



Actividad | 2 |

Privacidad por Diseño

Ética y Sustentabilidad

Ingeniería en Desarrollo de Software



academi**ag**lobal

TUTOR: Jessica Hernández Romero

ALUMNO: Yanira Lizbeth Lopez Navarro

FECHA: 13/07/2024

Índice

Introducción	3
Descripción	4
Justificación	5
Desarrollo:	6
Conclusión	11
Referencias	12

Introducción

La privacidad se ha convertido en una preocupación primordial en la era digital, donde la recopilación y el procesamiento de datos personales están en constante aumento. En respuesta a esta creciente preocupación, el concepto de "Privacidad por Diseño" (Privacy by Design) ha emergido como un enfoque integral y proactivo para proteger la información personal desde el inicio de cualquier proceso o sistema. Esta metodología no se limita a la mera implementación de medidas de seguridad, sino que integra principios de privacidad en todas las etapas del diseño y desarrollo de productos, servicios y operaciones organizacionales.

En esta actividad, exploraremos los fundamentos y la importancia de la Privacidad por Diseño, destacando cómo este enfoque puede garantizar que los datos personales se manejen de manera segura y ética desde el principio. Analizaremos los siete principios fundamentales que guían esta metodología, los cuales incluyen la proactividad, la prevención, la integración de medidas de privacidad como estándar predeterminado, y la transparencia, entre otros. Además, discutiremos ejemplos prácticos y casos de estudio que ilustran cómo las organizaciones pueden implementar estos principios para cumplir con las regulaciones de privacidad y proteger los derechos de los individuos.

Este conocimiento es esencial para desarrollar sistemas y procesos que respeten la privacidad de los usuarios, fomenten la confianza y cumplan con las normativas legales vigentes. La adopción de la Privacidad por Diseño no solo protege a los individuos, sino que también fortalece la reputación y la competitividad de las organizaciones en un mundo cada vez más consciente de la privacidad y la seguridad de los datos.

Descripción

La contextualización y el propósito de esta actividad radican en la identificación y el mejoramiento de las prácticas de seguridad y privacidad dentro de un sistema de denuncias en una organización. Partiendo de la base de la Actividad 1, donde se destacó la importancia de contar con un sistema robusto para reportar conductas inapropiadas de manera confidencial y segura, ahora se requiere avanzar un paso más allá. No solo es crucial establecer los medios de comunicación y los protocolos para gestionar las denuncias, sino también implementar cambios que fortalezcan la seguridad y privacidad de los datos desde el diseño del sistema.

La actividad solicitada consiste en formular tres recomendaciones específicas para cada función del sistema de denuncias: medios de comunicación, protocolos de comunicación y gestión de reportes. Estas recomendaciones deben garantizar que la privacidad de los datos se incorpore desde la concepción del sistema, siguiendo los principios de la Privacidad por Diseño. Es decir, la protección de la información personal no debe ser una medida añadida posteriormente, sino un componente esencial integrado desde el inicio.

Estas recomendaciones están diseñadas para asegurar que el sistema de denuncias no solo sea efectivo en la recepción y gestión de informes, sino que también priorice la protección de la privacidad de todos los involucrados desde su concepción. Implementar estos principios no solo cumplirá con las normativas legales, sino que también fortalecerá la confianza de los empleados y otras partes interesadas en la integridad del proceso de denuncia.

Justificación

Implementar un sistema de denuncias que integre la privacidad por diseño es esencial para cualquier organización moderna, especialmente en un entorno empresarial complejo y diverso como el descrito en la actividad. Este enfoque no solo protege la confidencialidad de los denunciantes, sino que también fortalece la confianza en la integridad del proceso de denuncia.

Lo principal para adoptar esta solución radica en la necesidad de fomentar un ambiente de trabajo seguro y ético. Cuando los empleados y otras partes interesadas saben que pueden reportar irregularidades sin temor a represalias y con la garantía de que su privacidad será protegida, están más dispuestos a levantar la voz contra las malas prácticas. Esto permite a la organización detectar y abordar problemas internos de manera oportuna, evitando daños mayores a la reputación y operaciones de la empresa.

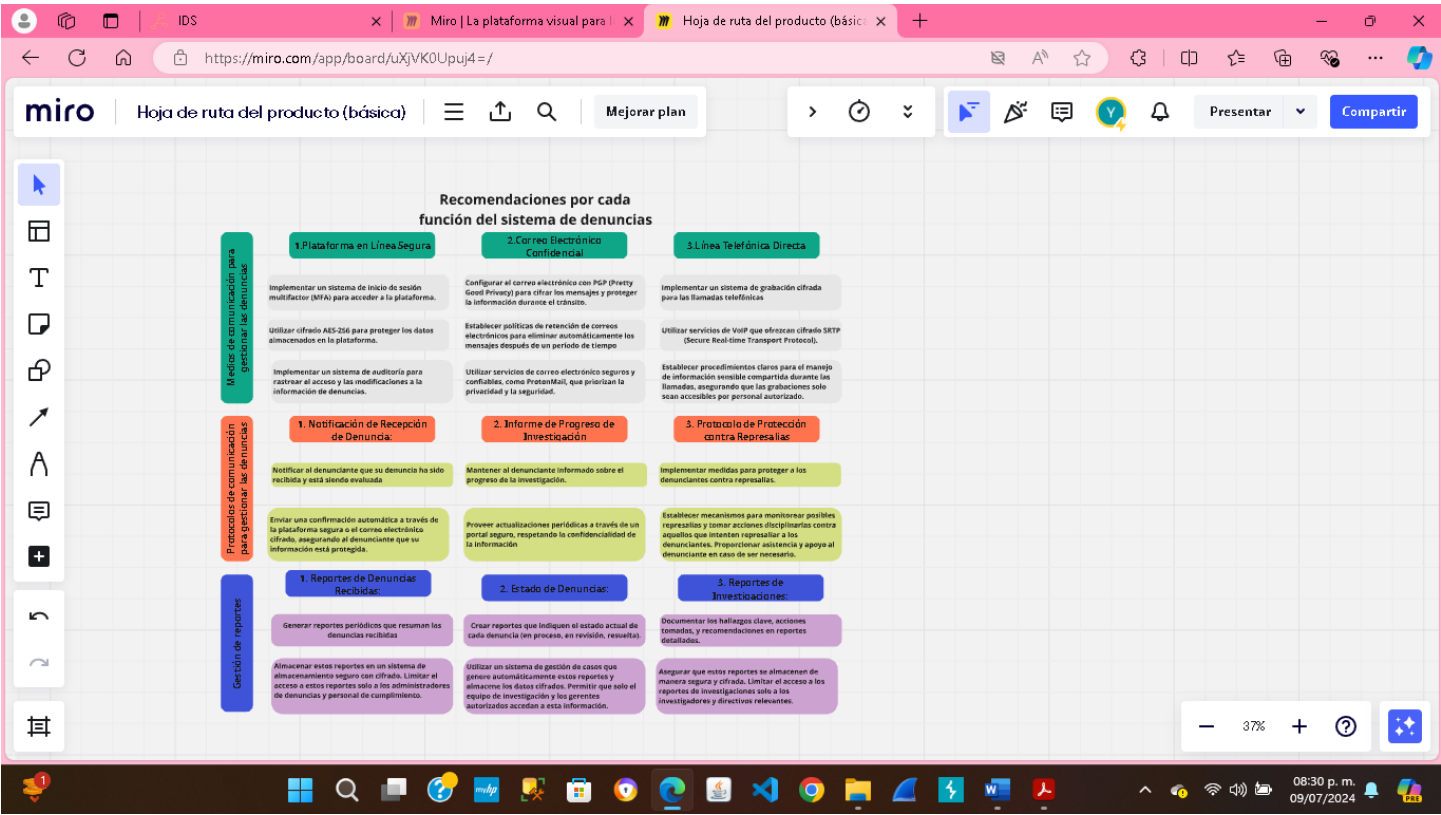
Además, la privacidad por diseño ayuda a cumplir con las regulaciones legales y normativas vigentes, como el Reglamento General de Protección de Datos (GDPR) en Europa y otras leyes de privacidad a nivel mundial. Cumplir con estas normativas no solo evita sanciones legales, sino que también demuestra el compromiso de la organización con la protección de los datos personales, lo cual es un valor añadido en términos de responsabilidad corporativa.

Otro aspecto crucial es la mejora de la moral y el compromiso de los empleados. Un sistema de denuncias bien diseñado y seguro puede reducir el miedo a las represalias y aumentar la percepción de justicia y transparencia dentro de la organización. Esto, a su vez, mejora la satisfacción y la retención de los empleados, creando un ambiente laboral más positivo y productivo.

Emplear una solución de denuncias que priorice la privacidad por diseño es fundamental para proteger la confidencialidad de los denunciantes, cumplir con las normativas legales, mejorar la confianza y el compromiso de los empleados y asegurar la detección temprana de problemas internos. Esta estrategia no solo beneficia a la organización al mantener su integridad y reputación, sino que también contribuye al bienestar y la seguridad de todos los involucrados.

Desarrollo:

En la siguiente imagen podemos observar la lluvia de ideas que me permitió desarrollar la actividad.



Recomendaciones por cada función del sistema de denuncias			
Medios de comunicación para gestionar las denuncias	1.Plataforma en Línea Segura	2.Correo Electrónico Confidencial	3.Línea Telefónica Directa
	Implementar un sistema de inicio de sesión multifactor (MFA) para acceder a la plataforma.	Configurar el correo electrónico con PGP (Pretty Good Privacy) para cifrar los mensajes y proteger la información durante el tránsito.	Implementar un sistema de grabación cifrada para las llamadas telefónicas
	Utilizar cifrado AES-256 para proteger los datos almacenados en la plataforma.	Establecer políticas de retención de correos electrónicos para eliminar automáticamente los mensajes después de un período de tiempo	Utilizar servicios de VoIP que ofrezcan cifrado SRTP (Secure Real-time Transport Protocol).
	Implementar un sistema de auditoría para rastrear el acceso y las modificaciones a la información de denuncias.	Utilizar servicios de correo electrónico seguros y confiables, como ProtonMail, que priorizan la privacidad y la seguridad.	Establecer procedimientos claros para el manejo de información sensible compartida durante las llamadas, asegurando que las grabaciones solo sean accesibles por personal autorizado.
Protocolos de comunicación para gestionar las denuncias	1. Notificación de Recepción de Denuncia:	2. Informe de Progreso de Investigación	3. Protocolo de Protección contra Represalias
	Notificar al denunciante que su denuncia ha sido recibida y está siendo evaluada	Mantener al denunciante informado sobre el progreso de la investigación.	Implementar medidas para proteger a los denunciantes contra represalias.
	Enviar una confirmación automática a través de la plataforma segura o el correo electrónico cifrado, asegurando al denunciante que su información está protegida.	Proveer actualizaciones periódicas a través de un portal seguro, respetando la confidencialidad de la información	Establecer mecanismos para monitorear posibles represalias y tomar acciones disciplinarias contra aquellos que intenten represaliar a los denunciantes. Proporcionar asistencia y apoyo al denunciante en caso de ser necesario.
Gestión de reportes	1. Reportes de Denuncias Recibidas:	2. Estado de Denuncias:	3. Reportes de Investigaciones:
	Generar reportes periódicos que resuman las denuncias recibidas	Crear reportes que indiquen el estado actual de cada denuncia (en proceso, en revisión, resuelta).	Documentar los hallazgos clave, acciones tomadas, y recomendaciones en reportes detallados.
	Almacenar estos reportes en un sistema de almacenamiento seguro con cifrado. Limitar el acceso a estos reportes solo a los administradores de denuncias y personal de cumplimiento.	Utilizar un sistema de gestión de casos que genere automáticamente estos reportes y almacene los datos cifrados. Permitir que solo el equipo de investigación y los gerentes autorizados accedan a esta información.	Asegurar que estos reportes se almacenen de manera segura y cifrada. Limitar el acceso a los reportes de investigaciones solo a los investigadores y directivos relevantes.

Medios de comunicación para gestionar las denuncias

1. **Plataforma en Línea Segura:**

- Implementar un sistema de inicio de sesión multifactor (MFA) para acceder a la plataforma.
- Utilizar cifrado AES-256 para proteger los datos almacenados en la plataforma.
- Implementar un sistema de auditoría para rastrear el acceso y las modificaciones a la información de denuncias.

2. **Correo Electrónico Confidencial:**

- Configurar el correo electrónico con PGP (Pretty Good Privacy) para cifrar los mensajes y proteger la información durante el tránsito.
- Establecer políticas de retención de correos electrónicos para eliminar automáticamente los mensajes después de un periodo de tiempo definido.
- Utilizar servicios de correo electrónico seguros y confiables, como ProtonMail, que priorizan la privacidad y la seguridad.

3. **Línea Telefónica Directa:**

- Implementar un sistema de grabación cifrada para las llamadas telefónicas.
- Utilizar servicios de VoIP que ofrezcan cifrado SRTP (Secure Real-time Transport Protocol).
- Establecer procedimientos claros para el manejo de información sensible compartida durante las llamadas, asegurando que las grabaciones solo sean accesibles por personal autorizado.

Protocolos de comunicación para gestionar las denuncias

1. Notificación de Recepción de Denuncia:

- **Descripción:** Notificar al denunciante que su denuncia ha sido recibida y está siendo evaluada.
- **Implementación:** Enviar una confirmación automática a través de la plataforma segura o el correo electrónico cifrado, asegurando al denunciante que su información está protegida.

2. Informe de Progreso de Investigación:

- **Descripción:** Mantener al denunciante informado sobre el progreso de la investigación.
- **Implementación:** Proveer actualizaciones periódicas a través de un portal seguro, respetando la confidencialidad de la información.

3. Protocolo de Protección contra Represalias:

- **Descripción:** Implementar medidas para proteger a los denunciantes contra represalias.
- **Implementación:** Establecer mecanismos para monitorear posibles represalias y tomar acciones disciplinarias contra aquellos que intenten represaliar a los denunciantes. Proporcionar asistencia y apoyo al denunciante en caso de ser necesario.

Gestión de reportes

1. Reportes de Denuncias Recibidas:

- **Descripción:** Generar reportes periódicos que resuman las denuncias recibidas.
- **Implementación:** Almacenar estos reportes en un sistema de almacenamiento seguro con cifrado. Limitar el acceso a estos reportes solo a los administradores de denuncias y personal de cumplimiento.

2. Estado de Denuncias:

- **Descripción:** Crear reportes que indiquen el estado actual de cada denuncia (en proceso, en revisión, resuelta).
- **Implementación:** Utilizar un sistema de gestión de casos que genere automáticamente estos reportes y almacene los datos cifrados. Permitir que solo el equipo de investigación y los gerentes autorizados accedan a esta información.

3. Reportes de Investigaciones:

- **Descripción:** Documentar los hallazgos clave, acciones tomadas, y recomendaciones en reportes detallados.
- **Implementación:** Asegurar que estos reportes se almacenen de manera segura y cifrada. Limitar el acceso a los reportes de investigaciones solo a los investigadores y directivos relevantes.

Conclusión

La implementación de un sistema de denuncias con un enfoque en la privacidad por diseño es una práctica esencial en el campo laboral y tiene implicaciones significativas en la vida cotidiana. Este tipo de sistema no solo fortalece la cultura organizacional al promover la ética y la transparencia, sino que también protege los derechos individuales de los empleados y otras partes interesadas, garantizando que puedan reportar irregularidades sin temor a represalias.

En el ámbito laboral, la actividad de diseñar e implementar un sistema de denuncias robusto y seguro demuestra el compromiso de la organización con la integridad y la responsabilidad social. Al integrar principios de privacidad desde el inicio, se asegura que la protección de los datos personales sea una prioridad constante, lo que es fundamental en un entorno donde las amenazas a la seguridad de la información son cada vez más frecuentes y sofisticadas.

Esta práctica también tiene un impacto positivo en la vida cotidiana al promover una mayor conciencia sobre la importancia de la privacidad y la seguridad de los datos. Las personas se vuelven más conscientes de sus derechos y de las medidas que pueden tomar para proteger su información personal, tanto en el trabajo como en otros aspectos de su vida.

La implementación de un sistema de denuncias que prioriza la privacidad por diseño es una inversión en la integridad, la seguridad y la sostenibilidad, beneficiando tanto a la organización como a la sociedad en su conjunto.

Referencias

Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 30 de junio de 2024, umi.edu.mx/coppel/IDS/mod/scorm/player.php

Video conferencing, web conferencing, webinars, screen sharing. (s. f.-h). Zoom. https://academiaglobal-mx.zoom.us/rec/play/bnLljXcoC2wmIoIx88VX_SKGZzrHHaRS6qhtE1poCrMDUKxi5n9cycw2hXEeQH9UoiKN1qv3x5j6q-8.jNk666R6dELfn64X?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FMkBMn8oUFRodHzcBoaEHDeg25mWs6oQfr54YLy17I68xjLkyAz1Sf4k6Yg0NVWcD.WVctScVYu-FqSbv0

Video conferencing, web conferencing, webinars, screen sharing. (s. f.-i). Zoom. https://academiaglobal-mx.zoom.us/rec/play/1Jkrb9cmkJI1KrNiGVsuMgGju1kI3_CpGEczAZ-IXCGmCyC0wTA9OLlin8fx1fewZimzSSCQxMGIBeIx.rgE5OH0i0rVb-j3a?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2Fo7P-UW33FCpFHfbRSOfriqsjZptzy1plfMz20XrUa8M8rc5bHsnnEThcKSjPR_MX.mRGrb-xGFtwZaDlCf