### 

### 

### 

### **Políticas de Seguridad**

### **para el Aplicativo**

### **Duoc Swap**

| **Revisión*: [01]*** |
| --- |
| **[27/08/2024]** |

| *Proyecto: Duoc Swap* |
| --- |

**Índice:**

[Políticas de Seguridad](#_95htwn6f8xht)

[para el Aplicativo](#_wfjqt5thug4s)

[Duoc Swap](#_pr58ujacbqrf)

[1. Política de Autenticación](#_dxtvyhm2lrmf)

[1.1. Identificación con dominio institucional](#_619niydr4q8b)

[2. Política de Protección de Datos Personales](#_n46r8diufvju)

[2.1. Encriptación de Datos](#_u89hd6adjowb)

[2.2. Cumplimiento de la Ley de Protección de Datos](#_7sh115s6syud)

[2.3. Retención y Eliminación de Datos](#_ock1oun3t2qi)

[3. Política de Seguridad de Transacciones](#_3tcfk0j3sq26)

[3.1. Monitoreo de Transacciones en Tiempo Real](#_pjy41knx4xfq)

[3.2. Límite de Transacciones](#_abvn2kr511x0)

[3.3. Auditoría de Transacciones](#_ran8gvitrm1h)

[4. Política de Control de Acceso](#_ytw9d667ve6b)

[4.1. Privilegios de Usuario](#_xrgqgmczg190)

[4.2. Registro de Actividad](#_dxdxy0byi9pd)

[5. Política de Protección contra Amenazas](#_lpw1a4agqbf1)

[5.1. Actualizaciones de Seguridad](#_tj4biazedls4)

[6. Política de Respuesta a Incidentes](#_o205785hfvlj)

[6.1. Protocolo de Respuesta a Incidentes](#_a1egi8sntlcz)

[6.2. Notificación a Usuarios](#_j93cguxizblh)

[7. Política de Confidencialidad y Privacidad](#_xsz9lmzevih0)

[7.1. Confidencialidad de la Información](#_mdofpbdlqkxv)

[7.2. Aceptación de Términos y Condiciones](#_ttdj2fudxej9)

[Glosario](#_pz8qckkko9ce)

**Introducción:**

El sistema **Duoc Swap** implementará las siguientes políticas de seguridad para asegurar la protección de los datos de los usuarios, la integridad del sistema y la seguridad de las transacciones dentro de la plataforma. Estas políticas están diseñadas para cumplir con las normativas locales e internacionales sobre seguridad de la información y protección de datos.

### **1. Política de Autenticación**

#### **1.1. Identificación con dominio institucional**

Se autenticarán las cuentas con el dominio del correo institucional de Duoc UC el cual se especifica de la siguiente manera: ***“@duocuc.cl”,*** esto para cumplir con las normas de seguridad de Duoc Swap.

### **2. Política de Protección de Datos Personales**

#### **2.1. Encriptación de Datos**

Toda la información personal y las transacciones de los usuarios estarán encriptadas utilizando algoritmos de encriptación avanzados (AES-256) durante el almacenamiento y la transmisión. Esto asegura que la información no sea accesible a terceros no autorizados.

#### **2.2. Cumplimiento de la Ley de Protección de Datos**

El sistema cumplirá con la legislación chilena de protección de datos (Ley 19.628). Los datos personales de los usuarios serán manejados de acuerdo con las normativas vigentes y sólo se usarán para los fines establecidos por la plataforma.

#### **2.3. Retención y Eliminación de Datos**

Los datos de los usuarios serán retenidos solo por el tiempo necesario para cumplir con los fines del sistema. Los usuarios tendrán la opción de eliminar sus cuentas y todos sus datos asociados permanentemente bajo solicitud.

### 

### 

### 

### **3. Política de Seguridad de Transacciones**

#### **3.1. Monitoreo de Transacciones en Tiempo Real**

Todas las transacciones serán monitoreadas en tiempo real. Cualquier comportamiento sospechoso o transacciones anómalas serán marcadas para revisión automática, y se notificará a los administradores y usuarios implicados.

#### **3.2. Límite de Transacciones**

Se implementarán límites en la cantidad de intercambios diarios y semanales para mitigar el riesgo de fraude. Estos límites podrán ser ajustados por el usuario bajo verificación adicional.

#### **3.3. Auditoría de Transacciones**

Se realizará una auditoría interna periódica de las transacciones para garantizar que se están cumpliendo las políticas de seguridad. Las auditorías externas también serán llevadas a cabo anualmente para garantizar la transparencia.

### **4. Política de Control de Acceso**

#### **4.1. Privilegios de Usuario**

El acceso a diferentes funcionalidades del sistema estará controlado mediante privilegios de usuario. Los usuarios estándar tendrán acceso limitado a las funciones de intercambio y publicación, mientras que los administradores tendrán control sobre la moderación, la gestión de usuarios y la administración del sistema.

#### **4.2. Registro de Actividad**

Cada acción realizada por los usuarios (como iniciar sesión, realizar transacciones o publicar artículos) será registrada en un log de actividad. Estos registros estarán disponibles para los administradores para análisis y auditoría.

### 

### 

### 

### 

### 

### **5. Política de Protección contra Amenazas**

#### **5.1. Actualizaciones de Seguridad**

El sistema se actualizará regularmente para incluir parches de seguridad y proteger contra las vulnerabilidades más recientes. Estas actualizaciones serán automáticas y no requerirán intervención del usuario.

### **6. Política de Respuesta a Incidentes**

#### **6.1. Protocolo de Respuesta a Incidentes**

En caso de que se detecte una violación de seguridad o un incidente, se activará un protocolo de respuesta inmediata. Esto incluirá la contención del incidente, notificación a los usuarios afectados y medidas correctivas para prevenir futuros incidentes.

#### **6.2. Notificación a Usuarios**

Los usuarios serán notificados de inmediato en caso de que su cuenta haya sido comprometida. Se les solicitará que restablezcan su contraseña y revisen sus actividades recientes.

### **7. Política de Confidencialidad y Privacidad**

#### **7.1. Confidencialidad de la Información**

Toda la información recolectada en la plataforma será tratada como confidencial y no será compartida con terceros sin el consentimiento explícito del usuario, a menos que lo exija la ley.

#### **7.2. Aceptación de Términos y Condiciones**

Los usuarios deberán aceptar los términos y condiciones del sistema, los cuales incluyen todas las políticas de seguridad y privacidad. Estos términos estarán disponibles para revisión en cualquier momento dentro de la plataforma.

### 

### 

### 

### 

### **Glosario**

* **Encriptación (AES-256):** Método avanzado de cifrado de datos que utiliza un algoritmo de clave simétrica de 256 bits, garantizando que los datos sean inaccesibles sin la clave correcta.
* **Phishing:** Intento de fraude mediante el cual un atacante se hace pasar por una entidad confiable para obtener información confidencial, como contraseñas o datos de tarjeta de crédito.
* **Log de Actividad:** Registro detallado de todas las acciones realizadas en un sistema, utilizado para auditoría y monitoreo.
* **Monitoreo en Tiempo Real:** Proceso de seguimiento continuo de las actividades dentro de un sistema para detectar anomalías o comportamientos sospechosos.
* **Ley 19.628:** Legislación chilena que regula la protección de la vida privada y los datos personales.
* **Auditoría Interna:** Evaluación realizada dentro de una organización para revisar la efectividad y cumplimiento de sus procedimientos y políticas.
* **Vulnerabilidad:** Fallo o debilidad en un sistema que puede ser explotado por un atacante para comprometer la seguridad.
* **Privilegios de Usuario:** Niveles de acceso que definen qué acciones puede realizar un usuario dentro del sistema, basados en su rol.
* **Protocolo de Respuesta a Incidentes:** Conjunto de procedimientos establecidos que describen cómo reaccionar y manejar una situación de seguridad comprometida.