

Ingeniería en Desarrollo de Software.

Nombre de la Actividad.

Actividad 2. Privacidad por Diseño.

Actividad [#2]

Etapas #2 – Privacidad por Diseño.

Nombre del Curso.

Ética y Sustentabilidad.

Tutor: Jessica Hernández Romero.

Alumno: José Luis Martín Martínez.

Fecha: 25/09/2023.

Índice.

| | |
|---|-----------|
| Contextualización y Actividades..... | 4 |
| Introducción..... | 6 |
| Descripción..... | 8 |
| Justificación..... | 12 |
| Desarrollo..... | 16 |
| ➤ Medio de comunicación para gestionar las denuncias. | |
| ➤ Protocolo de comunicación para gestionar las denuncias. | |
| ➤ Gestión de reportes. | |
| Conclusión..... | 17 |
| Referencias..... | 18 |

Contextualización y Actividades.

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.

Introducción.

En esta segunda actividad, hablaremos respecto la privacidad de datos desde su diseño con base en la actividad 1, y determinar 3 recomendaciones por cada función del sistema de denuncias como medio de comunicación, protocolo de comunicación para gestionar las denuncias y gestión de reportes. La privacidad de datos desde su diseño es esencial para abordar las preocupaciones éticas relacionadas con la recopilación y el uso de datos personales, así como para garantizar que los sistemas y tecnologías se utilicen de manera sostenible y responsable. La consideración de la privacidad desde el inicio es un paso fundamental para crear un entorno digital ético y sustentable en un mundo cada vez más conectado. En la era digital en la que vivimos, la privacidad de datos se ha convertido en un tema fundamental que afecta no solo a la forma en que interactuamos en línea, sino también a cuestiones éticas y sostenibles en nuestra sociedad. Desde sus inicios, Internet y las

tecnologías digitales han permitido la recopilación masiva de datos personales. Esta recopilación plantea cuestiones éticas acerca de cómo se utilizan, almacenan y protegen estos datos. Además, el aumento en la recopilación de datos tiene un impacto directo en la sustentabilidad, ya que puede llevar al agotamiento de recursos y a un mayor consumo de energía. La privacidad de datos desde su diseño se basa en la premisa de que la protección de la privacidad y la ética no deben ser consideraciones posteriores, sino principios fundamentales que deben incorporarse desde el inicio de cualquier proyecto, sistema o tecnología. Esto implica tomar medidas proactivas para garantizar que los datos personales estén protegidos y que las prácticas de recopilación y uso de datos sean éticas.

Descripción.

Como mencionamos en la introducción, es una infraestructura tecnológica y un conjunto de procesos que incorpora principios fundamentales de protección de datos personales, ética y responsabilidad ambiental. Este sistema no solo cumple con las normativas y regulaciones de privacidad de datos, sino que va más allá al fomentar la ética y la sustentabilidad en la toma de decisiones relacionadas con los datos. Contribuye a la construcción de una sociedad digital más confiable y ética, donde los individuos tienen un mayor control sobre su información personal y se minimiza el impacto ambiental de la recopilación y el uso de datos. En el contexto de la materia de ética y sustentabilidad, este sistema representa una herramienta esencial para abordar desafíos éticos y sustentables en un mundo digitalizado. El objetivo de un sistema de privacidad de datos desde su diseño es garantizar que la privacidad y la ética sean consideraciones centrales en la tecnología y los procesos, promoviendo la confianza pública, protegiendo los derechos individuales y contribuyendo a

un mundo más ético y sostenible. Esto implica no solo cumplir con las regulaciones de privacidad, sino también ir más allá y adoptar un enfoque proactivo que aborde las cuestiones éticas y de sustentabilidad relacionadas con la recopilación y el uso de datos.

Justificación.

Es momento de poder justificar el por qué debemos de conocer a detalle la implementación de nuestra actividad, para promover un sistema de denuncias que respete la privacidad de los denunciantes y se alinee con los objetivos de sustentabilidad y ética, es esencial desde una perspectiva legal, ética y de sostenibilidad. Esto no solo protege los derechos fundamentales de las personas, sino que también fomenta la confianza, la participación y la responsabilidad en la organización, contribuyendo a una cultura ética y sostenible. También se basa en varios argumentos claves como.

Protección de derechos fundamentales: Respetar la privacidad de los denunciantes es un imperativo ético y legal. Cada individuo tiene el derecho fundamental a la privacidad, y un sistema de denuncias que no protege adecuadamente la privacidad de los denunciantes podría infringir estos derechos. Garantizar la privacidad es una obligación ética y legal.

Fomento de la confianza y participación: Un sistema de denuncias ético fomenta la confianza de los denunciantes y la comunidad en general. Cuando las personas confían en que sus denuncias se manejarán de manera ética y respetuosa de la privacidad, es más probable que participen y denuncien irregularidades, lo que es esencial para la identificación y corrección de problemas.

Protección contra represalias: Proteger la privacidad de los denunciantes, incluida la posibilidad de realizar denuncias anónimas, es esencial para prevenir represalias. Un sistema

que no garantice la privacidad y la protección de los denunciantes podría desalentar la denuncia de problemas éticos o de sustentabilidad por temor a represalias.

Sustentabilidad y responsabilidad corporativa: La sustentabilidad no se trata solo de cuestiones ambientales, sino también de prácticas comerciales éticas y responsabilidad corporativa. La gestión adecuada de denuncias sobre cuestiones éticas y de sustentabilidad es esencial para garantizar la responsabilidad y sostenibilidad de la organización.

Cumplimiento normativo legal: En muchos países, existen regulaciones y leyes que requieren la implementación de sistemas de denuncias éticos y respetuosos de la privacidad. El incumplimiento de estas regulaciones puede dar lugar a sanciones legales y daños a la reputación.

Mejora continua: Un sistema de denuncias ético y respetuoso de la privacidad contribuye a la mejora continua de las prácticas éticas y sustentables de la organización. Las denuncias pueden servir como una fuente valiosa de retroalimentación para identificar áreas que requieren atención y mejora.

Reputación y responsabilidad social: Un sistema de denuncias ético y alineado con la sustentabilidad refuerza la reputación de la organización como un actor socialmente responsable. Esto puede ser atractivo tanto para los clientes como para los inversores y, en última instancia, puede contribuir a un mayor éxito a largo plazo.

Como podemos observar que en cada argumento promovemos un sistema de denuncias que respete la privacidad de los denunciantes y se alinee con los objetivos de sustentabilidad y ética es esencial desde una perspectiva legal, ética y de sostenibilidad. Esto no solo protege los derechos fundamentales de las personas, sino que también fomenta la confianza, la

participación y la responsabilidad en la organización, contribuyendo a una cultura ética y sostenible.

Desarrollo.

➤ Medio de comunicación para gestionar las denuncias.

Para diseñar medios de comunicación que cumplan con los principios de privacidad por diseño es fundamental, proteger la información personal de los usuarios desde el principio del desarrollo, promoviendo confianza de los usuarios y protección de datos personales. Le presento 3 recomendaciones.

Encriptación de Comunicaciones: Implementa una encriptación sólida para todas las comunicaciones dentro de tus medios de comunicación. Esto incluye la encriptación de extremo a extremo para mensajes privados y la encriptación de datos en tránsito. La encriptación protege la privacidad al garantizar que solo las partes autorizadas puedan acceder a la información, incluso si los datos se interceptan.

Gestión de Permisos de Usuario: Diseña tu plataforma de medios de comunicación para que los usuarios tengan un control claro y granular sobre sus datos y permisos. Esto incluye permitir a los usuarios elegir qué información comparten, con quién la comparten y cómo se utiliza. Ofrecer configuraciones de privacidad personalizables permite a los usuarios tomar decisiones informadas y ejercer control sobre su información.

Política de Retención de Datos Transparente: Establece una política de retención de datos clara y transparente que informe a los usuarios sobre cuánto tiempo se conservarán sus datos y cuándo se eliminarán. La retención de datos solo durante el tiempo necesario es

esencial para respetar la privacidad y cumplir con las regulaciones de privacidad. Comunica estas políticas de manera clara a los usuarios.

➤ **Protocolo de comunicación para gestionar las denuncias.**

Diseñar protocolos de comunicación que cumplan con los principios de privacidad por diseño es esencial, garantizar que la información se transmita de manera segura y respetando la privacidad de los usuarios desde la etapa inicial del desarrollo. La privacidad y la seguridad deben estar en el centro de cualquier protocolo de comunicación para proteger la información personal y fomentar la confianza de los usuarios. Le presento 3 recomendaciones.

Encriptación Fuerte y Estándares de Seguridad: Implementa una encriptación sólida y protocolos de seguridad estándar en todas las comunicaciones. Utiliza protocolos de cifrado de datos reconocidos y confiables, como TLS/SSL para transmisiones web. Asegúrate de que la información se transmita de forma segura y que las claves de encriptación se manejen de manera adecuada. La encriptación protege los datos durante la transmisión y es esencial para la privacidad por diseño.

Autenticación y Control de Acceso: Diseña protocolos que incluyan mecanismos de autenticación robustos para verificar la identidad de los usuarios y controlar el acceso a la información. Esto garantiza que solo las personas autorizadas puedan acceder a los datos. La autenticación multifactorial (MFA) es una capa adicional de seguridad que puede agregar una capa de protección significativa.

Registro y Auditoría Transparente: Implementa un registro transparente y mecanismos de auditoría para rastrear y registrar todas las actividades de comunicación. Esto no solo mejora la seguridad, sino que también permite la identificación de posibles brechas de

privacidad y el seguimiento de eventos relevantes. Los registros y auditorías son útiles para la detección y mitigación de incidentes de seguridad y para demostrar el cumplimiento normativo.

➤ **Gestión de reportes.**

Gestionar reportes de manera que cumplan con los principios de privacidad por diseño es esencial para garantizar la protección de la información personal de manera coherente y efectiva, asegurándose de que la información se maneje de manera ética y responsable. La privacidad es fundamental en la gestión de reportes y estas medidas garantizan su cumplimiento desde el diseño. Le presento 3 recomendaciones.

Anonimización y Pseudonimización de Datos: Antes de compartir o almacenar reportes, aplica técnicas de anonimización y pseudonimización de datos para proteger la privacidad de los individuos. Reemplaza la información identificable con identificadores únicos o datos despersonalizados. Esto garantiza que los reportes no contengan información que pueda vincularse directamente a individuos y, al mismo tiempo, mantienen su utilidad para análisis y seguimiento.

Control de Acceso y Gestión de Permisos: Implementa un sólido sistema de control de acceso y gestión de permisos para garantizar que solo personas autorizadas tengan acceso a los reportes. Define roles y permisos claros para garantizar que solo aquellos que necesitan la información tengan acceso a ella. Esto previene el acceso no autorizado y protege la privacidad de los datos.

Política de Retención y Eliminación de Datos: Establece una política de retención de datos clara que especifique cuánto tiempo se conservarán los reportes y cuándo se eliminarán de manera segura. La retención de datos solo durante el tiempo necesario garantiza que no se acumule información personal innecesaria y protege la privacidad de los individuos cuyos datos se incluyen en los reportes.

Conclusión.

En esta segunda actividad, en base a la actividad 1, aprendimos que se requiere no solo identificar mala prácticas de medios de comunicación, protocolos y gestión de reportes, sino promover cambios de seguridad que precisen el mejoramiento de estos aspectos. Como por ejemplos determinar 3 recomendaciones por cada función del sistema de denuncias, estas recomendaciones están enfocados en que el sistema promueva la privacidad de los datos desde su diseño. En esta actividad se define 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 practicas son el resultado de la falta de interés del personal de sistemas. Por ello, es de vital importancia fomentar los lineamientos para los códigos de ética y practicas sustentables tanto en las organizaciones como en la sociedad en general, de manera que se prioricen.

Referencias.

Implementación de Sistema de Denuncias. (s/f). Ethicsglobal.com. Recuperado el 26 de octubre de 2023, de <https://www.ethicsglobal.com/es/implementacion-del-sistema-etico-de-denuncias.html>

EthicsGlobal. (s/f). Ethicsglobal.com. Recuperado el 20 de octubre de 2023, de <https://www.ethicsglobal.com>

¿Qué es un canal de denuncias? (s/f). Worldcomplianceassociation.com. Recuperado el 26 de octubre de 2023, de <https://www.worldcomplianceassociation.com/1651/articulo-que-es-un-canal-de-denuncias.html>

