EcoLife

ANÁLISIS CON SENTIDO HUMANO

Aviso de Derechos de Autor

El desarrollo de **EcoLife** contó con la valiosa colaboración de estudiantes del Tecnológico de Monterrey:

- Abigail Pérez García
- Gerardo Deustúa Hernández
- Raymundo Iván Díaz Alejandre
- Rodrigo López Guerra

Índice

Introducción

Durante la creación de software y el manejo de redes, es fundamental garantizar la confianza de los usuarios para que puedan interactuar de manera efectiva, segura y confiable con las aplicaciones. Este principio cobra aún más relevancia en el desarrollo de herramientas destinadas a reducir la huella de carbono, donde la tecnología digital desempeña un rol crucial en los esfuerzos globales por mitigar el impacto ambiental. Sin embargo, para lograrlo, no basta con crear aplicaciones funcionales; es imprescindible integrar estrategias sólidas de ciberseguridad, comprender las normativas legales aplicables y fomentar un enfoque sostenible que abarque tanto el diseño como la operación de las soluciones tecnológicas.

La ciberseguridad no solo protege la información sensible de los usuarios, sino que también asegura la integridad y viabilidad de los sistemas en los que se confía para recolectar, procesar y analizar datos. En un entorno digital cada vez más complejo, resulta crítico implementar prácticas de gobernanza de Internet, fortalecer las posturas de seguridad y adoptar tecnologías innovadoras que minimicen el riesgo de ciber amenazas. Al mismo tiempo, el enfoque debe ser sostenible, promoviendo un desarrollo tecnológico que contribuya a la reducción de emisiones de carbono y al uso responsable de los recursos disponibles.

En este contexto, la creación de aplicaciones que aborden la problemática ambiental requiere de una visión integral que combine ciberseguridad, sostenibilidad y confiabilidad. Este enfoque no solo mejora la experiencia del usuario, sino que también permite garantizar un manejo ético y responsable de los datos recopilados, contribuyendo al desarrollo de sistemas confiables que inspiren confianza y reduzcan la exposición a riesgos. A través de esta visión holística, es posible proyectar un futuro tecnológico que apoye la lucha contra el cambio climático, fomente la sostenibilidad y asegure un entorno digital libre de cibercriminales.

La importancia de la Ciberseguridad

Ciberseguridad

Dentro del reto, el socio formador requiere una aplicación que maneje datos sensibles del usuario, como el sí tiene coche, sus horarios, su consumo eléctrico, entre otros factores que permitan el desarrollo correcto de las funcionalidades de la aplicación, sin embargo, es fundamental tener siempre a la vista el concepto de confidencialidad, ya que este va a ser el centro en el que basamos el manejo de datos, siempre procurando que todo lo que nosotros administremos sea propiamente del usuario y no se haga mal uso del mismo, como lo han hecho otras redes sociales como Facebook, ni sacar provecho de la confianza que nuestros usuarios puedan depositar en el proyecto.

El fin de recopilar información es para que nuestro sistema pueda trabajar de mejor manera, permitiendo un entendimiento mayor del contexto del usuario, y proveyendo soluciones reales a problemas cotidianos. El compartir estos datos con terceras personas, o venderlas pueden poner inclusive la vida de los usuarios en riesgos, ya que, al conocer sus hábitos, puedes planificar el cómo poder hacerle daño a alguien, o inclusive ver en qué momento en el mundo virtual son más vulnerables y propensos a caer e engaños y robar aún más información de ellos que les puede afectar de maneras graves.

Delitos y Posibles Consecuencias

Ya que vimos lo valioso que puede llegar a ser la confidencialidad a la hora de tratar a los clientes, es hora de ver qué podría pasar en dado caso que se llegase a romper este pacto. En primera instancia, el socio formador, denominado en esta sección como cliente, perdería su reputación y confiabilidad, y en vez de hacer un cambio hacia una problemática real a favor de la sociedad, simplemente está creando un nuevo problema, impulsando las inseguridades a los usuarios de la aplicación y sus servicios alrededor del mundo virtual y sus consecuencias, creando así una cadena de desinformación y disminuyendo la posibilidad de que otras aplicaciones también puedan lograr dicho cambio.

Siguiendo con este dilema, algunas de las consecuencias que trae el romper la confidencialidad pueden llegar a ser: fraudes bancarios, phishing, robo de identidad, secuestro, robo de propiedad, robo de datos personales, extorsión, trata de personas, mal uso de cuentas digitales, inculpa miento de inocentes a través de chantaje y pruebas falsas o incompletas, enfermedades mentales (tal como depresión, ansiedad, tendencias suicidas), asesinato, entre otros muchos más delitos. Esto debido al compartir datos sensibles del usuario que los pueden dejar vulnerables ante los criminales y tener un efecto inverso a lo planeado por el socio formador. Estas son algunas consecuencias que tienen estas acciones sobre los usuarios, pero ¿qué hay de nuestro cliente?

Afecciones al Cliente

Nuestro socio formador está confiando plenamente en que podamos hacer un trabajo grandioso manejando los datos y guardando el respeto debido para no afectar su imagen ante sus usuarios, la cual debemos de cuidar. En dado caso que no se tenga previsto el caso de ciberseguridad en la aplicación y un cibercriminal pueda entrar a nuestro producto, los resultados pueden llegar a ser severos. Para empezar, los objetivos del proyecto pueden verse afectados, ya que, al ser una aplicación enfocada a la concientización y educación en temas con relación al medio ambiente, puede llegar a crear y hacer crecer una cadena de desinformación a los usuarios, actualizando nuestras bases de datos a cosas que no son y manipulando a los usuarios para realizar acciones, o creer cosas, llegando a afectar en el mercado y en la sociedad a nuestro cliente.

De igual manera se rompería la confidencialidad, llegando a dejar a los usuarios vulnerables y al cliente con la responsabilidad de velar por el bienestar de sus usuarios para evitar crear mayor conflicto. Las brechas de seguridad que una aplicación puede tener pueden tener consecuencias como lo es el robo de datos e información, ya sea del cliente o los usuarios, dejando un sin fin de actos ilícitos que pueden llegar a perjudicar la causa que quiere el cliente erradicar y creando una herramienta ineficaz y dañando nuestra confiabilidad como desarrolladores.

Normativas y Leyes de la Ciberseguridad

Normativa de Ciberseguridad

El proyecto de la aplicación para la reducción de la huella de carbono requiere el manejo de datos sensibles, como el consumo energético y los hábitos de transporte de los usuarios. Es fundamental que estos datos se gestionan en conformidad con las normativas de protección de datos, tales como el Reglamento General de Protección de Datos (GDPR) o la Ley General de **Protección de Datos Personales (LGPD).** Estas normativas establecen los estándares para el manejo y almacenamiento de datos, garantizando que la información personal de los usuarios esté protegida y se utilice solo para los fines específicos del proyecto.

El incumplimiento de estas normativas puede llevar a sanciones graves y a una pérdida de confianza en la aplicación, afectando su reputación y viabilidad a largo plazo. Además, la violación de las leyes de ciberseguridad puede exponer a los usuarios a riesgos como el robo de identidad, el fraude financiero y la manipulación de datos.

Delitos Cibernéticos

La falta de seguridad adecuada en el manejo de datos puede derivar en la comisión de delitos cibernéticos. Estos delitos incluyen phishing, robo de identidad, fraude bancario, y extorsión, entre otros. Cuando los datos sensibles de los usuarios no se protegen adecuadamente, los cibercriminales pueden acceder a esta información y utilizarla para realizar actividades ilícitas, poniendo en peligro tanto la privacidad como la seguridad de los usuarios.

La confidencialidad de los datos es esencial para evitar que terceros puedan aprovecharse de la información sensible. Si los datos de los usuarios son vulnerados, las consecuencias pueden ser devastadoras, desde pérdidas económicas hasta daños a la reputación tanto del cliente como de los desarrolladores de la aplicación. Además, esto puede tener un efecto en cadena, afectando la confianza de los usuarios en otras aplicaciones similares y dificultando el avance de soluciones digitales sostenibles.

Consecuencias Legales

El no observar las normativas y los estándares de ciberseguridad puede generar serias consecuencias legales para el cliente y los desarrolladores del proyecto. Las regulaciones internacionales como el **GDPR** imponen multas significativas para las organizaciones que no protejan adecuadamente los datos personales. Las sanciones pueden ser de hasta el 4% de los ingresos globales anuales de la empresa, lo que representa una carga financiera considerable.

Además, la pérdida de confianza por parte de los usuarios puede resultar en una disminución significativa del uso de la aplicación, afectando la capacidad del proyecto para lograr sus objetivos. La seguridad de los usuarios no solo es una obligación ética, sino también un requerimiento legal y comercial indispensable para el éxito del proyecto.

¿Cómo se Implementa la Ciberseguridad?

Gobernanza del Internet

Para garantizar que la aplicación sea sostenible y segura, se deben implementar prácticas sólidas de gobernanza de Internet. La gobernanza de Internet abarca las normas y políticas que rigen el uso de Internet, con énfasis en la protección de datos y en la eficiencia en el manejo de recursos.

En este contexto, la aplicación reflejará la gobernanza de Internet mediante políticas de privacidad de datos que cumplan con las normativas internacionales de protección de la información, como el Reglamento General de Protección de Datos (GDPR). Al limitar el acceso y uso innecesario de datos, no solo se protege al usuario, sino que también se minimiza el consumo energético, ya que el procesamiento de datos representa una fuente importante de emisión de carbono.

Además, la aplicación se diseñará para optimizar el flujo de datos. Esto implica reducir la cantidad de información transmitida y almacenada en la nube, ya que el almacenamiento masivo y la transmisión frecuente de datos pueden elevar significativamente el consumo de energía. Al implementar prácticas de gobernanza que prioricen una transmisión y almacenamiento de datos eficiente, se contribuye a la reducción de la huella de carbono en el entorno digital.

Estrategias de Ciberseguridad: Características Básicas

La aplicación integrará estrategias básicas de ciberseguridad para garantizar que la protección de los datos no comprometa su objetivo principal de reducción de la huella de carbono. Estas estrategias abarcan medidas de protección contra ataques, detección de incidentes y respuestas rápidas a amenazas, todo esto orientado a proteger tanto la seguridad del usuario como la sostenibilidad de la aplicación.

En primer lugar, se emplearán medidas de protección como la encriptación de datos y la autenticación multifactorial para evitar accesos no autorizados. La encriptación de datos, por ejemplo, es una medida que ayuda a proteger la información de los usuarios sin generar un consumo elevado de energía cuando se optimiza adecuadamente. Esto es clave en una aplicación orientada a la sostenibilidad, ya que evita el uso innecesario de recursos computacionales y reduce la carga en los servidores.

Además, la aplicación contará con herramientas de detección de amenazas que permitan identificar y mitigar cualquier riesgo de ciberseguridad en tiempo real. Al tener una respuesta rápida ante posibles ataques, se asegura la continuidad de la operación de la aplicación, evitando interrupciones que podrían aumentar el consumo de energía, como las reiniciaciones o el uso de más servidores de respaldo. Estas estrategias de seguridad contribuyen no solo a la protección de los datos del usuario, sino también a mantener una operación sostenible.

Postura de Ciberseguridad

La postura de ciberseguridad de la aplicación será proactiva y preventiva, lo que significa que se buscará anticipar los riesgos y actuar antes de que ocurran los incidentes. Al adoptar esta postura, no solo se protege a los usuarios, sino que también se asegura que la aplicación funcione de forma continua y eficiente, reduciendo así el impacto ambiental.

Parte de esta postura incluye la evaluación continua de riesgos y la implementación de prácticas de monitoreo constantes. Esto permite identificar de manera temprana cualquier vulnerabilidad en el sistema, de modo que se puedan tomar acciones correctivas antes de que la aplicación sea afectada. Una postura de ciberseguridad robusta evita la necesidad de realizar intervenciones energéticamente intensivas, como el restablecimiento de sistemas o la recuperación de datos, las cuales pueden aumentar el consumo de recursos.

Otra práctica importante dentro de esta postura es la educación y concientización de los usuarios en temas de seguridad. Al informarles sobre la importancia de utilizar la aplicación de forma segura y de no compartir datos sensibles, se fortalece la ciberseguridad general de la plataforma y se contribuye indirectamente a la sostenibilidad, al reducir

Eco espacio

Tecnológico de Monterrey