrado de historiales de chat.
- Formulario Web o Portal de Ética:Debe usar cifrado HTTPS/TLS estricto. La información enviada debe ser cifrada antes de ser almacenada en la base de datos (cifrado en reposo). Nunca almacenar datos sensibles en la URL.

2. Medios Telefónicos y de Voz:

- Línea Telefónica Directa (Línea Ética): Usar servicios que permitan la supresión automática de la identificación del número llamante (Caller ID/ANI) y que graben las llamadas solo si es legalmente necesario, con un aviso claro y cifrado de las grabaciones.
- Buzón de Voz Dedicado: El buzón debe estar configurado para ser accedido sólo por personal autorizado y las grabaciones deben ser transcritas y eliminadas de forma segura tras un periodo mínimo de retención.

3. Medios Físicos:

- Buzón de Sugerencias/Denuncias Físicas: Debe estar ubicado en un lugar seguro y controlado al que solo acceda el personal de gestión de denuncias. El protocolo debe estipular la apertura por dos personas para garantizar la integridad y la confidencialidad.

Protocolos de comunicación para gestionar las denuncias.

Los protocolos de comunicación rigen cómo el equipo gestor interactúa con la denuncia y, potencialmente, con el denunciante anónimo una vez que se ha recibido. Es fundamental que estos protocolos están diseñados para aislar y proteger la identidad durante todo el ciclo de vida de la investigación.

1. Minimización de Datos por Defecto:

- Recopilación Mínima: El formulario o sistema de denuncia debe solicitar sólo la información estrictamente necesaria para investigar el caso.
    - Si una denuncia anónima es viable, debe ser la opción predeterminada, y solo se debe pedir información de contacto si el denunciante opta por una comunicación de seguimiento.
- Anonimización/Seudonimización: El sistema debe incorporar mecanismos automáticos para seudonimizar o anonimizar los datos del denunciante y del denunciado tan pronto como sea posible, y antes de compartir la información con el equipo de investigación o asesores legales.

2. Confidencialidad y Seguridad:

- Cifrado de Extremo a Extremo: Los datos de la denuncia (texto, archivos adjuntos) deben estar cifrados desde el momento en que se envían hasta que se almacenan. Solo las personas autorizadas del equipo de gestión de denuncias deben tener las claves de descifrado.
- Control de Acceso Estricto (Need-to-Know): El sistema debe implementar un control de acceso basado en roles que restrinja quién puede ver qué partes de la denuncia.
    - El personal de Recursos Humanos puede ver la naturaleza de la queja, pero no necesariamente la identidad del denunciado hasta una etapa avanzada de la investigación.
- Canal de Comunicación Seguro: El protocolo debe especificar el uso de plataformas o correos electrónicos seguros con cifrado TLS/SSL y posiblemente PGP, para las comunicaciones de seguimiento con el denunciante o las partes. Nunca se debe usar un canal inseguro como SMS no cifrado o chat público para transmitir detalles sensibles de la denuncia.

3. Transparencia y Responsabilidad:

- Política de privacidad específica: Debe existir una política de privacidad clara y visible que detalle:
    - Qué datos se recogen.
    - Quién tendrá acceso a la denuncia.
    - Cuánto tiempo se conservarán los datos (plazo de retención).
    - Los derechos del denunciante y el denunciado (rectificación, acceso, supresión, etc.).
- Trazabilidad (Logging): El sistema debe registrar automáticamente quién, cuándo y por qué accedió a los datos de la denuncia mecanismo de logging. Este registro es crucial para la auditoría y la responsabilidad (Accountability).

Gestión de reportes.

La gestión de reportes se refiere a cómo la información de la denuncia es almacenada, procesada e nvestigada. En este punto, el enfoque de Privacidad por Diseño es vital para asegurar que los datos del denunciante sigan protegidos, minimizados durante la investigación y posterior archivado.

1. Evaluación de Impacto de la Protección de Datos:

- Este es el reporte central. Se realiza antes de iniciar un proyecto de tratamiento de datos que pueda entrañar un alto riesgo.
- Contenido: Describe el tratamiento de datos, evalúa su necesidad y proporcionalidad, analiza los riesgos para los derechos y libertades de los interesados, y especifica las medidas técnicas y organizativas (incluidas las de PbD) para mitigar dichos riesgos.

2. Inventario o Registro de Actividades de Tratamiento (RAT):

- Aunque no es un "reporte" como tal, es una documentación fundamental que detalla qué datos se tratan, para qué finalidad, quién tiene acceso, y cómo se implementan las medidas de seguridad y privacidad. Esto es la base para demostrar la transparencia y minimización de datos.

3. Reportes de Auditoría de Privacidad:

- Documentos generados periódicamente para verificar que los sistemas y procesos implementados sigan cumpliendo con los principios de PbD y las políticas internas.

Conclusion.

En conclusión: La Privacidad por Diseño (Privacy by Design) ha trascendido de ser un concepto legal a convertirse en una filosofía esencial tanto en el ámbito laboral como en la vida cotidiana. En el entorno corporativo, ejemplificado por el sistema de denuncias, su implementación garantiza que la ética y la transparencia no se vean comprometidas. Al asegurar la pseudoanonimización y la minimización de datos desde la concepción del sistema, se fomenta la confianza de los empleados para reportar irregularidades sin temor a represalias.

En la vida cotidiana, este principio es igualmente crucial. Cada vez que usamos una aplicación, un dispositivo IoT o una red social, debemos exigir que la privacidad sea la opción por defecto y que nuestros datos están protegidos por cifrado de extremo a extremo. Adoptar Privacy by Design significa construir un futuro donde la protección de la información personal sea proactiva y preventiva, permitiéndonos interactuar con la tecnología y los sistemas empresariales con mayor seguridad e integridad.

Referencias.

Google. (n.d.). Gemini. Retrieved November 12, 2025, from https://gemini.google.com/

Figma: The Collaborative Interface Design Tool. (n.d.). Figma. Retrieved November 15, 2025, from https://www.figma.com/