

## **Ingeniería en Desarrollo de Software**

**Actividad:** Número 2.

**Nombre de la Actividad:** Privacidad por diseño.

**Nombre del Curso:** Ética y sustentabilidad.

**Tutor:** Jessica Hernández Romero.

**Alumno:** Omar Juárez Carmona.

**Fecha:** 23 - Octubre – 2023.

## INDICE

Contextualización y actividad.....	3
Introducción.....	4
Descripción.....	6
Justificación.....	8
Desarrollo (Recomendaciones).....	10
- Medios de comunicación para gestionar las denuncias.....	10
- Protocolos de comunicación para gestionar las denuncias.....	12
- Gestión de reportes.....	15
Conclusión.....	17
Referencias y link.....	18

## **CONTEXTUALIZACION Y ACTIVIDAD**

### **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.

## INTRODUCCION

La ética y la sustentabilidad en entornos digitales son dos conceptos que están ganando cada vez más atención en la sociedad actual.

La ética digital se refiere a la responsabilidad de las empresas y los individuos en el uso de la tecnología y los datos, y cómo estos pueden afectar a la privacidad, la seguridad y los derechos humanos.

La sustentabilidad digital se refiere a la necesidad de reducir el impacto ambiental de la tecnología y garantizar que se utilice de manera responsable y sostenible. Ambos conceptos son importantes para garantizar un futuro digital justo, seguro y sostenible.

La privacidad por diseño (PbD) es un enfoque preventivo para la protección de la privacidad de los datos desarrollado en la década de 1990. Su propósito inicial era desarrollar un modelo robusto y escalable para la privacidad de los datos que superaría las “tecnologías de mejora de la privacidad” y los requisitos de cumplimiento normativo más débiles en ese momento para garantizar la privacidad total de los datos.

Los principios fundamentales de PbD son los siguientes:

- Proactivo no reactivo; preventivo, no reparador.
- Privacidad por defecto.
- Privacidad integrada en el diseño.
- Funcionalidad completa: suma positiva, no suma cero.
- Seguridad de un extremo a otro: protección del ciclo de vida completo.
- Visibilidad y transparencia.
- Respeto por la privacidad del usuario.

En el contexto de un sistema de denuncias, se puede implementar PbD mediante la incorporación de medidas técnicas y organizativas adecuadas para aplicar los principios de protección de datos y salvaguardar su tratamiento para cumplir con los requisitos del RGPD y proteger los derechos individuales.

Es importante que el canal de denuncias interno o canal ético tenga mecanismos fáciles y rápidos de usar, para que los empleados no tengan problemas a la hora de realizar sus denuncias. Además, se debe preservar el anonimato y mantener la confidencialidad de los datos.

## DESCRIPCION

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.

En esta actividad número 2 nuestro principal objetivo es identificar los riesgos que afectan a los usuarios en los sistemas de información, y de igual manera identificar las prácticas no éticas en los sistemas de información de las empresas. Debemos saber que los sistemas de información pueden estar expuestos a una variedad de riesgos que pueden afectar a los usuarios. Algunos de los riesgos comunes son:

- Amenazas:

Las amenazas son posibles ataques que pueden ser internos o externos. Los ataques internos pueden ser realizados por empleados descontentos o ex empleados, mientras que los ataques externos pueden ser realizados por hackers o crackers. Los ataques pueden incluir virus, gusanos, troyanos y otros tipos de malware.

- Vulnerabilidades:

Las vulnerabilidades son debilidades en la tecnología o en los procesos asociados con la información. Estas debilidades pueden ser explotadas por personas malintencionadas para poner en riesgo la seguridad de la información.

- Fugas de información:

Las fugas de información pueden ocurrir deliberadamente como resultado de una acción intencional de algún empleado descontento, como consecuencia de un ciberataque, o inadvertidamente, por un colaborador desprevenido víctima de un software malicioso.

Es importante que las organizaciones y los usuarios tomen medidas para protegerse contra estos riesgos. Algunas medidas que se pueden tomar incluyen el uso de software antivirus, la implementación de políticas de seguridad sólidas y la educación de los usuarios

sobre las mejores prácticas de seguridad.

La ética en los sistemas de información es un tema importante en la gestión empresarial. Las empresas deben asegurarse de que sus sistemas de información sean utilizados de manera ética y responsable. Las prácticas no éticas pueden incluir el uso indebido de información confidencial, la manipulación de datos, el robo de propiedad intelectual y la violación de la privacidad del usuario.

Según un artículo, la ética tecnológica permite orientar la conducta humana en la tecnología, orienta y guía las acciones del ser humano. La ética tecnológica involucra muchas decisiones estratégicas, como inversión en recursos humanos, modernización, desarrollo y servicios de productos. Las amenazas y oportunidades, pueden afectar de manera significativa el desempeño, caracterizándose por su singularidad, complejidad y velocidad. La revolución de la información ha magnificado la capacidad para adquirir, manipular, almacenar y comunicar información. La ética tecnológica juega un papel fundamental en este proceso.

En otro artículo, se menciona que el código de ética es una medida importante para prevenir las conductas no éticas en las empresas. Su creación, actualización y correcta transmisión a través de todos los niveles de la organización es una de las mejores medidas de prevención contra las conductas no éticas y repercute positivamente mejorando la relación entre empleados, proveedores y clientes, además de que fortalece la imagen y reputación de la empresa.

Es importante que las empresas tengan políticas claras sobre el uso ético de los sistemas de información y que los empleados estén capacitados para reconocer y evitar prácticas no éticas. La educación continua sobre ética empresarial también es fundamental para garantizar que los empleados estén al tanto de las últimas tendencias y problemas relacionados con la ética empresarial.

Sin mas pre ambulo, manos a la obra con la actividad.

## **JUSTIFICACION**

Un sistema de quejas y denuncias es una herramienta gerencial para el control y mejoramiento continuo de la empresa o institución, toda vez que posibilita el conocimiento sobre la percepción de los clientes de los bienes o servicios que se comercializan en la empresa o institución; esto es, cuáles son las inquietudes, quejas y sugerencias que tienen los usuarios con respecto a los servicios, con miras a mejorar la calidad de los mismos.

En cuanto a las malas prácticas corporativas en un sistema de denuncias, es importante mencionar que la protección del denunciante es fundamental para garantizar la efectividad del sistema. En este sentido, se recomienda que el sistema ofrezca condiciones óptimas de confidencialidad, como la posibilidad de enviar denuncias anónimas, y protección al denunciante frente a represalias.

Es importante destacar que existen normativas que regulan la implementación de sistemas de denuncia en empresas e instituciones. Por ejemplo, en México, desde el 17 de diciembre de 2021, las empresas con más de 250 empleados están obligadas a implementar una solución para la denuncia segura.

Las afectaciones a los usuarios y las malas prácticas corporativas son importantes en un sistema de denuncias por varias razones. En primer lugar, las empresas tienen la responsabilidad de proteger los derechos de sus clientes y usuarios. Si una empresa no cumple con esta responsabilidad, puede causar daños irreparables a sus clientes y usuarios, lo que puede tener un impacto negativo en su reputación y en su capacidad para hacer negocios en el futuro. En segundo lugar, las malas prácticas corporativas pueden tener un impacto negativo en la economía en general.



Por ejemplo, si una empresa utiliza prácticas comerciales deshonestas para obtener una ventaja competitiva, puede distorsionar el mercado y perjudicar a otras empresas que compiten de manera justa. En tercer lugar, las malas prácticas corporativas pueden tener un impacto negativo en la sociedad en general. Por ejemplo, si una empresa contamina el medio ambiente o viola los derechos humanos, puede causar daños irreparables a la sociedad y al medio ambiente<sup>1</sup>.

Es importante que los sistemas de denuncia sean efectivos para garantizar que las empresas sean responsables de sus acciones. Los sistemas de denuncia pueden ayudar a identificar y prevenir malas prácticas corporativas y a proteger los derechos de los usuarios y consumidores. Además, los sistemas de denuncia pueden ayudar a crear un entorno empresarial más justo y equitativo al fomentar la competencia justa y la transparencia.

Ahora que ya sabemos la importancia de lo mencionado anteriormente, seguiremos con nuestra actividad de Ética y Sustentabilidad.

## **DESARROLLO (RECOMENDACIONES)**

Medios de comunicación para gestionar las denuncias, Protocolos de comunicación para gestionar las denuncias, Gestión de reportes.

### **Medios de comunicación para gestionar las denuncias**

En general, existen varios medios de comunicación que se pueden utilizar para gestionar las denuncias, como la línea telefónica, el correo electrónico, el sitio web corporativo, los formularios en línea y los buzones físicos. Además, también se pueden utilizar otros medios como la intranet de la empresa, el boletín de la empresa, los tableros de anuncios, las reuniones informativas u otros eventos internos, las sesiones de formación y el manual del empleado.

Es importante que las organizaciones piensen detenidamente a qué grupos en concreto hay que informar de la existencia de un canal de denuncias (a menudo, son más de los que creemos). Casi todas las partes interesadas, internas y externas, resultan siempre relevantes. Para empresas con sede social en la UE, una de las razones de peso para ampliar el público objetivo de su canal es que muy pronto entrará en vigor una nueva directiva que proporcionará protección a las partes interesadas tanto internas como externas que se atrevan a dar la voz de alarma ante la sospecha de irregularidades dentro de una organización.

### **Recomendaciones para diseñar medios de comunicación que cumplan con los principios de privacidad por diseño:**

- Minimiza la cantidad de datos personales que se recopilan: Asegúrate de que solo se recopilen los datos personales necesarios para el propósito específico del medio de comunicación. No recopiles información adicional que no sea relevante para el propósito.

- Asegúrate de que los datos personales estén protegidos: Utiliza medidas de seguridad adecuadas para proteger los datos personales que se recopilan. Esto puede incluir el cifrado de datos, la autenticación de usuarios y la implementación de políticas de privacidad claras.
- Incluye opciones de privacidad en el diseño del medio: Asegúrate de que los usuarios tengan opciones claras y fáciles de usar para controlar cómo se utilizan sus datos personales. Esto puede incluir opciones para optar por no recibir publicidad personalizada o para eliminar sus datos personales.
- Mantén la transparencia en el uso de datos personales: Proporciona información clara y fácilmente accesible sobre cómo se utilizan los datos personales recopilados por el medio de comunicación. Esto puede incluir una política de privacidad fácilmente accesible y una explicación clara del propósito del medio.
- Realiza pruebas regulares para garantizar el cumplimiento: Realiza pruebas regulares del medio de comunicación para garantizar que cumpla con los principios de privacidad por diseño. Esto puede incluir pruebas de seguridad, pruebas de usabilidad y revisiones regulares de la política de privacidad.

## **Protocolos de comunicación para gestionar las denuncias**

- El Protocolo para la Atención de Denuncias del Comité de Ética y de Prevención de Conflictos de Interés del Organismo Promotor de Inversiones en Telecomunicaciones (PROMTEL).

Este protocolo tiene como objetivo orientar a las personas servidoras públicas de PROMTEL para la presentación de denuncias por posibles incumplimientos al Código de Ética, Reglas de Integridad o al Código de Conducta del Organismo; así como para atender y sancionar el hostigamiento sexual, el acoso sexual y los casos de discriminación en el Organismo.

- El Procedimiento del Canal de Denuncias elaborado por Grupo Atico34.

Este procedimiento describe cómo se debe presentar una denuncia, qué hechos son denunciables, los plazos de respuesta y de la investigación interna, entre otros aspectos.

- El artículo Cómo implementar un sistema de denuncias publicado por WhistleB.
- Este artículo ofrece una guía detallada sobre cómo implementar un sistema de denuncias efectivo en una organización. En particular, se enfoca en la comunicación vinculada directa o indirectamente a un sistema de denuncias.

## **Recomendaciones para diseñar protocolos de comunicación que cumplan con los principios de privacidad por diseño.**

El canal de denuncias surge como medida para proteger a todas las personas que denuncian o informan sobre casos de corrupción, fraude o violaciones de las leyes en los países de la UE.

Estos canales de denuncia van a estar protegidos para evitar que se produzcan represalias contra las personas denunciantes.

La obligación, incluida en la Ley de protección del denunciante que entró en vigor el 13 de marzo de 2023, indica una obligación empresarial que va a afectar a compañías del sector privado con 50 o más personas en plantilla.

Tener un canal de denuncias va a ser obligatorio para las empresas con más de 50 empleados.

Un canal de denuncias debe incluir los siguientes aspectos:

- Tener los medios necesarios para asegurar la confidencialidad en cuanto a la identidad del denunciante, de la persona denunciada y de los testigos. Es decir, únicamente las personas autorizadas tendrán acceso para conocer la identidad de la persona que denuncia y de quienes mencione en su comunicación.
- Mantener la información almacenada durante el tiempo requerido para realizar las investigaciones.
- Permitir la formalización de denuncias tanto escritas como verbales.
- Designar a una persona responsable e imparcial para realizar el seguimiento de las denuncias.
- Mantener almacenadas las denuncias durante un tiempo determinado. Según la Ley habrá que almacenarlas durante un período de 2 años.
- Emitir un acuse de recibo en un plazo no superior a 7 días.
- Permitir únicamente el acceso a las denuncias por parte del personal autorizado.

Para implementar el canal de denuncias obligatorio en la empresa se deben seguir estos pasos:

- Seleccionar las vías de comunicación de las denuncias.

En este paso, habrá que seleccionar si será un canal interno o externo. Además, será necesario diseñar que vías de comunicación se van a usar.

- Nombrar al responsable del canal de denuncias.

El siguiente paso es nombrar a un responsable del canal de denuncias. Puede ser que esa función la realice un equipo de personas y no una única persona responsable.

- Gestionar y elaborar el reglamento del canal de denuncias

En este paso será necesario establecer cuál va a ser el protocolo de recepción, gestión e investigación de las denuncias.

Para ello, habrá que indicar qué personas pueden usar el canal de denuncias, qué vías de comunicación tienen disponibles, qué hechos se pueden denunciar y en qué plazos se van a responder e investigar las mismas.

- Mantener en un registro todas las denuncias.

El canal de denuncias siempre debe contemplar un registro que recoja las denuncias que se reciban, se tramiten o se investiguen.

- Nombrar un Delegado de Protección de Datos.

Este paso no es obligatorio pero sí es muy recomendable designar a una persona como Delegado de Protección de Datos para garantizar la protección de los datos personales incluidos en las denuncias.

- Informar a la plantilla sobre la existencia del canal de denuncias y cómo acceder a él.

El último paso para la correcta implementación del canal de denuncias es comunicarlo a la plantilla para que todas las personas trabajadoras sepan cómo usarlo.

## **Gestión de reportes.**

La gestión de reportes es un conjunto de documentos corporativos que contienen información sobre proyectos y áreas operativas y financieras, lo cual permite monitorear y evaluar el rendimiento de un negocio. Los informes de gestión son una herramienta que se utiliza con la finalidad de tener una visión más estratégica de tu negocio. Gracias a la información contenida en este documento, es posible tomar decisiones basadas en datos valiosos.

Un informe de gestión es una herramienta aplicada en las empresas para mantener a todas las partes interesadas sobre la gestión empresarial siempre actualizadas sobre las actividades son llevadas a cabo en la organización. En definitiva, se encuentran entre los informes internos que los gerentes y ejecutivos utilizan para administrar la organización, tomar decisiones comerciales y monitorear el progreso.

Si deseas tener una visión más estratégica de tu negocio, puedes aprender a hacer un informe de gestión. Sigue nuestras sugerencias. Aquí te dejamos algunos elementos clave para hacer un informe de gestión increíble:

**Definir objetivos claros:**

- Define los objetivos que deseas alcanzar con el informe.

**Seleccionar los indicadores adecuados:**

- Selecciona los indicadores que te permitan medir el progreso hacia tus objetivos.

**Recopilar datos precisos:**

- Asegúrate de recopilar datos precisos y confiables.

**Presentar los datos de manera clara y concisa:**

- Presenta los datos de manera clara y concisa para que sean fáciles de entender.

**Tomar decisiones basadas en los datos:**

- Utiliza los datos para tomar decisiones informadas.

## **Recomendaciones para gestionar reportes que cumplan con los principios de privacidad por diseño.**

La privacidad por diseño es un enfoque preventivo para la protección de la privacidad de los datos. Fue desarrollado en la década de 1990 y su propósito inicial era desarrollar un modelo robusto y escalable para la privacidad de los datos que superaría las «tecnologías de mejora de la privacidad» y los requisitos de cumplimiento normativo más débiles en ese momento para garantizar la privacidad total de los datos. Los principios fundamentales de la privacidad por diseño son los siguientes:

1. Proactivo no reactivo; preventivo, no reparador.
2. Privacidad por defecto.
3. Privacidad integrada en el diseño.
4. Funcionalidad completa: suma positiva, no suma cero.
5. Seguridad de un extremo a otro: protección del ciclo de vida completo.
6. Visibilidad y transparencia.
7. Respeto por la privacidad del usuario.

Para implementar la privacidad por diseño en la actividad empresarial, se recomienda lo siguiente:

1. Considerar la privacidad por diseño como un requisito obligatorio en cualquier nuevo producto o servicio.
2. Realizar un análisis de riesgos de los derechos personales y evaluaciones de impacto relativas a la protección de datos personales.
3. Documentar las decisiones que se adopten dentro de la iniciativa o por parte de la organización que protejan y garanticen la privacidad.



## CONCLUSION

Las afectaciones a los usuarios y las malas prácticas corporativas son importantes en un sistema de denuncias porque pueden causar daños irreparables a los clientes y usuarios, perjudicar la economía y la sociedad en general. Los sistemas de denuncia son importantes para garantizar que las empresas sean responsables de sus acciones y para crear un entorno empresarial más justo y equitativo.

En esta unidad se definen algunas situaciones no éticas que los sistemas de información pueden ocasionar en sus usuarios. La intención de estos, es generar conciencia de problemas que se han normalizado. El interés de resaltar el problema es que nuevas mentes puedan utilizar su talento para disminuir o eliminar los riesgos de afectación a los usuarios de los sistemas de información e internet.

Tanto las afectaciones a los usuarios como las malas prácticas son el resultado de la falta de interés del persona de sistemas. Por ellos, es de vital importancia fomentar los lineamientos para los códigos de ética y prácticas sustentables tanto en las organizaciones como en la sociedad en general, de manera que se prioricen.

Las afectaciones a los usuarios y las malas prácticas corporativas son importantes en un sistema de denuncias por varias razones. En primer lugar, las empresas tienen la responsabilidad de proteger los derechos de sus clientes y usuarios. Si una empresa no cumple con esta responsabilidad, puede causar daños irreparables a sus clientes y usuarios, lo que puede tener un impacto negativo en su reputación y en su capacidad para hacer negocios en el futuro. En segundo lugar, las malas prácticas corporativas pueden tener un impacto negativo en la economía en general.

Ya hemos analizado las afectaciones a usuarios y malas prácticas corporativas en un sistema de denuncias, ahora nos hace falta conocer un poco más en la siguiente actividad.

## REFERENCIAS Y LINK

*Privacidad por diseño en un sistema de denuncias.* (n.d.). Bing. Retrieved October

21, 2023, from

<https://www.bing.com/search?q=privacidad+por+dise%C3%B1o+en+un+sistema+de+denuncias&qsn&form=QBRE&sp=-1&lq=o&pq=privacidad+por+dise%C3%B1o+en+un+sistema+de+denuncias&sc=o-48&sk=&cvid=1B18F2CCB59642BA95FE892FD6C1E5A3&ghsh=o&ghacc=o&ghpl>

*Prácticas no éticas en los sistemas de información de las empresas.* (n.d.). Bing.

Retrieved October 21, 2023, from

<https://www.bing.com/search?q=pr%C3%A1cticas+no+%C3%A9ticas+en+los+sistemas+de++informaci%C3%B3n+de+las+empresas&qsn&form=QBR E&sp=-1&lq=1&pq=pr%C3%A1cticas+no+%C3%A9ticas+en+los+sistemas+de++informaci%C3%B3n+de+las+empresas&sc=2-67&sk=&cvid=39F44DF9877C408DAE479F0321AD9AD9&ghsh=o&ghacc=o&ghpl>

Agea, O. (2023, April 24). *Canal de denuncias obligatorio: ¿qué es y cómo*

*implantarlo?* Firmafy. <https://firmafy.com/canal-de-denuncias-obligatorio-que-es-y-como-implantarlo/>

## LINK DE GITHUB

[Omarsitho1988 \(github.com\)](https://github.com/Omarsitho1988)