### 

****

**PLAN DE SEGURIDAD “ANIMATI APP”**

### **(basado en la norma UNE-ISO/IEC 27001:2023 / UNE-EN/IEC 27002:2023)**

**Creadores:**

**Ferace, Luciana**

**Palacio, Lautaro**

**Arevalo, Luciano**

**Burrut, Yasmin**

**Palomeque, Dalila**

**De Nieto, Gabriel**

**Salinas, Juan**

**Samsam, Emir**

**Christiansen, Malvina**

**Rochetti, Uriel**

*Año 2024*

### **1. Objetivo**

#### **Desarrollar un entorno seguro para AnimatiApp, una aplicación móvil de Android que incluye un carrito de compras, pasarela de pagos y un formulario de contacto. Se implementarán políticas de seguridad basadas en buenas prácticas para proteger contra ciberataques comunes, asegurando la integridad, confidencialidad y disponibilidad de los datos del usuario.**

### **2. Contexto de la organización**

**2.1 Comprensión del contexto interno y externo**

Para asegurar la confidencialidad, integridad y disponibilidad de la información en *AnimatiApp*, es fundamental identificar factores internos (capacidades de desarrollo, recursos tecnológicos, y objetivos comerciales) y externos (normativas legales, competidores, y tecnologías emergentes) que puedan afectar el sistema de seguridad de la aplicación. Esto está alineado con el apartado 4.1 de la norma ISO 27001, que exige evaluar el contexto para determinar riesgos y oportunidades clave que afecten la seguridad de la información.

**2.2 Necesidades y expectativas de las partes interesadas**

*AnimatiApp* debe identificar las partes interesadas relevantes como usuarios finales, procesadores de pago, desarrolladores y entidades regulatorias, así como los requisitos de seguridad específicos que estas puedan tener (como la protección de datos personales y transacciones seguras). Según el apartado 4.2, se requiere que se evalúen las expectativas de estas partes, incluyendo obligaciones legales y contractuales, para integrarlas dentro del sistema de gestión de seguridad de la información.

**2.3 Alcance del sistema de gestión de la seguridad de la información**

El sistema de gestión de la seguridad de la información de *AnimatiApp* se aplicará a todas las áreas que involucran el tratamiento de datos sensibles, desde la gestión del carrito de compras hasta la pasarela de pagos. Se abordarán todas las actividades internas y las interfaces con proveedores externos, en línea con el apartado 4.3 de la norma, que establece la necesidad de determinar el alcance basado en factores internos, externos y dependencias.

### **3. Liderazgo**

**3.1 Liderazgo y compromiso**

El Equipo de Desarrollo de *AnimatiApp* debe demostrar un fuerte compromiso con la seguridad de la información, asegurando que los objetivos de seguridad estén alineados con la estrategia de la aplicación y proporcionando los recursos necesarios. Según el apartado 5.1 de la norma, es esencial que los miembros de la organización comuniquen la importancia de una gestión efectiva de la seguridad, promuevan la mejora continua y supervisen que el sistema alcance los resultados previstos.

**3.2 Política de seguridad de la información**

*AnimatiApp* establecerá una política de seguridad de la información adecuada para proteger los datos del usuario y garantizar la confiabilidad de los servicios ofrecidos. Esta política incluirá objetivos claros y medibles, compromisos de cumplimiento normativo, y planes para la mejora continua, tal como exige el apartado 5.2 de la norma. La política será comunicada internamente y estará disponible para las partes interesadas.

**3.3 Roles y responsabilidades**

Se asignarán claramente los roles y responsabilidades relacionadas con la seguridad de la información dentro de *AnimatiApp*. Siguiendo el apartado 5.3, los responsables deberán asegurar que se cumplan los requisitos del sistema de gestión de la seguridad y realizar los reportes pertinentes.

### **4. Planificación**

**4.1 Acciones para abordar riesgos y oportunidades**

El plan de seguridad de *AnimatiApp* incluirá un análisis exhaustivo de los riesgos potenciales, tales como brechas de seguridad en la pasarela de pagos o accesos no autorizados al carrito de compras. Esto será tratado de acuerdo con el apartado 6.1, donde se identifican los riesgos, sus posibles consecuencias, y se diseñan acciones preventivas o de mitigación.

**4.2 Objetivos de seguridad de la información**

*AnimatiApp* establecerá objetivos claros y medibles de seguridad de la información, en coherencia con su política. Estos objetivos estarán enfocados en garantizar transacciones seguras, proteger la privacidad de los usuarios y mantener la integridad del sistema, tal como indica el apartado 6.2 de la norma.

### **5. Operación**

**5.1 Planificación y control operacional**

Se implementarán controles operacionales en todos los procesos críticos de *AnimatiApp*, desde el manejo de datos en el carrito de compras hasta la interacción con proveedores externos, conforme al apartado 8.1 de la norma. El control de cambios será esencial para mitigar cualquier efecto adverso no previsto.

**5.2 Evaluación y tratamiento de riesgos**

*AnimatiApp* llevará a cabo evaluaciones periódicas de los riesgos de seguridad, especialmente cuando se introduzcan cambios significativos en la aplicación. Los resultados de estas evaluaciones serán documentados y se implementarán planes de tratamiento para mitigar los riesgos, siguiendo los apartados 8.2 y 8.3 de la norma.

### **6. Soporte**

**6.1 Recursos y competencia**

La organización deberá proporcionar los recursos necesarios para implementar y mantener el sistema de gestión de seguridad de la información. Además, garantizará que el equipo de desarrollo tenga la formación y competencias adecuadas, tal como se establece en el apartado 7.1 y 7.2.

**6.2 Comunicación y documentación**

Se establecerán procedimientos claros para la comunicación interna y externa sobre la seguridad de la información, así como para la creación y actualización de la información documentada, de acuerdo con los apartados 7.4 y 7.5 de la norma.

### **7. Medidas sobre la prevención de amenazas**

#### **7.1. Autenticación y Autorización**

* **Política**: Uso de **JWT (JSON Web Token)** para gestionar la autenticación de usuarios en la aplicación.
* **Fundamentación**: JWT permite que las solicitudes entre el cliente y el servidor sean verificables de manera segura. Los tokens son firmados por el servidor y permiten que el backend confíe en el usuario autenticado sin necesidad de mantener sesiones en el servidor.
* **Prevención de ataques**: Previene ataques de **fuerza bruta** y **ataques de sesión**, ya que los tokens tienen expiración y se pueden invalidar rápidamente en caso de ser comprometidos.
* **Autenticación multifactor (MFA)**: Implementar una segunda capa de autenticación (por ejemplo, usando un autenticador físico o una app MFA como Google Authenticator), que protege contra ataques de **phishing** y **ataques de contraseña**. **Fundamentación**: La autenticación multifactor dificulta el acceso no autorizado incluso si un atacante ha comprometido la contraseña.

#### **7.2. Protección Contra Malware y Ransomware**

* **Política**: Todos los datos ingresados, tanto en el formulario de contacto como en el carrito de compras, deben ser validados y saneados para evitar la introducción de scripts maliciosos.
* **Prevención de ataques**: Se previene la ejecución de **malware**, **ransomware** y **ataques de inyección SQL**, asegurando que los datos introducidos sean seguros antes de su procesamiento.
* **Medida adicional**: Uso de **antivirus y firewall** en servidores, y revisión periódica de las bibliotecas de terceros utilizadas en el desarrollo de la aplicación.

#### 

#### **7.3. Política de Seguridad en las Comunicaciones**

* **Política**: Todo el tráfico entre la aplicación móvil y el servidor debe estar cifrado mediante **HTTPS** con **TLS 1.2** o superior.
* **Fundamentación**: El uso de HTTPS cifra la información transmitida, lo que previene ataques de **interceptación de datos** como el **Man-in-the-Middle (MitM)**.
* **VPN recomendada para Wi-Fi pública**: Al acceder a la pasarela de pagos desde redes Wi-Fi públicas, se sugiere que los usuarios utilicen una **VPN** para evitar que su información sea interceptada.

#### **7.4. Protección de la Base de Datos**

* **Política**: Implementar el principio de **mínimos privilegios** en el acceso a la base de datos. Solo los usuarios y servicios esenciales deben tener acceso a los datos críticos, como información personal y financiera.
* **Prevención de ataques**: Esta medida protege contra **ataques de inyección SQL** y **amenazas internas**.
* **Medida adicional**: Todas las consultas a la base de datos deben ser **parametrizadas** para prevenir inyecciones de código malicioso.

#### **7.5. Gestión de Contraseñas**

* **Política**: Forzar a los usuarios a crear contraseñas complejas (mínimo 8 caracteres, con combinación de números, símbolos y letras mayúsculas y minúsculas).
* **Prevención de ataques**: Protege contra **ataques de diccionario** y **ataques de fuerza bruta**. Utilizar un generador de contraseñas y no reutilizar contraseñas en distintas plataformas también mitiga riesgos.
* **Fundamentación adicional**: Las contraseñas almacenadas deben estar **hasheadas** utilizando algoritmos seguros como **bcrypt** o **PBKDF2** para evitar su desencriptación en caso de comprometerse la base de datos.

#### **7.6. Protección Contra Phishing**

* **Política**: Instruir a los usuarios para evitar hacer clic en enlaces sospechosos y promover buenas prácticas de seguridad, como verificar la autenticidad de los mensajes de correo o aplicaciones.
* **Prevención de ataques**: Ayuda a evitar ataques de **phishing**, que pueden llevar a la revelación de información sensible, como credenciales.
* **Cultura de ciberseguridad**: Crear conciencia entre los usuarios y el equipo de desarrollo acerca de los riesgos de ataques de ingeniería social.

#### **7.7. Protección de Datos y Copias de Seguridad**

* **Política**: Implementar **cifrado de datos en reposo** en los servidores y realizar **copias de seguridad periódicas** para proteger la integridad de la información en caso de ataques como el **ransomware**.
* **Prevención de ataques**: Protege contra la **pérdida de datos** y garantiza que se pueda restaurar la información comprometida.
* **Medida adicional**: Las copias de seguridad deben almacenarse en ubicaciones seguras (idealmente fuera del entorno de producción) y estar cifradas para evitar robos de información.

#### **7.8. Monitoreo y Respuesta a Incidentes**

* **Política**: Implementar un sistema de monitoreo de tráfico y actividad sospechosa en la red. Además, contar con un **plan de respuesta a incidentes** para actuar rápidamente en caso de un ataque.
* **Prevención de ataques**: El monitoreo en tiempo real permite la detección temprana de ataques como **denegación de servicio (DoS/DDoS)** y posibles intentos de **exfiltración de datos**.
* **Simulaciones de ataques**: Realizar pruebas de seguridad periódicas, como **penetration testing** (simulaciones de ciberataques) para identificar posibles vulnerabilidades y mejorar la preparación del equipo.

### **8. Conclusión:**

Con la implementación de este plan de seguridad, **AnimatiApp** se protege frente a una amplia variedad de ciberataques conocidos, garantizando un entorno seguro para los usuarios y sus datos. Se considera tanto la protección técnica como la concientización del usuario, para minimizar el riesgo de vulnerabilidades y ataques.

Asimismo, se proporciona una base sólida para la implementación de un sistema de gestión de la seguridad de la información, asegurando el cumplimiento con la norma UNE-ISO/IEC 27001:2023 y garantizando la protección de los datos de los usuarios.