Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |2| Privacidad por diseño.

Ética y Sustentabilidad.

Ingeniería en Desarrollo de Sofwtare.

academia global

TUTOR: Urbano Francisco Ortega Rivera

ALUMNO: Carlos Ariel Nicolini

FECHA: 11/11/2025

Índice

Introducción

La privacidad por diseño es un enfoque que busca proteger la privacidad individual y la seguridad de los datos mediante decisiones de diseño intencionales. A diferencia de los métodos tradicionales que consideran la privacidad como una cuestión secundaria, la privacidad por diseño la convierte en un elemento central desde las primeras etapas del diseño.

Con el rápido crecimiento de la recopilación y el intercambio de datos en el panorama digital actual, la preocupación publica por la privacidad de los datos a aumentado considerablemente, las personas quieren tener la certeza de que su información personal se manejara de forma ética y segura. La privacidad desde el diseño se ha vuelto fundamental para que las organizaciones mantengan la confianza de los usuarios en los datos y cumplan con las normativas de protección de datos en constante evolución. Al priorizar la privacidad desde el principio, las organizaciones pueden integrarla en el núcleo de sus tecnologías, practicas comerciales y sistemas. Este enfoque proactivo representa un cambio crucial con respecto a la practica tradicional de reaccionar ante las preocupaciones sobre la privacidad solo después de que los sistemas ya están desarrollados. En el mundo actual, impulsado por los datos, la privacidad desde el diseño proporciona un marco esencial para una gestión de datos sostenible y ética que respeta los derechos y las decisiones personales.

Descripción

Contextualización:

Con base en la información de la actividad 1 se requiere no solo identificar malas prácticas, medios de comunicación o protocolos, sino promover los cambios de seguridad que precisen el mejoramiento de estos aspectos.

Actividad:

Con base en la actividad 1, determinar 3 recomendaciones por cada función del sistema de denuncias (por ejemplo: medios de comunicación, protocolos de comunicación para gestionar las denuncias, gestión de reportes), Estas recomendaciones deben enfocarse en que el sistema promueva la privacidad de los datos desde su diseño.

Al realizar este ejercicio note que el diseño realizado en el primer ejercicio tenia mejoras sustanciales en cuanto a manejo de información, resguardo, datos claves, clasificación que si bien fueron pensados no quedaron bien documentados cuales iban a ser su tratamiento y de que manera, lo cual podía generar situaciones de malas prácticas y demás casos. Fue muy bueno realizarlo para darme cuenta que se tiene que ser muy detallista en esos detalles ya que los datos son muy importantes y deben ser tratados así, desde el diseño de la aplicación o proceso y tener en cuenta cada detalle a documentar y evaluar.

Justificación

En esta actividad realizaremos al sistema de denuncias que realizamos en la actividad uno, unas recomendaciones y revisiones para evitar malas prácticas. Además, aprenderemos e intentaremos aplicar privacidad por diseño. Realizaremos algunas modificaciones en el proceso del sistema para prevenir malas prácticas y riesgos de seguridad que puedan alterar la unanimidad de la denuncia.

Aprender y realizar estas mejoras al sistema es una muy buena practica para asegurarnos que todo el proceso funcione de la mejor manera, que sea más seguro y que genere confianza en los usuarios que lo utilicen. Muchas veces los sistemas fallan por que no están pensandos en cuestiones de privacidad o seguridad lo que puede provocar filtraciones indebidas y que la gente no quiere realizar las denuncias con la consiguiente falta de confianza.

Con estas mejoras el flujo es claro desde el inicio hasta el cierre, con lo cual no pueden quedar casos perdidos y que no sean cerrados de manera correcta, las denuncias se procesan de manera más rápida, de manera más anónima, sin filtraciones, donde solo pueden ser revisadas por personal con autorización. Estas mejoras no solo mejoran el sistema, sino la confianza del usuario en el sistema y en la empresa, lo cual ayudara a mejorar el ambiente y corregir malas prácticas, lo cual beneficia a el personal y a la empresa.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/-tica-y-Sustentabilidad

Desarrollo

De acuerdo al diagrama y sistema definido en la primera actividad, determinaremos 3 recomendaciones para su mejora enfocados en que el sistema promueva la privacidad de los datos desde su diseño.

En este punto se realizan modificaciones al diagrama y proceso para prevenir malas prácticas, promover la seguridad y confianza del usuario en el sistema.

A continuación, pasaremos a explicar

1- Se ingresa a la app de la aplicación.
2- Se selecciona el tipo de denuncia, Mala práctica, Ética cuestionable o sustentabilidad (Categorías claras y ejemplos para evitar clasificaciones incorrectas por parte del usuario).
3- Se captura la denuncia anónima de manera segura (se realiza una descripción detallada, lugar y fecha y de manera opcional se adjuntan evidencias de forma segura). Campos opcionales, cifrado extremo a extremo,
4- El sistema genera un número de folio aleatorio y lo presenta en la app al usuario. (información guardada en base de datos auditada).
5- Se realiza una recepción automática, se filtra la renuncia por tipo y región, se verifica automáticamente cualquier que no haya conflicto de interés y se envía automáticamente al comité de ética y cumplimiento para su revisión.
6- Se revisa en un plazo de 24 a 48 horas si la denuncia procede y se realiza una evaluación preliminar. Si procede se continua con los siguientes casos sino se cierra el folio, se informa al denunciante que no procede y el motivo. Se retiene de forma limitada el registro, se genera el reporte estadístico mensual, sin información personal, solo con indicadores generales y se elimina de manera segura los datos al finalizar.

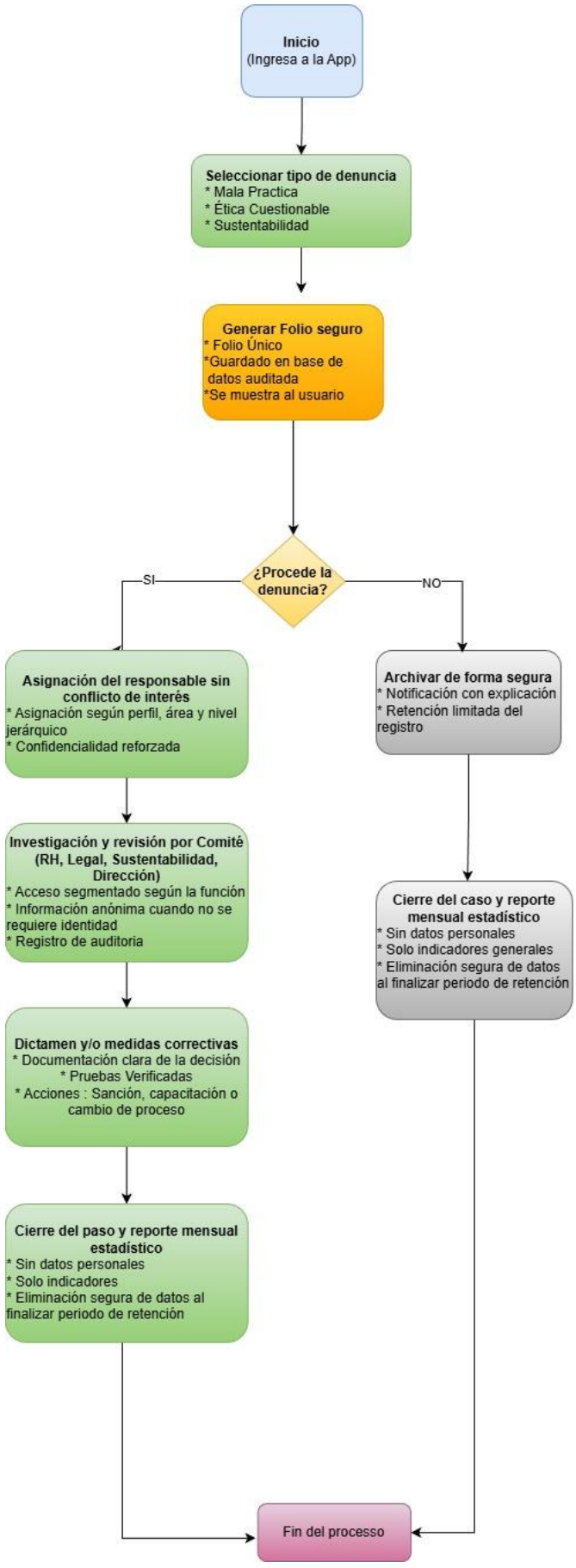
7- Se asigna a un responsable según el perfil, área y nivel jerárquico requerido para el caso. Se trata el tema con confidencialidad reforzada.

8- Se realiza una revisión por el comité de Recursos humanos, el área legal, sustentabilidad y dirección con tipo de acceso segmentado según la función, con información anónima y se realiza el registro de auditoría.

9- Con la documentación clara y con pruebas verificadas, se revisa si es merecedora de una sanción, capacitación o cambios en el proceso.

10- Se cierra el caso, se generan los indicadores generales con información sin datos personales y se elimina de forma segura los datos al finalizar el periodo de retención.

11- Fin del proceso


Inicio
(Ingresa a la App)
Seleccionar tipo de denuncia
* Mala Practica
* Ética Cuestionable
* Sustentabilidad
Generar Folio seguro
* Folio Único
*Guardado en base de datos auditada
*Se muestra al usuario
¿Procede la denuncia?
SI
NO
Asignación del responsable sin conflicto de interés
* Asignación según perfil, área y nivel jerárquico
* Confidencialidad reforzada
Archivar de forma segura
* Notificación con explicación
* Retención limitada del registro
Investigación y revisión por Comité (RH, Legal, Sustentabilidad, Dirección)
* Acceso segmentado según la función
* Información anónima cuando no se requiere identidad
* Registro de auditoria
Cierre del caso y reporte mensual estadístico
* Sin datos personales
* Solo indicadores generales
* Eliminación segura de datos al finalizar periodo de retención
Dictamen y/o medidas correctivas
* Documentación clara de la decisión
* Pruebas Verificadas
* Acciones : Sanción, capacitación o cambio de proceso
Cierre del paso y reporte mensual estadístico
* Sin datos personales
* Solo indicadores
* Eliminación segura de datos al finalizar periodo de retención
Fin del processo

Recomendaciones

Medios de comunicación para gestionar las denuncias

En este punto realizaremos 3 recomendaciones para diseñar los medios de comunicación de la app de denuncias que cumplan con los principios de privacidad por diseño.

- Minimizar la recolección de datos personales: La aplicación de denuncia, al ingresar o generar la denuncia solo debe pedir la información necesaria, ya que, al ser anónima, no debe solicitar nombre, correo, teléfono ni cualquier información que de manera indirecta pueda identificar al usuario demandante.
- Utilizar cifrado de extremo a extremo: Toda la información que es ingresada y enviada desde la aplicación de denuncia anónima (texto, capturas, fotos, archivos) debe ir cifrada, por si llegara a haber una filtración o intercepción, no se pueda interpretar lo que se reporta.
- Implementar almacenamiento seguro y de manera temporal: la información sensible debe guardarse en servidores con alta seguridad y con autenticación fuerte. Dichos datos deben eliminarse después de un periodo definido para su retención. Dicha información solo debe estar disponible para el comité encargado de la revisión y para nadie mas que no tenga esa jerarquía.

Protocolos de comunicación para gestionar las denuncias

En este punto realizaremos 3 recomendaciones para los protocolos de comunicación para gestionar las denuncias enfocados en un control interno y protección del denunciante.

A continuación, listaremos las recomendaciones.

- Implementar accesos basados en roles (RBAC): Cada área debe poder solo tener acceso y ver la información que le corresponde. Esto evita que información sensible sea vista por personal no autorizado.
- Registro de actividad fijos (logs): La interacción con los datos (Abrir, leer, modificar, cerrar un caso) debe quedar registrado en una bitácora donde no se pueda modificar ni borrar para tener una trazabilidad y proteger los datos contra usos indebidos o desautorizados.
- Automatizar anonimato de información sensible: A menos que el denunciante haya decidido identificarse (en este caso la información debe entregarse de forma separada y con las correspondientes advertencias de privacidad), el comité debe recibir la denuncia sin datos personales

Gestión de reportes

En este punto realizaremos 3 recomendaciones para la gestión de los reportes, los cuales deben ser extremadamente útiles, pero sin exponer información personal o sensible.

A continuación, listaremos las recomendaciones

- Generación de reportes estadísticos sin nombres: Los reportes solo deben mostrar los datos agrupados, como el numero de casos, tipo, región, tiempo de atención, etc. Nunca deben incluir los datos del denunciante ni detalles que puedan provocar la identificación de personas.
- Clasificación automática de la información sensible: Antes de que se genere el reporte, automáticamente el sistema debe filtrar nombres, documentos, ubicaciones u otros datos personales y no presentarlos en el reporte, con el fin de evitar realizar exposiciones accidentales que puedan terminar en la identificación de la persona denunciante.
- Control sobre quien tiene acceso para descargarlo y el tiempo de posesión: Dichos reportes solo deben estar accesibles para personal o áreas autorizadas y deben tener un periodo de caducidad, no deben ser guardados indefinidamente por seguridad para evitar riesgos de filtración de información sensible.

Conclusión

En este ejercicio aplicamos mejoras en el sistema de denuncias anónimas, lo cual no solamente nos generó un cambio en algunos puntos del proceso y el flujo, lo cual mejora notablemente la seguridad y confidencialidad del sistema, en el cual se pone principal atención a el manejo de los datos, controles de quienes deben tener acceso a que información y como debe ser tratada. Se corrigieron posibles malas prácticas que se había dejado posibilidad de que sucedan por un mal enfoque en su diseño.

Además nos enseña que un sistema de denuncias no es solo un buzón digital para dejar opiniones, sino es una herramienta muy útil que puede mejorar la transparencia, ética y el ambiente organizacional de una empresa, por tal motivo debe ser realizado en esos principios, donde la información debe ser tratada con todo el profesionalismo posible, que la información debe ser protegida a cada momento, todos sus participantes tienen sus responsabilidades y que el sistema debe ayudar a los involucrados a que dichos datos deben estar catalogados, seguros, cifrados, almacenados de manera correcta, solo deben tener acceso las personas o áreas responsables y que pasado el tiempo de gracia dicha información debe ser eliminada de manera segura y definitiva.

Un excelente trabajo sobre el uso debido de los datos y su manera de tratarlos, que me hiso realizar cambios en mi primer diseño por que no estaba bien diseñado.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/-tica-y-Sustentabilidad

Referencias

Claves para implementar un canal de denuncias para empresas. (2024, March 1). Personio. https://www.personio.es/glosario/canal-denuncias-empresas/

Flowchart maker & online diagram software. (n.d.). Diagrams.net. Retrieved November 16, 2025, from https://app.diagrams.net/

La implementación de un canal de denuncias: nuestros 6 consejos. (2022, May 5). Whistlelink. https://www.whistlelink.com/es/blog/la-implementacion-de-un-canal-de-denuncias-nuestros-6-consejos/

Mejores prácticas para canales de denuncia o línea ética. Blog#2. (2024, September 23). B-GRC. https://www.b-grc.com/index.php/mejores-practicas-para-canales-de-denuncia-o-linea-etica-blog2/

Privacy by Design - general data protection regulation (GDPR). (n.d.). General Data Protection Regulation (GDPR). Retrieved November 16, 2025, from https://gdpr-info.eu/issues/privacy-by-design/

Rufino, G. (2024, July 18). Mejores prácticas para un canal de denuncias anónimo y seguro. Edorteam; Edorteam | Consultoría Compliance & Protección de datos. https://edorteam.com/practicas-para-un-canal-de-denuncias-anonimo-y-seguro/

(N.d.). Ieee.org. Retrieved November 16, 2025, from https://digitalprivacy.ieee.org/publications/topics/what-is-privacy-by-design-and-why-it-s-important/