HUGO SOLUTIONS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Razón Social: HUGO FERNANDO JIMÉNEZ DE JESÚS

Nombre de la Plataforma: HUGOSOFT

Versión: 1.0

Fecha de Emisión: **15-06-2026**

1. OBJETIVO

La presente Política de Seguridad de la Información tiene como objetivo establecer los controles y medidas de seguridad implementados en la plataforma HUGOSOFT, con el propósito de garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información procesada, almacenada y transmitida por el sistema de Facturación Electrónica.

2. ALCANCE

Esta política aplica a todos los procesos, usuarios, servicios, documentos electrónicos, certificados digitales, bases de datos y demás recursos tecnológicos utilizados para la prestación de los servicios de Facturación Electrónica.

3. CONTROL DE ACCESO

a) El acceso al sistema se realiza mediante autenticación por usuario y contraseña.

b) Cada usuario dispone de credenciales únicas e intransferibles.

c) El sistema implementa un esquema de roles y permisos, permitiendo restringir el acceso a funcionalidades y vistas de acuerdo con las responsabilidades asignadas. Los permisos de acceso son asignados bajo el principio de mínimo privilegio, otorgando únicamente los accesos necesarios para el desempeño de las funciones asignadas.

d) El acceso administrativo se encuentra limitado únicamente a los usuarios autorizados.

El personal autorizado que tenga acceso a información confidencial deberá utilizarla únicamente para los fines relacionados con la prestación del servicio y mantener la debida confidencialidad durante el ejercicio de sus funciones.

4. SEGURIDAD DE LA INFORMACIÓN Y BASE DE DATOS

a) La información es almacenada en bases de datos protegidas mediante controles de acceso.

b) Las bases de datos son alojadas en la infraestructura tecnológica de los clientes y su acceso es restringido a personal autorizado.

c) Se implementan medidas de protección para evitar accesos no autorizados a la información.

d) Se aplican medidas para preservar la confidencialidad, integridad y disponibilidad de la información.

5. PROTECCIÓN DE CERTIFICADOS DIGITALES

a) Los certificados digitales utilizados para la firma de los Comprobantes Fiscales Electrónicos son almacenados de manera cifrada.

b) Las contraseñas asociadas a los certificados digitales se almacenan de forma cifrada.

c) El acceso a los certificados digitales se encuentra restringido exclusivamente a los procesos autorizados del sistema.

d) Los certificados digitales únicamente son utilizados durante los procesos autorizados de firma electrónica.

6. SEGURIDAD DE LAS COMUNICACIONES

a) Las comunicaciones entre la plataforma y los servicios externos, incluyendo los servicios de la Dirección General de Impuestos Internos (DGII), se realizan mediante protocolos seguros de comunicación HTTPS con TLS 1.2 o superior..

b) Las credenciales sensibles utilizadas por los servicios son administradas mediante variables de entorno y mecanismos de acceso restringido.

7. SEGURIDAD DE DOCUMENTOS ELECTRÓNICOS

a) Los archivos XML correspondientes a los Comprobantes Fiscales Electrónicos son almacenados en un usuario dedicado del sistema operativo con acceso restringido.

b) Los documentos electrónicos son replicados automáticamente en un almacenamiento externo para fines de disponibilidad y recuperación.

c) Los documentos firmados no son modificados posteriormente.

8. TRAZABILIDAD Y AUDITORÍA

a) El sistema registra los eventos relevantes de seguridad y operación, permitiendo la trazabilidad de las acciones realizadas por los usuarios autorizados.

b) Los registros de auditoría incluyen, entre otros, eventos de autenticación, emisión y anulación de Comprobantes Fiscales Electrónicos, así como las operaciones administrativas efectuadas en el sistema.

c) El sistema mantiene bitácoras de auditoría que registran las operaciones de inserción, actualización y eliminación de información (INSERT, UPDATE y DELETE), indicando el usuario responsable, la fecha y hora de la operación y los datos necesarios para su trazabilidad.

d) Los registros de auditoría son utilizados para fines de seguimiento, control, investigación de incidentes y verificación de la integridad de las operaciones realizadas.

9. PROTECCIÓN DE LA INFRAESTRUCTURA

a) Los equipos y servidores utilizados en la prestación del servicio disponen de mecanismos de protección, incluyendo antivirus y firewall.

b) El acceso a la infraestructura tecnológica se encuentra restringido al personal autorizado.

10. GESTIÓN DE INCIDENTES

Todo incidente de seguridad será registrado, evaluado y tratado de acuerdo con su impacto, implementando las acciones necesarias para restablecer la operación, preservar la integridad de la información y reducir la posibilidad de recurrencia.

11. REVISIÓN Y ACTUALIZACIÓN

La presente política podrá ser revisada y actualizada periódicamente con el fin de adecuarla a nuevas necesidades operativas, tecnológicas o regulatorias.

HUGO FERNANDO JIMÉNEZ DE JESÚS

Representante Responsable

HugoSolutions