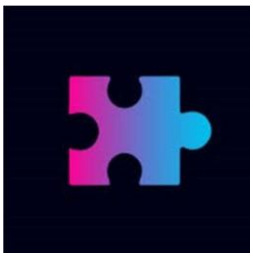

Super App security kit

Vertical: Cybersecurity

Sector de Negocio: Fintech

“Capacitación y Conciencia”

Título:

Capacitación y Conciencia en Ciberseguridad para la Super App Security Kit

1. Función en el proyecto:

“Yo voy a presentar la parte de Capacitación y Conciencia, es decir, cómo vamos a preparar al equipo humano para que la seguridad no dependa solo de la tecnología, sino también de las personas”.

2. Contexto: ¿Por qué necesitamos capacitar?

Super apps fintech = muchos datos sensibles

Errores humanos = causa frecuente de incidentes

Sin cultura de seguridad, cualquier control técnico se puede romper

“Las fintech son un blanco atractivo. Aunque tengamos cifrado, políticas y herramientas, si el equipo cae en un phishing o comparte credenciales, la seguridad se rompe. Por eso en el proyecto diseñamos un programa específico de capacitación y conciencia”.

3. Objetivo general y específicos

Objetivo general:
Crear un programa de capacitación que reduzca el riesgo humano y fortalezca la cultura de seguridad.

Específicos:

Explicar riesgos en super apps.

Enseñar buenas prácticas diarias.

Concientizar sobre phishing e ingeniería social.

Definir cómo reportar incidentes.

“La idea es que cualquier persona del equipo, aunque no sea experta en ciberseguridad, sepa qué hacer y qué no hacer cuando trabaja con datos sensibles”.

4. Público objetivo

Desarrolladores y equipo técnico

Producto y negocio

Soporte al cliente

Líderes y gerentes

“No es un curso solo para el área de TI. Lo planteamos para todo el equipo de la super app: desde desarrollo hasta soporte, porque todos tienen contacto con información sensible o con los usuarios”.

5. Módulos del programa

Introducción a la seguridad en super apps fintech

Gestión de contraseñas y autenticación multifactor

Phishing e ingeniería social

Buenas prácticas diarias y uso seguro de herramientas

(Opcional) Respuesta y reporte de incidentes

“Estructuramos la capacitación en módulos cortos. Empezamos con conceptos básicos, luego credenciales, phishing, buenas prácticas y finalmente cómo responder ante un incidente sospechoso”.

6. Metodología de capacitación

Sesiones breves (1–2 h)

Ejemplos reales y demostraciones

Simulaciones de phishing

Material de apoyo: guía escrita y checklists

“No queremos una capacitación teórica y aburrida. Se usarán ejemplos reales, correos de phishing simulados y una guía práctica para que las personas tengan algo a mano en el día a día”.

7. Concientización continua + métricas

Concientización continua

Tips mensuales de seguridad

Recordatorios visuales (banners, fondos de pantalla)

Mini-quizzes periódicos

Dimétricas

% de participación

Resultados de quizzes

Clics en simulaciones de phishing

Incidentes reportados a tiempo

“La conciencia no se logra con una sola charla. Planteamos acciones continuas y medimos resultados: si las personas dejan de hacer clic en phishing y aumentan los reportes, significa que el programa funciona”.

B) Presentación: “Guía de Concientización de Equipo”

8. ¿Qué es la Guía de Concientización?

Documento práctico para todo el equipo

Reglas claras y simples

Complementa la capacitación

“Además del curso, el proyecto incluye una Guía de Concientización: un documento sencillo que resume qué debe hacer cada persona para trabajar de forma segura”.

9. Contenido principal de la guía

Principios básicos: confidencialidad, integridad, disponibilidad

Buenas prácticas con:

Contraseñas y autenticación

Correo y mensajería

Manejo de datos sensibles

Dispositivos y entorno de trabajo

“La guía traduce los conceptos de seguridad a acciones concretas: cómo crear contraseñas seguras, cómo tratar los datos de los usuarios, qué hacer con los dispositivos de trabajo, etc.”

10. Phishing, incidentes y *checklist*

Phishing e incidentes

*Señales de alerta de ph*ishing

Pasos si recibes algo sospechoso

Qué hacer si crees que hubo un incidente

Checklist personal

¿Uso MFA?

¿Comparto contraseñas?

¿Bloqueo mi pantalla?

¿Sé a quién reportar incidentes?

“Incluimos ejemplos de phishing y un proceso claro de reporte. Al final, un checklist para que cada miembro del equipo pueda evaluarse rápidamente”.

11. Cierre de tu exposición

Diapositiva final: Conclusión

La tecnología sola no es suficiente.

La capacitación y la guía forman la base de la cultura de seguridad.

Un equipo consciente reduce el riesgo y protege la confianza de los usuarios.

“En resumen, nuestra parte del proyecto busca que la seguridad sea un hábito diario del equipo, no solo una herramienta técnica. Si el equipo está bien capacitado y tiene una guía clara, reducimos mucho el riesgo de errores humanos y fortalecemos la confianza

en la super app”.