Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |3| Afectación a Usuario.

Ética y Sustentabilidad.

Ingeniería en Desarrollo de Software.

TUTOR: Urbano Francisco Ortega Rivera.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 15/11/2025.

Introducción.

En esta actividad final de la materia Ética y sustentabilidad, nos enfocamos en la protección del usuario en el entorno digital es primordial. Mientras que en la actividad anterior nos centramos en las recomendaciones para el diseño de medios y protocolos con el fin de proteger la Privacidad por Diseño, ahora cambiaremos el enfoque.

En esta sesión, nuestra meta es desarrollar directrices específicas para el diseño de medios de comunicación y sus protocolos que busquen evitar afectaciones directas a los usuarios. Esto implica ir más allá de la mera privacidad y considerar aspectos como la seguridad, la usabilidad, la transparencia, y la confianza. Adicionalmente, se establecerán pautas cruciales para la gestión de reportes. Un sistema de reporte efectivo y sensible es fundamental para mitigar daños post-incidentes, asegurando que las quejas y vulnerabilidades sean tratadas de manera rápida, ética y transparente, minimizando así las consecuencias negativas para el usuario final. El resultado será un marco de recomendaciones para un diseño de sistemas de comunicación más seguros y centrados en el usuario.

Descripción.

En esta actividad final de Ética y Sustentabilidad, culminamos nuestro estudio enfocándonos en la protección integral del usuario en el ecosistema digital. Si bien la fase anterior abordó la Privacidad por Diseño en medios y protocolos, ahora la prioridad es generar recomendaciones específicas para evitar afectaciones directas a los usuarios.

Esto nos obliga a ampliar nuestra visión ética, integrando principios de seguridad, usabilidad intuitiva, transparencia total en el manejo de datos y la construcción de confianza a través de protocolos robustos. El objetivo es diseñar medios de comunicación inherentemente más seguros. Una pieza clave será la creación de pautas para la gestión de reportes. Un sistema de reporte debe ser más que una casilla de quejas: debe ser una herramienta efectiva, rápida y sensible que permita una mitigación de daños post-incidente ética y transparente. El resultado es un marco de recomendaciones para un diseño de

sistemas de comunicación que priorice la dignidad y la seguridad del usuario.

Justificación.

La actividad anterior sentó las bases al enfocarse en la Privacidad por Diseño (Privacy by Design) aplicada a los medios de comunicación y sus protocolos. Sin embargo, una perspectiva centrada únicamente en el diseño podría pasar por alto las afectaciones directas y tangibles a los usuarios finales.

Este ejercicio se enfoca en expandir las recomendaciones hacia la experiencia y seguridad del usuario como principal preocupación. Es crucial diseñar no solo para la privacidad técnica, sino también para prevenir el daño o la victimización de los usuarios como por ejemplo, por desinformación, acoso o exposición de datos sensibles. Se determinarán pautas para el diseño de protocolos y medios, como la encriptación, la moderación de contenido y la minimización de datos que proteja activamente a las personas. Además, se abordará la gestión de reportes para garantizar una respuesta efectiva y humana que mitigue rápidamente el daño, evitando la revictimización o la inacción. Así, se garantiza una aproximación integral que prioriza tanto la protección estructural como el bienestar del usuario.

Desarrollo.

En esta parte final de la actividad nos enfocaremos a realizar la documentación de la materia Ética y sustentabilidad donde nos enfocaremos en expandir las recomendaciones hacia la experiencia y seguridad del usuario como principal preocupación. Nos centramos en las recomendaciones para evitar las afectaciones a los usuario dando 3 ejemplos de cada una de las funciones del sistema: el diseño de medios, protocolos y gestión de reportes.

Link: GitHub.

Afectaciones a usuarios Recomendaciones:

Medios de comunicación para gestionar las denuncias.

Para evitar afectaciones a los usuarios en una aplicación con funcionalidad de gestión de denuncias, el diseño de los medios de comunicación debe centrarse en la transparencia, la seguridad de los datos y la minimización del daño.

1. Protocolo de cifrado y minimización de datos:

- Recomendación: Implementar el cifrado de extremo a extremo para cualquier canal de comunicación que transmita información sensible (ej. detalles de la denuncia, datos personales de la víctima o del reportado).
- Para evitar afectaciones: Esto garantiza que solo los usuarios denunciante/administrador puedan acceder al contenido, protegiéndolo de interceptaciones y filtraciones. Además, aplicar la minimización de datos asegura que solo se recopile la información estrictamente necesaria para procesar la denuncia, reduciendo el riesgo en caso de una brecha de seguridad.

2. Canal de denuncia asistido y no victimizante:

- Recomendación: Diseñar el flujo de denuncia para que sea guiado, claro y empático, usando un lenguaje neutral y ofreciendo opciones de anonimato.
- Para evitar afectaciones: Un medio de comunicación mal diseñado puede revictimizar al usuario “si tiene que repetir los detalles traumáticos varias veces o si se siente juzgado”. El sistema debe incluir checklists y preguntas cerradas cuando sea posible, y ofrecer recursos de apoyo, “enlaces a soporte legal o psicológico” inmediatamente después de enviar la denuncia.

Esto facilita el proceso y minimiza el estrés emocional.

3. Protocolo de trazabilidad y notificación transparente:

- Recomendación: Establecer un protocolo de comunicación claro donde el usuario reciba una notificación inmediata de recepción, un código de seguimiento único y actualizaciones periódicas sobre el estado de su denuncia: "En Revisión," "Escalado," "Acción Tomada".
- Para evitar afectaciones: La inacción o la falta de información genera ansiedad, desconfianza y la percepción de que la denuncia fue ignorada, lo cual es una afectación emocional y disuadir a futuros reportes. La trazabilidad transparente empodera al usuario, le da control sobre el proceso y asegura que se está actuando de manera responsable.

Protocolos de comunicación para gestionar las denuncias.

Diseñar protocolos de comunicación efectivos y seguros es esencial para prevenir la afectación a usuarios en una aplicación de gestión de denuncias, y van más allá del simple medio de la interfaz.

1. Protocolo de identidad y autenticación ciega:

- Recomendación: El protocolo debe permitir el envío de una denuncia o reporte de forma auténtica pero anónima mediante el uso de credenciales ciegas “criptografía o identificadores temporales” no vinculables al usuario real como tokens únicos.
- Para evitar afectaciones: Esto evita la afectación por represalias o exposición de datos personales. El protocolo garantiza que el sistema pueda verificar que la denuncia es legítima “no spam” y darle seguimiento, mientras que la identidad real del denunciante permanece

encriptada o disociada para el personal de moderación, eliminando el riesgo de fuga de información o presión externa.

2. Protocolo de comunicación asíncrona y segura para el feedback:

- Recomendación: Utilizar un protocolo de mensajería asíncrona para todas las notificaciones de feedback sobre la denuncia. Estas comunicaciones deben enviarse a través de un buzón interno seguro dentro de la app “no a emails o SMS” y notificar al usuario solo que "hay un mensaje nuevo" sin revelar el contenido sensible.
- Para evitar afectaciones: Los protocolos de comunicación externa “email, SMS” son susceptibles a la interceptación y pueden revelar detalles sensibles de la denuncia a terceros no autorizados. Al usar un protocolo asíncrono y seguro, se asegura que el feedback como el estado de la investigación o la acción tomada solo sea accesible después de que el usuario haya iniciado sesión de forma segura en la aplicación, protegiendo la confidencialidad del proceso.

3. Protocolo de escalamiento jerárquico con registro inmutable:

- Recomendación: El protocolo de flujo de trabajo debe incluir niveles de escalamiento predefinidos “Nivel 1: Moderadores, Nivel 2: Legal, Nivel 3: Alta Dirección”, con tiempos de respuesta máximos obligatorios y un registro inmutable (logging) de quién accedió a la denuncia y cuándo.
- Para evitar afectaciones: Esto combate la inacción y el riesgo de manipulación interna. Al protocolizar el tiempo de respuesta y la jerarquía, se asegura que las denuncias no queden estancadas y se actúe a tiempo para mitigar la afectación como “detener un acoso o eliminar contenido dañino”. El registro inmutable actúa como una auditoría permanente, asegurando la responsabilidad de los gestores y protegiendo al usuario de posibles fallas en el proceso.

Gestión de reportes.

Una gestión de reportes efectiva es la línea de defensa final para evitar que los usuarios sufran afectaciones prolongadas o secundarias (revictimización). Estas recomendaciones se centran en el proceso posterior al envío del reporte.

1. Protocolo de triage y respuesta en plazos definidos:

- Recomendación: Implementar un sistema de triage automatizado que clasifique las denuncias por nivel de riesgo/urgencia y asigne un Acuerdo de Nivel de Servicio (SLA) estricto para la acción inicial. Ejemplo de Triage:
    - Riesgo Alto (amenazas de violencia física o suicidio) SLA: Respuesta y acción en menos de 1 hora.
    - Riesgo Medio (acoso no violento) SLA: Respuesta inicial en 24 horas.
- Para evitar afectaciones: Combate la inacción y garantiza la mitigación rápida del daño. Al protocolizar los tiempos de respuesta según el riesgo, se asegura que las situaciones más graves que representan un peligro inminente para el usuario sean abordadas de inmediato, evitando que la afectación escale.

2. Protocolo de Soporte Interdisciplinario y Referencia Externa:

- Recomendación: Establecer un protocolo de referencia obligatoria a recursos externos como líneas de ayuda, servicios legales, soporte psicológico para todos los reportes que involucren daño emocional o físico.
- Para evitar afectaciones: Reconoce las limitaciones de la aplicación como gestor de denuncias. La aplicación puede tomar la acción técnica “bloquear al usuario acosador”, pero no puede

ofrecer soporte emocional o legal. Este protocolo evita la afectación por falta de apoyo integral, proporcionando al usuario herramientas profesionales externas que lo ayuden a recuperarse del incidente.

3. Protocolo de calidad y cierre confirmado con auditoría:

- Recomendación: El proceso de cierre del reporte debe requerir una doble verificación de la acción tomada (Auditoría) y una comunicación clara al usuario, permitiéndole apelar la decisión si considera que no se ha resuelto su afectación.
- Para evitar afectaciones: Esto previene la afectación por fallas en el proceso, error humano o la sensación de impunidad. La doble verificación asegura que la acción correctiva haya sido aplicada correctamente "el contenido dañino realmente fue eliminado". El derecho a la apelación mitiga la revictimización al devolverle al usuario el control y la voz si considera que la gestión fue inadecuada.

Conclusion.

En conclusión: estas recomendaciones, tanto para el diseño de protocolos de comunicación como para la gestión de reportes, tiene una importancia crítica que trasciende el desarrollo técnico de la aplicación.

En el campo laboral, esta actividad subraya la transición de un enfoque centrado solo en la funcionalidad a uno basado en la responsabilidad social y la ética del producto. Implementar protocolos de triage con SLA, cifrado de datos sensibles y anonimato auténtico es fundamental para cualquier profesional del diseño UX/UI, seguridad o desarrollo, asegurando que el producto cumpla con estándares legales y minimice el riesgo reputacional.

En la vida cotidiana, la relevancia es aún más profunda. Las aplicaciones de denuncia manejan las experiencias más vulnerables de las personas "acoso, violencia, fraude". Un sistema no revictimizante y con trazabilidad transparente protege directamente el bienestar emocional y la seguridad física del

usuario. Hemos pasado de simplemente recibir un reporte a garantizar una respuesta humana, segura y efectiva, haciendo de la tecnología una herramienta de protección y no una fuente de daño adicional. Esto establece un estándar de confianza esencial en la era digital.

Referencias.

Google. (n.d.). Gemini. Retrieved November 16, 2025, from https://gemini.google.com/