1. OBJETIVO, ALCANCE Y USUARIOS

El propósito de esta política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la Seguridad de la información en el servicio de Facturación Electrónica - Factible.

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información SGSI, según se define en el Documento del Alcance del SGSI.

Los usuarios de este documento son todos los empleados de Fenalco Antioquia, que tengan relación con el servicio de Facturación Electrónica - Factible, dentro del alcance de SGSI, así como terceros externos a la organización relacionados con dicho servicio.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del SGSI
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales

3. DEFINICIONES

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo es modificada por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1 OBJETIVO GENERAL

El objetivo general para el sistema de gestión de seguridad de la información es proteger los activos de información que se usan en el servicio de Facturación Electrónica - Factible, buscando crear un marco de confianza para las partes interesadas, controlando la confidencialidad, la integridad y la disponibilidad, gestionando los riesgos, reduciendo los incidentes, capacitando al personal en los conceptos de seguridad de la información y el sistema de gestión de la seguridad, todo enmarcado en un proceso de mejora continua.

4.2 OBJETIVOS ESPECÍFICOS

- Diseñar e implementar controles relacionados con la disponibilidad, confidencialidad e integridad del servicio de Facturación Electrónica - Factible
- Identificar, valorar y controlar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información del servicio de Facturación Electrónica - Factible
- Definir los controles para la gestión de los incidentes de seguridad de la información del servicio de Facturación Electrónica - Factible, para garantizar el mejoramiento continuo del sistema de gestión de la seguridad de la información.
- Establecer mecanismos para incentivar la cultura organizacional al personal de la Federación encargado del servicio de Facturación Electrónica - Factible, en el ámbito de seguridad de la información.

4.3 MEDICIÓN DE LOS OBJETIVOS

El Oficial de Seguridad de la información es el responsable de medir el cumplimiento de los objetivos; la medición se realizará al menos una vez al año y el Oficial de Seguridad de la información analizará y evaluará los resultados y los reportará a la Alta Dirección como material para la revisión por parte de la misma.

Mínimamente evaluará las siguientes medidas que están relacionadas con los objetivos específicos definidos anteriormente.

- Cantidad de controles que fueron diseñados e implementados
- De los riesgos identificados y valorados, cuántos de los riesgos que requieren tratamiento, fueron efectivamente tratados con un control.
- Durante la operación del servicio, se mide la cantidad de incidentes mensuales y las medidas correctivas implementadas asociadas a los mismos.
- Medir la proporción entre la cantidad de empleados involucrados con el servicio de Facturación Electrónica - Factible y los asistentes a las capacitaciones ejecutadas.

4.4 REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos (ver Lista de requisitos legales, jurídicos, contractuales) importantes para Fenalco Antioquia en el ámbito de la seguridad de la información relacionado con el servicio de Facturación Electrónica - Factible.

5. PROCEDIMIENTOS Y POLÍTICAS ESPECÍFICOS

Para poder lograr el objetivo general y los objetivos específicos, es necesario declarar otros procedimientos y políticas que complementen esta política general y apoyen el sistema de gestión de seguridad de la información.

Las últimas versiones de todos estos procedimientos y políticas se pueden encontrar en ISOftware y en las carteleras informativas para su consulta.

5.1 POLÍTICA SOBRE DISPOSITIVOS MÓVILES

El usuario de los equipos de computación y telefonía móvil, debe cumplir con ciertas reglas al llevar su equipo por fuera de las instalaciones de la entidad, en especial en lo que se refiere a:

- El usuario debe procurar no dejar desatendido su equipo de computación y telefonía móvil.
- El usuario debe procurar que su trabajo no sea visible a otras personas que se encuentren en su cercanía.
- El usuario debe procurar por mantener actualizado y con los últimos parches de seguridad su equipo de computación y telefonía móvil.
- El usuario debe procurar por mantener actualizado su antivirus y software de control contra código malicioso.
- El usuario es el responsable de realizar las copias de seguridad de datos.
- El usuario debe verificar que cuando realiza una conexión a un servicio web, éste sea seguro.

5.2 POLÍTICA DE USO ACEPTABLE

La Federación ha definido una política de uso aceptable para los empleados que tengan relación con el servicio de Facturación Electrónica – Factible relacionada con:

- Responsabilidad sobre los activos y el inventario de los mismos.
- Actividades prohibidas.
- Devolución de los activos al finalizar el contrato.
- Procedimiento para copias de seguridad.
- Protección antivirus.
- Autorización para el uso de sistemas de información.
- Responsabilidades sobre la cuenta de usuario.
- Responsabilidades sobre la clave o contraseña.
- Uso de impresoras, escáner y fotocopiadoras.
- Uso de internet.
- Correo electrónico, mensajes de texto y redes sociales.

- Derechos de autor.
- Uso de almacenamientos externos.

Este documento estará disponible para la lectura del usuario o empleado relacionado con el servicio de Facturación Electrónica - Factible, en ISOftware y en las carteras informativas.

5.3 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

La Federación ha establecido una política de escritorio limpio y pantalla limpia, donde los empleados que tengan relación con el servicio de Facturación Electrónica – Factible, deben cumplir con lo siguiente:

- Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como contratos, modelos de confianza, información de los facturadores, entre otros, de acuerdo a su clasificación, deben ser retirados del escritorio o de otros lugares (impresoras, fotocopiadoras, escáner, etc.) para evitar el acceso no autorizado a los mismos. Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo a lo establecido en la Política de Clasificación de la Información.
- Si la persona autorizada no se encuentra en su puesto de trabajo, debe proceder con el bloqueo inmediato de su estación de trabajo, para denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

5.4 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

La Federación ha definido para los empleados que tengan relación con el servicio de Facturación Electrónica – Factible que la información está clasificada en tres niveles, así:

1. Pública: la información está disponible para todo público.
2. Confidencial: la información está disponible para todos los empleados y para algunos terceros seleccionados, por tanto, no se puede compartir con el público en general.
3. Secreta: la información está disponible para algunos empleados específicos, por tanto, no podrán compartirla con alguien más.

La información confidencial y secreta deben estar acompañadas de una marca que identifiquen su clasificación, la demás información, será clasificada automáticamente como pública, tenga o no tenga la marca correspondiente.

Todas las personas que tienen acceso a la información confidencial y secreta, deberán seguir las reglas especificadas en el documento Política de clasificación de la información.

5.5 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

La información de la Federación para los empleados que tengan relación con el servicio de Facturación Electrónica – Factible puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, sistemas de almacenamiento en la nube y sistemas web de transferencia. La forma de transferencia y el uso del cifrado dependerán de la clasificación de cada activo de la información a transferir.

5.6 PROCEDIMIENTO PARA TRABAJO EN ÁREAS SEGURAS

El ingreso de personal a las áreas seguras está restringido, solo los empleados que tengan relación con el servicio de Facturación Electrónica - Factible, se les dará acceso, según se establece en la Política de Control de Acceso. Los visitantes deberán estar acompañados en todo momento por uno de los empleados con acceso.

5.7 PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES

Cada empleado, proveedor o tercero que esté en contacto con activos de información están obligados a reportar todos los incidentes al Oficial de Seguridad de la Información, de la siguiente manera:

ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Reportar posible incidente de seguridad	Reportar el posible evento que afecte el correcto funcionamiento de los sistemas y comunicaciones.	Funcionario / Contratista	Correo Institucional
Registrar incidente de seguridad	El Oficial de Seguridad de la Información realiza el registro del incidente en el formato Apéndice Registro de incidentes S-SI-30	Oficial de Seguridad de la Información	Formato de documentación de incidentes
Identificar el tipo de incidente	Identificar el tipo de incidente, de acuerdo con la tabla de clasificación de incidentes, verificar las evidencias, realizar las pruebas para determinar la veracidad de la incidencia, las causas y el impacto	Oficial de Seguridad de la Información	Formato de documentación de incidentes
Análisis y clasificación	El Oficial de Seguridad de la Información hará su análisis y clasificará el incidente	Oficial de Seguridad de la Información	Formato de documentación de incidentes
Gestionar el incidente de seguridad recibido	Analizar y clasificar el incidente de seguridad tomando como referencia la tabla de clasificación de los incidentes y/o eventos de seguridad, para proceder a realizar las acciones de contención.	Oficial de Seguridad de la Información	Formato de documentación de incidentes
Contener incidente de seguridad	Tomando como base el reporte del incidente de seguridad se procede con la acción inmediata para contener el incidente y determinar el nivel de afectación sobre los activos	Oficial de Seguridad de la Información / Comité de seguridad de la Información	Formato de documentación de incidentes
Erradicar la causa raíz del incidente de seguridad de la información	El comité de seguridad de la información realizara aquellas tareas necesarias con el fin de erradicar la causa raíz detectada. Ejecutar actividades de mitigación y remediación del incidente con el fin de controlar la vulnerabilidad explotada y activando o implementando controles.	Oficial de Seguridad de la Información / Comité de seguridad de la Información	Formato de documentación de incidentes

Recuperar sistemas afectados	Ejecutar actividades de recuperación de sistemas de información o restauración, se debe desplegar el cargue de copias de respaldo actualizada, configuración y/o bases de datos.	Oficial de Seguridad de la Información / Jefatura de Servicios Tecnológicos	Formato de documentación de incidentes
Documentar incidentes de seguridad	Comprueba la eficacia y oportunidad de la solución al incidente de seguridad de la información, se documenta el incidente de seguridad presentado y se procede con el cierre, con indicación del análisis de sitio, fecha, descripción del hecho y cuales fueron las causas, la estrategia de atención, las acciones preventivas, correctivas y conclusiones.	Oficial de Seguridad de la Información / Jefatura de Servicios Tecnológicos	Formato de documentación de incidentes/ Acta de reunión para cierre del comité de SI
Revisión post incidente de seguridad de la información	Realizar revisión de las respuesta y solución dada al incidente de seguridad de acuerdo con los lineamientos establecidos por el comité	Oficial de Seguridad de la Información / Comité de Seguridad de la Información	Formato acta de reunión / Formato de lecciones aprendidas

5.8 OTRAS POLÍTICAS Y PROCEDIMIENTOS

Para garantizar el correcto funcionamiento del sistema de gestión, las siguientes políticas y procedimientos se han definido:

- Procedimientos para la identificación de requisitos
- Política trae tu propio dispositivo
- Política de control de acceso
- Política de claves
- Política del uso de controles criptográficos
- Política de eliminación y destrucción
- Procedimientos operativos para TI y comunicaciones
- Política de gestión del cambio
- Política de creación de copias de seguridad
- Política de desarrollo seguro
- Política de seguridad para proveedores

6. ROLES Y RESPONSABILIDADES

Todo el equipo de Fenalco Antioquia relacionado con el servicio de Facturación Electrónica - Factible es responsable de la seguridad de la información. Adicionalmente existen los siguientes roles y responsabilidades específicas dentro del SGSI.

6.1 Comité de Seguridad

El Comité de Seguridad, es el encargado de:

- Definir la estrategia, el gobierno y la dirección de la gestión de la seguridad de la información.
- Aprobar la política de seguridad de la información.
- Promover la gestión de la seguridad de la información mediante el compromiso de la dirección y la asignación de los recursos adecuados.
- Estudiar y aprobar las iniciativas de seguridad de la información que le sean propuestas.
- Atender los incidentes de seguridad que puedan poner en riesgo el servicio de Facturación Electrónica - Factible.
- Recomendar a la Alta Dirección las sanciones que deberían aplicarse a quien incumpla lo establecido en el Sistema de Gestión de Seguridad de la Información.
- Coordinar la implementación del Modelo de Seguridad y privacidad de la información al interior de la Federación.
- Revisar los diagnósticos del estado de la seguridad de la información en la Federación Nacional de Comerciantes – FENALCO
- Acompañar e impulsar el desarrollo de proyectos de seguridad
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Federación Nacional de Comerciantes – FENALCO
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Revisar los resultados de los análisis de riesgos e identificar los niveles aceptables y el impacto en el negocio
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- Poner en conocimiento de la Federación, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma

6.2 Responsable del funcionamiento del SGSI

El responsable del funcionamiento del SGSI es la Gerencia de Factible. Sus principales responsabilidades son:

- Asegurar la disponibilidad de los recursos necesarios para la definición, la implementación y el mantenimiento del SGSI.
- Revisar periódicamente los documentos y controles del SGSI para asegurar que el SGSI logre los resultados previstos.
- Definir lineamientos que den guía al Oficial de Seguridad de la Información.

6.3 Oficial de seguridad de la información

Sus principales responsabilidades son:

- Coordinar con los propietarios de los activos de información y los dueños de procesos las acciones para el cumplimiento del SGSI.
- Hacer el seguimiento a la implementación y el cumplimiento de los controles de seguridad.
- Apoyar a los funcionarios y contratistas para que cumplan con las responsabilidades de su rol frente al SGSI.

- Liderar el proceso de gestión de incidentes de seguridad de la información.
- Administrar y coordinar el proceso de Seguridad Informática del servicio de Facturación Electrónica - Factible
- Asegurar el buen funcionamiento del proceso de Seguridad de la Información del servicio de Facturación Electrónica – Factible y a su vez ser el punto de referencia para todos los procesos de seguridad relacionados con los procedimientos para la protección de los recursos de software y hardware.
- Guiar al cuerpo directivo y a la administración de la Federación ante incidentes de seguridad mediante un Plan de Respuesta a Incidentes, con el fin de atender rápidamente este tipo de eventualidades.
- El OSI es responsable de proponer y coordinar la realización de un análisis de riesgos formal en seguridad de la información que abarque el servicio de Facturación Electrónica - Factible.
- Es deber del OSI el desarrollo de procedimientos de seguridad detallados que fortalezcan la política de seguridad información.
- Es responsabilidad del OSI promover la creación y actualización de las políticas de seguridad informática, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.
- El OSI debe atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.
- Es responsabilidad del OSI la elaboración de un Plan de Respuesta a Incidentes de Seguridad, con la finalidad de dar una respuesta rápida, que sirva para la investigación del evento y para la corrección del proceso mismo.
- Es responsabilidad del OSI coordinar la realización periódica de auditorías a las prácticas de seguridad de la información, así como, dar seguimiento al corto plazo de las recomendaciones que hayan resultado de cada auditoría.

6.4 Propietario de los activos de información

Es el empleado o contratista que tengan relación con el servicio de Facturación Electrónica – Factible, al cual se le ha asignado la responsabilidad formal sobre un activo de información. Sus principales responsabilidades son:

- Cumplir con la política de seguridad de la información aprobada por el comité de seguridad de la información.
- Identificar, establecer el alcance y el impacto de los activos de información de los cuales es propietario.
- Clasificar los activos de información siguiendo la metodología de identificación y clasificación de activos aprobada por el responsable del funcionamiento del SGSI.
- Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.
- Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.
- Informar los requerimientos y controles requeridos por los activos de información a los custodios y usuarios de los activos de información.
- Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.

6.5 Dueño de procesos

Es el empleado o contratista, al cual se le ha asignado la responsabilidad formal sobre un proceso del servicio de Facturación Electrónica - Factible. Sus principales responsabilidades son:

- Apoyar la identificación de los activos de información que intervienen en el proceso correspondiente.
- Validar los activos de información identificados junto con las características básicas de cada uno de ellos.
- Apoyar y validar la identificación y designación de los propietarios de los activos de información de su proceso.

6.6 Usuario de la información

Es el empleado o contratista que tengan relación con el servicio de Facturación Electrónica – Factible que utiliza la información para desempeñar sus funciones. Sus principales responsabilidades son:

- Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones.
- Conocer la clasificación de los activos de información que maneja.
- Preservar la seguridad de la información utilizada en el desempeño de sus funciones y obligaciones.
- No divulgar la información confidencial y secreta sin autorización del propietario del activo de información.
- Procurar el buen manejo de todos los activos, buscando protegerlos en relación con los principios de seguridad.

7. COMUNICACIÓN DE LA POLÍTICA

El Oficial de Seguridad de la información debe asegurarse de que todos los empleados de Fenalco Antioquia relacionados con el servicio de Facturación Electrónica - Factible, como también los participantes externos correspondientes, estén familiarizados con esta Política. Específicamente para el Sistema de Gestión de Seguridad de la información, se desarrolla un Plan de concienciación y capacitación orientado a los grupos de interés con temas específicos. La última versión de esta Política estará disponible para su lectura en ISOftware y las carteras informativas.

7.1 Matriz de comunicaciones

El Sistema de Gestión de Seguridad de la Información se adapta a la Matriz de Comunicaciones que tiene la Federación Matriz de Comunicaciones A-MC-2.

8. REPORTE DE INCIDENTES Y CONTACTO CON AUTORIDADES

Algunos incidentes de seguridad no solo constituyen un riesgo para la organización, sino que están tipificados como delitos contra la protección de la información y los datos, por el Estado

Colombiano. De ocurrirse cualquiera de estas situaciones, es obligación reportar a las autoridades competentes dicha ocurrencia, así:

DESCRIPCIÓN	ORGANIZACIÓN	CONTACTO
• Acceso abusivo a sistemas informáticos • Violación datos personales • Uso software malicioso • Suplantación sitios web • Transferencia no consentida de activos • Hurto por medios informáticos • Phishing • Ingeniería Social	Centro Cibernético Policial (CCP)	http://www.ccp.gov.co/
Respuesta a emergencias cibernéticas de Colombia	COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	www.colcert.gov.co/
Atención para incidentes de seguridad informática colombiano	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co

9. RENUNCIA A LA INFORMACIÓN PERSONAL

Los empleados de FENALCO ANTIOQUIA, que están relacionados con el servicio de Facturación Electrónica - Factible, renuncian libremente a la propiedad de la información personal que se encuentre almacenada en todos los elementos proporcionados por la Federación para la ejecución de sus labores. Esto incluye todos los documentos electrónicos y físicos almacenados en cualquier medio propiedad de FENALCO ANTIOQUIA.

En todo caso, la Federación será responsable del tratamiento de la información relacionada con datos personales de sus empleados, en los términos que exige la ley.

10. AUTORIZACIÓN PARA LA INVESTIGACIÓN

Los empleados de FENALCO ANTIOQUIA, que están relacionados con el servicio de Facturación Electrónica - Factible, autorizan libremente que los activos de información propiedad de la Federación, a su cargo, sean auditados, monitoreados y analizados sin su consentimiento durante cualquier investigación relacionada con la seguridad de la información.

11. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido hasta el 31 de diciembre de 2020.

El propietario de este documento es el Oficial de Seguridad de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

MODIFICACIONES EFECTUADAS

Versión a Modificar	Modificación que se le efectúa	Revisó	Aprobó
-	Se crea documento	Camilo Torres Velandia Oficial de Seguridad de la Información Fecha: 31/01/2020	Juan Carlos Cardeño Director Administrativo y Financiero Fecha: 07/02/2020
0	Se agrega ítem 7.1 Matriz de comunicaciones	Camilo Torres Velandia Oficial de Seguridad de la Información Fecha: 18/05/2020	Juan Carlos Cardeño Director Administrativo y Financiero Fecha: 26/05/2020