POLÍTICA DE SEGURIDAD Y RIESGO INFORMÁTICO

28 de marzo de 2023

REVISADO POR:	APROBABADO POR:
Mario Gómez Arciniegas – Jefe de Tecnología Informática	Comité estratégico de Tecnología Informática - CETI

POLÍTICA DE SEGURIDAD Y RIESGO INFORMÁTICO

PRESENTACIÓN

Este documento plasma las políticas, objetivos y responsabilidades que soportan las conductas aceptadas por la Federación en el manejo seguro de la información, en el ámbito de la seguridad y riesgo informático.

Cualquier modificación propuesta antes o durante el desarrollo de este Documento, requiere de autorización del Comité Estratégico de Tecnología Informática (CETI).

USUARIOS DE LA POLÍTICA

Este documento de Políticas está dirigido a todas las áreas y colaboradores de Fedepalma y Cenipalma (en adelante La Federación) y a los terceros que sean contratados por éstos.

El documento es propiedad de La Federación; su versión oficial reposa en el Sistema de Gestión de Calidad y en tal virtud es intransferible a cualquier título sin autorización previa de la Oficina de Tecnología Informática. De la misma manera la reproducción de este o entrega a terceros sin autorización de la Oficina de Gestión Organizacional está prohibida. La Federación se reserva los Derechos de Autor.

Toda actualización se deberá efectuar a la primera oportunidad y se deberá registrar en la hoja de registro de revisiones. Las solicitudes de cualquier corrección, aclaración, etc. sobre el documento y su contenido pueden ser dirigidas al correo electrónico jefe.tecnologia@fedepalma.org

1. OBJETIVO DE LAS POLÍTICAS

Establecer las directrices requeridas para la implantación y gestión de un modelo de Seguridad y Riesgo Informático confiable y flexible, también define el marco básico que guiará la implantación de cualquier proceso, procedimiento, estándar y/o acción, relacionado con la Seguridad y Riesgo Informático.

1.1. Objetivos específicos de las políticas

- Establecer los fundamentos para la implantación y el desarrollo del Modelo de Seguridad y Riesgo Informático.

- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos informáticos y activos de información custodiados por TI.

- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.

- Administrar la seguridad informática y los riesgos en TI.

- Establecer los canales de comunicación que le permitan a la alta gerencia mantenerse informada de los riesgos, incidentes y uso inadecuado de los recursos informáticos y activos de información custodiados por TI, así como las acciones tomadas para su mitigación y corrección.

- Proteger la imagen, los intereses y el buen nombre de La Federación.

2. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Acceso: Qué información requiere el rol de los recursos informáticos de la Federación para cumplir con las responsabilidades asignadas por el negocio.

Aceptar riesgo: Es una respuesta al riesgo. En esta respuesta no se emprende ninguna acción que afecte a la probabilidad o el impacto del riesgo; en esta respuesta la entidad está dispuesta a asumir el riesgo y las consecuencias en caso de materializarse.

Activo de información: Es una pieza de información que se recibe o produce en el ejercicio de la función. Un activo de información incluye la información estructurada y no estructurada que se encuentre presente en forma impresa, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo y servidores propios o externos, incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes. Los activos de información tienen las siguientes características:

- Tiene valor para la FEDERACIÓN
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o combinación de estos.
- Es indispensable para la generación de un producto o servicio ofrecido por la FEDERACIÓN

Activo o recurso informático: Cualquier componente tecnológico de carácter físico o lógico involucrado en la prestación de los servicios, pueden ser cualquiera de los siguientes:

- **Información lógica (o electrónica)**: Bases de datos, archivos, contratos y acuerdos, documentación de sistema, información de investigación, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad del negocio, registros de auditoría, e información de archivo (electrónico).

- **Software**: sistemas operativos, aplicaciones, sistemas de información, códigos fuente de aplicaciones, herramientas de desarrollo, herramientas de oficina, herramientas de conectividad a Internet y utilidades.

- **Licenciamiento**: Puede ser físico o digital, en custodia de la Federación, que evidencie el derecho a uso de cualquier producto o servicio tecnológico. Incluye las subscripciones.

- **Hardware**: equipos de cómputo, equipos de comunicaciones, medios removibles, equipos de protección de centros de procesamiento, equipos de protección de acceso a las oficinas, entre otros.

- **Servicios**: servicios computacionales y de comunicación.

Administrador de la información: Individuo a cargo de la recolección, recepción, custodia, uso, procesamiento, tratamiento, almacenamiento, divulgación y determinación de la disposición final de la información de la organización y de sus grupos de interés. Los administradores de los sistemas de información (usuarios líderes) están definidos como administradores de información.

Administrador de los sistemas de información: Individuo a cargo de la definición de las reglas de negocio, evolución del sistema de información, su mantenimiento y operación funcional; así como la administración de los usuarios (creación, eliminación, cambio de perfil y depuración de los usuarios) que ingresan y utilizan el sistema.

Autenticación: Proceso de validación de la identidad del usuario, dispositivo o proceso que intenta acceder al sistema.

Autorización: Proceso de otorgamiento de privilegios para la ejecución de acciones en el sistema.

Colaboradores: Incluye a las personas contratados directa por La Federación.

Compartir riesgo: Es una respuesta al riesgo que busca reducir la probabilidad o el impacto del riesgo compartiendo. Equivale a compartir con un tercero el peso de la pérdida generada por la materialización de un riesgo. Bajo este concepto se utilizan los seguros o procesos tercerizados.

Confiabilidad: Propiedad que determina que la información utilizada para el cumplimiento de las actividades de la Federación brinda la confianza para el logro de su objetivo.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Medida que modifica el riesgo. Los controles incluyen políticas, procedimientos, dispositivos o prácticas que modifican el riesgo (pueden ser tecnológicos, manuales o semiautomáticos).

Cuenta de Servicio: Credenciales de acceso y/o interfaz de comunicación utilizados por los sistemas de información para integrar los diferentes componentes de su arquitectura (base de datos, servicios, otros sistemas de información, etc.) o ejecutar actividades automatizadas.

Disponibilidad: Propiedad que determina que la información sea accesible y utilizable por solicitud de un individuo, entidad o proceso autorizado o en el momento que se requiera.

Ente de seguridad y riesgo informático: Un evento o serie de eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos que la soportan, que tiene(n) una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Es también, el acto de violar, forzar o amenazar con violar alguna política de Seguridad y Riesgo Informático.

Información crítica: Criterio que identifica información indispensable para la realización de un proceso de negocio.

Información privada: Información que pertenece a una persona natural o jurídica, que puede ser sensible y confidencial para el individuo u organización y cuya administración es restringida para los grupos de interés internos y su acceso es denegado para los grupos de interés externos de la Federación, a no ser que cuente con facultad legal o medie solicitud o acción judicial. Esta información solo puede ser administrada con autorización expresa del titular.

Información semiprivada: Información que pertenece a una persona natural o jurídica cuyo conocimiento y divulgación de los datos puede interesar no solamente al titular sino también a la Federación y a otros actores del sector palmero. La información es semiprivada dado que para poder brindar un servicio a los palmicultores se requiere compartir información de identificación, económica, social, ambiental, fitosanitaria, técnica, y de producción de los titulares con otras instituciones y empresas cooperantes, así como con proveedores de servicios especializados. Cuando esta sea la condición, la Federación informará previamente a los titulares para obtener su autorización.

Información pública: Es toda información que la Federación administre, que no tenga ningún tipo de reserva legal y se encuentre disponible para todos los grupos de interés. La información Semiprivada o Privada que es procesada por la Federación y se anonimiza, codifica o agrega podrá tener la condición de información de carácter público, siempre y cuando no se afecten los derechos de los titulares.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los datos independiente del medio en que se encuentren.

Llave de encripción: Secuencia que indica al cifrado cómo encriptar y descifrar la información.

Manual de administración de información de los grupos de interés: Documento que desarrolla los principios, políticas, procedimientos para la administración de la seguridad de la información de la Federación.

Normatividad: Hace referencia al marco legal externo y a las políticas y procedimientos internos para la administración de la seguridad de información y la seguridad informática.

OGRC: Oficina de Gestión de Riesgo Corporativo, encargada de establecer las políticas de control interno y administración de riesgo de la Federación, incluidas las de administración y seguridad de la información de los grupos de interés.

Operaciones TI: Sección de la Oficina de TI, encargada la Gestión de la Seguridad Informática y Riesgos de TI.

Patrocinador de la información: Identifica a un individuo o unidad organizacional que tiene responsabilidad aprobada por parte de la Dirección para delegar la administración de la información y facilitar el cumplimiento de las políticas de seguridad informática y seguridad de la información.

Perfil de riesgos: Nivel de exposición global de riesgo inherente y residual que tiene cada unidad de riesgo elegida.

Perímetro o área segura: Área o agrupación dentro de la cual un conjunto definido de políticas de seguridad y medidas se aplica, para lograr un nivel específico de seguridad. Las áreas o zonas son utilizadas para segmentar requisitos de seguridad y niveles de riesgo similares y de esta forma asegurar que cada zona se separa adecuadamente de las otras.

Principios de seguridad informática: Lineamientos organizacionales para el diseño e implementación de la seguridad informática.

Privilegio: Niveles de acceso a la información. Ejemplo: Consulta, modificación, administración, etc.

Procedimiento: Pasos o acciones operacionales específicas que los individuos deben tomar para lograr las metas definidas en las políticas.

Reducir riesgos: Es una respuesta al riesgo que implica llevar a cabo acciones para reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez.

Riesgo: La posibilidad de que ocurra un evento que tenga impacto negativo sobre el logro de los objetivos.

Riesgo inherente: Es el riesgo que enfrenta una organización en ausencia de respuestas al riesgo y controles.

Riesgo residual: Nivel de riesgo que permanece luego de tomar las respuestas al riesgo e implementar los controles.

Seguridad informática: Medidas de protección que se ejercen contra la divulgación, modificación, hurto o destrucción accidental o intencionada de los recursos informáticos y la información asociada a ellos.

Severidad: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad.

Sistema de información: Sistema dedicado a la entrada de datos, su procesamiento y salida de información bajo unas especificaciones previstas.

Sistema de seguridad de la información: Conjunto de principios, políticas, procedimientos, estándares de seguridad y demás elementos utilizados para brindar protección a los activos de información y evitar el acceso no autorizado accidental o intencional, su modificación, destrucción o publicación.

Terceros: Entidad externa que provee o presta un servicio a La Federación a través de un contrato.

Usuario de la información: Individuo que tiene autoridad limitada y específica otorgada por el administrador de la información para verla, modificarla, adicionarla, divulgarla o eliminarla (mediante los accesos y privilegios asignados). Dentro de este concepto están incluidos los colaboradores directos, temporales, miembros de Junta Directiva, proveedores, contratistas, entes internos y externos de control y empresas que tengan alguna relación comercial o estratégica, y que accedan ya sea interna o externamente, a cualquier activo de información de La Federación.

Usuario líder del sistema de información: Usuario de un sistema de información con conocimientos expertos de su funcionalidad y con amplio conocimiento de los procesos del área en la cual se desempeña. En la mayoría de los casos es el administrador del sistema.

3. GENERALIDADES

3.1. Introducción

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con las tendencias actuales en cuanto a transformación digital, que incluyen aspectos como el Internet de las cosas (IoT), la Inteligencia Artificial (AI) y la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en el ámbito informático.

Puesto que muchas organizaciones gubernamentales y no gubernamentales internacionales desarrollan políticas que norman el uso adecuado de estas destrezas tecnológicas y recomendaciones para aprovechar estas ventajas, es necesario evitar su uso indebido, que puede ocasionar problemas en los bienes y servicios de las entidades.

De esta manera, las políticas de Seguridad & Riesgo Informático de la Federación, emergen como el instrumento para crear conciencia en sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la Federación cumplir con su misión.

Esta política de Seguridad Informática requiere un alto compromiso de la alta dirección de la Federación, agudeza técnica para establecer fallas y deficiencias, y constancia para renovar y actualizar dicha política en función del ambiente dinámico de la realidad actual y futura.

3.2. Aplicabilidad

La Seguridad Informática de la Federación deberá ser administrada de acuerdo con lo definido en el presente documento. Todos los colaboradores y terceros, que accedan a la información de la Federación mediante los recursos informáticos de manera habitual u ocasional en el desarrollo de sus funciones, son responsables de informarse, cumplir y/o hacer cumplir su responsabilidad respecto a los riesgos en su administración. Las Políticas de Seguridad y Riesgo Informático están basadas en las mejores prácticas en la materia y están acordes con las políticas internas y legislación nacional e internacional. Por ende, en caso de incumplimiento en la aplicación de lo definido en este documento, se usarán los mecanismos necesarios, incluyendo las medidas legales aplicables, para proteger sus recursos informáticos y el uso de ellos.

3.3. Principios de la seguridad y riesgo informático

Los principios en los cuales La Federación basa la ejecución de la Seguridad y Riesgo Informático se apoyan en la Seguridad de la Información, y son:

- La información es uno de los activos más importantes de La Federación y por lo tanto se espera que la misma sea utilizada de acuerdo con los requerimientos del negocio.

- La confidencialidad de la información relacionada con el negocio y de los terceros debe ser preservada, independientemente del medio o formato donde se encuentre.

- La información del negocio debe mantener su integridad independientemente de su ubicación temporal o permanente, o la forma en que esta sea transmitida.

- La información del negocio debe estar disponible cuando sea requerida.

3.4. Responsabilidades de la seguridad y riesgo informático

El Comité Estratégico de Tecnología Informática (CETI) es el responsable de aprobar las Políticas de Seguridad y Riesgo Informático.

La Oficina de TI, por intermedio de la Sección de Operaciones TI, es responsable por diseñar, implementar, mantener y comunicar las Políticas de Seguridad y Riesgo Informático y directivas organizacionales relacionadas.

La Oficina de Tecnología Informática debe velar por la seguridad y riesgo informático de los recursos informáticos y activos de información.

La Oficina de Seguridad deberá diseñar, implementar y administrar los controles relacionados con el ambiente físico y adelantar las investigaciones relacionadas con incidentes de seguridad física asociados a los recursos informáticos, los cuales deberán notificarse a la Oficina de Gestión de Riesgo a través del Reporte de Eventos de Riesgo.

La función de auditoría interna debe verificar el cumplimiento de las políticas, procedimientos y cualquier legislación aplicable, en cuanto a la seguridad informática. Los administradores de los sistemas de información, con el apoyo de TI, son responsables por desarrollar, aplicar, mantener y revisar las medidas de seguridad informática, custodiar la información e implementar sistemas de control de acceso para prevenir divulgación no autorizada y acogerse a la estrategia de backup establecida

por la Oficina de TI para asegurar que la información no se pierda. Igualmente, tanto los administradores como los usuarios de información son los responsables de conocer, adoptar y cumplir las Políticas de Seguridad y Riesgo Informático.

La Oficina de Gestión Humana, en conjunto con la Alta Dirección son los responsables de aplicar las acciones disciplinarias en respuesta a las violaciones de las políticas de seguridad y riesgo informático.

3.5. Responsabilidades de la seguridad de la información

La Oficina de Gestión de Riesgo Corporativo, es responsable de diseñar, implementar y comunicar las políticas de control interno y administración de riesgo de la Federación incluidas las de seguridad de la información y las de administración de información de los grupos de interés.

La Oficina de Seguridad deberá diseñar, implementar y administrar los controles relacionados con el ambiente físico y adelantar las investigaciones relacionadas con incidentes de seguridad física asociados a la información, los cuales deberán notificarse a la Oficina de Gestión de Riesgo a través del Reporte de Eventos de Riesgo.

La función de auditoría interna debe verificar el cumplimiento de las políticas, procedimientos y cualquier legislación aplicable, en cuanto a la seguridad de información.

Tanto los administradores como los usuarios de información son los responsables de conocer, adoptar y cumplir con el Manual de Administración de la Información de los Grupos de Interés.

La Oficina de Gestión Humana, en conjunto con la Alta Dirección son los responsables de aplicar las acciones disciplinarias en respuesta a las violaciones del Manual de Administración de la Información de los Grupos de Interés.

3.6. Marco conceptual

La definición de las políticas está alineada con los siguientes estándares internacionalmente aceptados para la práctica de seguridad informática y seguridad de la información:

- NORMA ISO/IEC 17799 – 27001:2013
- NORMA ISO/IEC 17799-2 – 27002:2013

- Estándar COBIT 5: Control Objectives for Information and Related Technology.

3.7. Otras políticas asociadas

- EC-RC-MA-002 - Manual de Política y Lineamientos para la Gestión Integral de Riesgos y Oportunidades
- EC-RC-MA-004 - Manual para la Administración de la Información de los Grupos de Interés de la Federación
- EC-RC-LN-001 - Lineamiento de Protección de Datos Personales – Fedepalma
- EC-RC-LN-002 - Lineamiento de Protección de Datos Personales – Cenipalma
-
- TI-PO-001 - Políticas Corporativas de Prestación de Servicios de Tecnología Informática y Telecomunicaciones

4. POLITICAS DE SEGURIDAD Y RIESGO INFORMÁTICO

4.1. Seguridad y riesgo informático

La información del negocio es un activo vital de la Federación y por lo tanto debe ser protegida.

La información de La Federación sin importar su presentación, medio o formato en el que sea creada o utilizada para el soporte a las actividades de la Federación, se califica como información del negocio o como activo de información.

La Seguridad Informática es el conjunto de medidas de protección que ejerce La Federación contra divulgación, modificación, hurto o destrucción accidental o intencionada de sus recursos informáticos y la información asociada a ellos. Estas medidas de protección se basan en el valor relativo de la información y el riesgo en el que se pueda ver comprometida.

La Federación dispondrá de los medios necesarios para asegurarse de que todos los colaboradores preserven y protejan los activos de información. Cualquier colaborador que intente inhabilitar, vencer, o sobrepasar cualquier control de Seguridad y Riesgo Informático establecido, será sujeto de una acción disciplinaria de acuerdo con lo establecido en el Reglamento interno de Trabajo y el Código de Ética de la Federación.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Protección Homogénea de la información**

La información del negocio de La Federación debe tener un nivel de protección definido de acuerdo con su clasificación y ésta debe mantenerse dentro del nivel de protección sin importar su presentación, medio o formato en el que sea creada o utilizada. Queda prohibido el acceso, transmisión y retransmisión de información para negocios particulares usando los recursos informáticos de la Federación.

- **Desarrollo de tareas de Administración de la Seguridad y Riesgo Informático**

Establecer procedimientos para el desarrollo de las actividades de administración de la seguridad y riesgo informático que obedezcan a estándares de proceso y no al desarrollo de actividades informales.

- **Propiedad de la Administración de Seguridad y Riesgo Informático**

La administración de la seguridad y riesgo informático es una actividad privilegiada y exclusiva de La Oficina de TI y no debe ser ejecutada por personal ajeno a ella o terceras personas sin previa autorización.

4.2. Patrocinador de la información

Cada activo de información en la Federación debe tener un patrocinador que debe ser responsable de su seguridad.

La Federación utiliza información en el desarrollo de su actividad; información que se crea y es entregada a cada responsable de la Federación para que pueda desarrollar y cumplir sus respectivas metas y ejecuciones de proceso dentro del marco del negocio.

La información que La Federación utilice para el desarrollo de sus objetivos de negocio debe tener asignado un Patrocinador, quien la utiliza para el desarrollo de su proceso y es el responsable por su correcto uso. De esta manera él toma las decisiones que son pertinentes para la protección de su información y determina quienes son sus administradores delegados.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Establecimiento formal de los patrocinadores de la información**

La Alta Dirección es la encargada de establecer, asignar, comunicar y formalizar a los Patrocinadores de la información a toda la Federación y éstos debe contar con su

apoyo para dar cumplimiento a las políticas de seguridad informática y seguridad de la información.

- **Obligaciones del patrocinador de información**

Designar un delegado para la administración de la información, así como para facilitar el cumplimiento de las políticas de seguridad informática y seguridad de la información.

4.3. Clasificación de la información

Los encargados de la información deben clasificarla de acuerdo con lo establecido en los lineamientos para la administración de la información de la Federación.

Al igual que otros activos, no toda la información tiene el mismo uso o valor, y por consiguiente requiere diferentes niveles de protección. Ver EC-RC-MA-004 - Manual para la Administración de la Información de los Grupos de Interés de la Federación

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Clasificación de información**

Toda la información, independientemente del medio en el que se encuentre, debe estar clasificada en una de las siguientes categorías:

a. Pública
b. Semi privada
c. Privada

- **Responsable de la información**

Toda la información de la Federación deberá tener un responsable designado quien tendrá la obligación de velar por su confidencialidad, integridad y disponibilidad.

- **Rotulado de medios de información**

Toda información confidencial y de uso interno almacenada en cualquier medio (físico, magnético, portable o impreso), debe ser etiquetada con la clasificación correspondiente. En el caso que la información contenga piezas de distinto tipo, ésta debe etiquetarse con la clasificación más alta de cualquier elemento de información contenida.

- **Recursos informáticos con información de diferentes categorías de clasificación**

Si un recurso informático contiene información con varias categorías de clasificación, los controles usados para su protección deben reflejar la mayor de las categorías que contenga.

- **Divulgación de la clasificación de la Información**

Todos los usuarios de la información deben conocer la clasificación de la información que utilizan para el desarrollo de sus actividades.

- **Protección de información de los grupos de interés**

La información de los grupos de interés debe ser protegida de acuerdo con la clasificación de la información establecida en EC-RC-MA-004 - Manual para la Administración de la Información de los Grupos de Interés de la Federación.

- **Información privada almacenada electrónicamente**

Cuando se vaya a respaldar, trasladar o almacenar externamente información confidencial de manera electrónica, se deberán implementar mecanismos de cifrado o encripción.

- **Información privada almacenada en recursos informáticos**

Se debe propender por evitar tener información confidencial en los discos duros locales de los PC's corporativos o dispositivos de almacenamiento extraíbles. Además de la contraseña de acceso a la red, el PC deberá contar con bloqueo automático de sesión de escritorio por tiempo de inactividad.

- **Intercambio de información privada con entes externos, entes de control y otras entidades**

El intercambio de información privada con entes externos debe hacerse únicamente con la autorización del Administrador de la Información, previa notificación al patrocinador, y con la existencia previa de un acuerdo o términos contractuales de confidencialidad.

- **Acceso a información privada por parte del personal interno de la Federación**

El acceso, transmisión y retransmisión de información que la organización establezca como privada deberá estar limitada al personal designado como responsable de su administración y cualquier solicitud de uso por parte de otra área o proceso deberá ser formalmente aprobada por el Administrador de la Información, previa notificación al patrocinador.

- **Confidencialidad de las llaves de encripción de la información**

Las llaves de encripción de la información son consideradas un recurso informático altamente crítico y están clasificadas como información privada.

- **Mecanismos para incrementar la seguridad de las credenciales de aplicaciones críticas**

Se debe propender porque las credenciales de las aplicaciones de misión crítica de la Federación utilicen para su uso y administración, factores adicionales que incrementen su confidencialidad, integridad y disponibilidad, tales como: clave dual, tiempo definido de expiración, mecanismos de emergencia, autenticación dual, seguridad de almacenamiento, entre otros.

- **Eliminación de información**

Cuando la información de la Federación, por razones de negocio deba ser eliminada, se debe destruir de manera segura, independiente del medio en que se encuentre.

- **Eliminación de información contenida en recursos informáticos que se entregan a terceros**

Cuando un recurso informático va a ser reemplazado, enviado a servicio o dado de baja, la información almacenada en él debe ser eliminada conforme a los métodos establecidos por la Oficina de TI. Cuando el recurso informático contenga información de la Federación que no se encuentra dispuesta en los medios oficiales de almacenamiento, el usuario podrá solicitar la copia de seguridad de información previa a su eliminación.

- **Respaldo de información**

Se deben ejecutar respaldos o backups a la información almacenada en los medios dispuestos por la Oficina de TI para tal fin. Los colaboradores tienen prohibido almacenar la información corporativa en las estaciones de trabajo individuales.

4.4. cumplimiento de regulaciones

La Federación debe cumplir con las regulaciones locales e internacionales de privacidad y seguridad de la información.

Las políticas de Seguridad Informática deben estar acordes y apoyar el cumplimiento de las leyes y regulaciones locales e internacionales relativas a la Seguridad de la Información. Por lo tanto, tales requerimientos deben ser incluidos en el desarrollo del Sistema de Seguridad de la Información y se deben tomar acciones específicas para mantener alineada permanentemente a La Federación con tales disposiciones. Ejemplos de dichas disposiciones son el licenciamiento de software, la legislación o normatividad emitida por el gobierno y la proveniente de estándares internacionales.

Así mismo, y con el fin de mantener un buen nivel de seguridad, esta Política se apoya en las mejores prácticas de Seguridad de la Información como por ejemplo las Normas ISO/IEC 17799 y 27001:2013.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Cumplimiento de normas y disposiciones legales y/o requerimientos de entes de control externo**

Toda reglamentación, regulación o requerimiento emitido por las entidades de control externas, debe estar definida y documentada formalmente por el área encargada o el personal de enlace con dicho ente de control. La Oficina de TI se alineará con dicha documentación y atenderá los requerimientos en consecuencia.

- **Cumplimiento de los derechos de autor**

Deben implantarse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de creaciones que puedan estar sujetas a derechos de propiedad intelectual, tales como derechos de autor y propiedad industrial.

La instalación de software externo en los recursos informáticos tanto de la Federación como de terceros que presten sus servicios a la Federación debe ser previamente autorizada y debe cumplir con los requerimientos legales de derechos de autor que faculten su utilización.

- **Instalación de software autorizado**

El software que reside en los recursos informáticos de la Federación sólo podrá ser el autorizado por la Oficina de TI. No se autorizará la instalación de hardware y/o software personal en las estaciones de trabajo de la Federación.

La autorización del uso de software libre dependerá de que exista una evaluación por parte del área solicitante y de la Oficina de TI para su uso en la Federación, de manera que no genere sub-licenciamiento y no se afecte la confidencialidad, integridad y disponibilidad de la información en los recursos informáticos. Este software debe estar inventariado para su control indicando cantidad, ubicación y responsable.

- **Custodia de medios magnéticos, manuales de instalación y licencias de uso**

Las versiones originales de los medios magnéticos, manuales de instalación y licencias de uso de los recursos informáticos adquiridos por la Federación son custodiadas por la Oficina de TI y no deben ser reemplazadas por copias. Cuando existan, la Federación debe conservar en un lugar seguro y específico para este fin, los originales de los medios, manuales de instalación y licencias de uso de los recursos informáticos adquiridos.

- **Administración del licenciamiento**

El licenciamiento adquirido por la Federación (en cualquiera de sus modalidades) debe ser administrado de forma tal que a solicitud de las autoridades competentes y como parte del informe de gestión se obtenga al menos la siguiente información: nombre del producto, descripción, versión, fabricante, número de licencia (si aplica), ubicación de las mismas, tipo de software, tipo de licencia, licencias instaladas, licencias no instaladas, no. total, de licencias, fecha de vencimiento.

Todas las licencias adquiridas por la Federación deben contar con los respectivos soportes: licencia física o electrónica, factura de compra y/o contrato de adquisición.

- **Software utilizado por terceros**

Los terceros al servicio de la Federación deberán garantizar que el software que utilicen para la prestación de sus servicios esté debidamente licenciado, de acuerdo con la(s) ley(es) de propiedad intelectual vigente(s) y aplicable(s).

La utilización de software de propiedad de la Federación por parte de terceros deberá estar autorizada por el Patrocinador de la Información administrada por dicho software y por la Oficina de TI, en cumplimiento de las disposiciones de derechos de autor, de

seguridad de la información y de seguridad informática y el marco normativo que sea aplicable.

4.5. Administración del riesgo en seguridad de la información

Los riesgos a los que están expuestos los activos de información de la Federación deben ser identificados, evaluados y mitigados acorde con su valor, probabilidad de ocurrencia e impacto en el negocio.

Esta política se ciñe a lo establecido en el EC-RC-MA-004 - Manual para la Administración de la Información de los Grupos de Interés de la Federación

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Análisis de riesgo de los recursos informáticos**

La Oficina de TI debe realizar un análisis de riesgos periódico que permita identificar los recursos informáticos de mayor criticidad y orientar los esfuerzos a proteger dichos recursos.

- **Evaluación de riesgos de seguridad de información**

La Oficina de Gestión de Riesgo será la encargada de evaluar los riesgos de la seguridad de información y en conjunto con la Oficina de TI propondrán medidas de mitigación para los mismos.

- **Seguros con cobertura para los recursos informáticos**

Se deben contratar seguros que cubran los recursos informáticos de la Federación. La gestión de dichas pólizas está a cargo de la Oficina de Servicios Administrativos.

- **Garantía para los recursos informáticos críticos**

Los recursos informáticos de misión crítica deben contar con garantías de hardware y software por parte del fabricante.

4.6. Capacitación y creación de cultura en seguridad informática de la información

La Federación debe establecer un programa permanente de creación de cultura en seguridad informática para los usuarios y terceros.

Con el fin de crear conciencia en sus colaboradores y terceros frente al papel que tiene en el manejo seguro de la información, la Federación debe contar con un programa permanente que permita mantener a los colaboradores informados acerca de las políticas y las responsabilidades asociadas a la seguridad informática, y continuas amenazas que ponen en riesgo la información que administra y/o procesa.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Concientización**

En las jornadas de inducción y re-inducción corporativa, se debe realizar la respectiva concientización que enfatice la importancia del cumplimiento del Modelo de Seguridad Informática y su contribución al logro de los objetivos de la Federación. Este ejercicio permite preparar al colaborador desde su ingreso o cuando inicie su relacionamiento con los Grupos de Interés.

- **Divulgación de los lineamientos de administración de información y sus modificaciones**

La Oficina de Gestión de Riesgo debe implementar el plan de divulgación de los lineamientos de administración de información y sus respectivas modificaciones cuando se presenten. Estos lineamientos dictan las pautas bajo las cuales se alinea la Política de Seguridad Informática.

4.7. Identificación y autenticación individual

Todos los usuarios que acceden a la información de la Federación deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal.

Cada usuario es responsable por sus acciones mientras utiliza cualquier recurso informático de la Federación. Por lo tanto, la identidad de cada usuario que accede a dichos recursos deberá ser establecida y autenticada de una manera única y no podrá ser compartida; tampoco se podrán usar cuentas de otro colaborador o terceros.

Es responsabilidad directa de cada colaborador velar por la confidencialidad y buen uso de su contraseña; en casos excepcionales y previa justificación se podrá solicitar la creación de cuentas de usuario genéricas a la Oficina de TI, siempre estableciendo a un colaborador de la Federación como responsable del uso de la misma.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Control de accesos**

La solicitud de acceso a Sistemas de Información y/o Red de Datos para colaboradores o terceros solo podrá ser realizada a partir del nivel de jefe o líder a la Oficina de Tecnología Informática a través de Helpdesk.

La autorización de accesos a los sistemas de información será función del Administrador del Sistema de Información.

El usuario líder del sistema de información deberá documentar los esquemas de perfiles y privilegios de acceso, así como registrar y mantener vigente la información de personas y privilegios autorizados para acceder al sistema.

Todas las novedades sobre retiros y cambios organizacionales del personal en la Federación deberán ser reportadas oportunamente por la Oficina de Gestión Humana a los Administradores de los Sistemas de Información, red de datos y telefonía, quienes atenderán de manera inmediata dicha novedad para que los privilegios de acceso sobre la información sean consistentes con las funciones asignadas a cada cargo y el estado contractual.

- **Unicidad de cuentas de usuario – identificador de usuario**

Cada colaborador o tercero debe tener asignada una única cuenta de usuario (identificador) para obtener acceso a las plataformas, aplicaciones y sistemas de información que utilice en la Federación.

- **Uso Personalizado de la cuenta (identificador) de usuario**

Los usuarios de los recursos informáticos de la Federación no deben compartir con nadie su cuenta de usuario / contraseña o cualquier mecanismo otorgado para su identificación y autenticación.

La responsabilidad que un usuario de la Federación adquiere al recibir su cuenta de usuario / contraseña o cualquier mecanismo de identificación y autenticación se extiende a todo tipo de interacción que ese identificador tenga con el sistema. En ninguna circunstancia está permitido compartir la contraseña de un sistema de la Federación entre diferentes usuarios; de ser necesario, se podrá solicitar la creación de cuentas de usuario genéricas de asignación individual (pasantes, por ejemplo) a la Oficina de TI, previa justificación de las mismas.

Cualquier acción realizada sobre los recursos informáticos con el medio de identificación suministrado, será responsabilidad del colaborador a quien la Federación le hubiese asignado el mismo.

- **Identificación y autenticación de usuarios y programas**

Para el acceso a cualquier recurso informático de la Federación mediante la red pública o privada se requiere un proceso de identificación y autenticación del usuario o del programa que lo está intentando.

- **Mecanismos de identificación y autenticación**

Todos los recursos informáticos de la Federación deben contar con mecanismos que soliciten la identificación y autenticación al usuario o a los programas que pretendan accederlos y estos serán de uso personal e intransferible; por lo tanto, su uso compartido no es aceptable en ninguna circunstancia.

- **Creación y desactivación de cuentas (identificador) de usuario**

Debe existir un procedimiento formal para la creación y desactivación de cuentas de usuario el cual es definido por el Usuario Líder del Sistema de Información o quien haga sus veces. Se debe contar con herramientas o mecanismos que permitan salvaguardar la información de los usuarios desactivados, manteniendo la información histórica de los mismos, almacenada en los medios oficiales suministrados por la oficina de TI.

- **Inhabilitación de usuarios**

Se requiere disponer de mecanismos para inhabilitar el acceso a los usuarios cuando:

a) estos se ausenten o no hayan accedido a los recursos informáticos por un período largo de tiempo,

b) hayan presentado un número determinado de intentos fallidos durante el ingreso de la contraseña,

c) el encargado de la información explícitamente así lo indique, o

d) cuando se detecten hallazgos por parte de los proveedores de aseguramiento

Durante las ausencias por vacaciones o licencias temporales autorizadas por la Federación, los usuarios de las personas ausentes no podrán utilizarse. De presentarse la necesidad de acceso en este período por parte de un usuario, se debe tramitar la solicitud de excepción a través de la Oficina de Gestión Humana.

- **Creación de Contraseñas**

Todas las contraseñas deben ser creadas de acuerdo con el estándar establecido por la Oficina de TI de la Federación para tal fin. Se debe considerar el uso de herramientas automáticas que aseguren el cumplimiento del estándar de creación de contraseñas. Este estándar debe basarse en la construcción de contraseñas fuertes para evitar la fácil identificación de la misma.

- **Asignación de Contraseñas**

La asignación de contraseñas debe ser controlada por un proceso de administración formal que permita asegurar que los usuarios acaten los estándares y recomendaciones para la elección y el cambio de contraseñas.

- **Vigencia de Contraseñas**

Las contraseñas usadas para acceder a los recursos informáticos de la Federación deberán ser cambiadas periódicamente. La contraseña vencerá automáticamente después de transcurrida una vigencia máxima.

Un usuario con contraseña vencida requiere ingresar una nueva contraseña para acceder a los recursos informáticos. El usuario debe ser informado previamente al vencimiento de su contraseña.

Se debe llevar un registro histórico de las últimas contraseñas para evitar que las mismas sean repetidas después de un cierto número de cambios.

Las cuentas de usuario definidas como de “servicio” por su naturaleza deberán estar documentadas, su contraseña no tendrá vigencia.

- **Cambio de contraseñas**

Debe existir un procedimiento para cambio de contraseña de los usuarios. El procedimiento de cambio de contraseña debe ser ejecutado en forma automática cuando un usuario acceda a los recursos informáticos por primera vez, cuando la vigencia de la contraseña haya expirado o cuando la contraseña haya sido reinicializada.

Este procedimiento también estará disponible para que pueda ser realizado manualmente por el usuario cuando lo estime conveniente.

- **Confidencialidad de la contraseña**

Las contraseñas o cualquier otro método de autenticación deben mantener el nivel de información confidencial. Las contraseñas o cualquier otro mecanismo de autenticación deben ser entregadas de forma personal y/o a través de un medio que asegure su confidencialidad.

- **Encripción de contraseñas**

Las contraseñas de acceso deben ser almacenadas por medio de un algoritmo de encripción reconocido por la industria y no deben ser susceptibles de ser desencriptadas. Las contraseñas nunca deben ser almacenadas en formato texto. Durante el transporte de las contraseñas a través de medios de comunicación estas deberán viajar cifradas (mediante la utilización de mecanismos de encripción) o contar con elementos que garanticen la confidencialidad e integridad de la misma.

- **Bloqueo de contraseñas**

La identificación del usuario será inhabilitada si éste falla durante un número limitado de intentos al ingresar la correspondiente contraseña.

- **Acceso a recursos informáticos mediante el uso de una sesión desatendida.**

Los usuarios deben acceder a los recursos informáticos mediante una sesión iniciada utilizando su propia cuenta de usuario y contraseña. Un usuario no debe usar una sesión de trabajo iniciada por otro usuario.

- **Cuentas de usuarios por defecto**

A todas las cuentas de usuario que vienen por defecto con los sistemas operativos, bases de datos y productos de las diferentes plataformas de la Federación se les debe restringir el acceso o tomar las medidas del caso para que no tengan contraseñas débiles y no se conserven las establecidas por el fabricante.

- **Usuarios privilegiados**

La asignación de privilegios de acceso a la información de la Federación debe ser controlada mediante un proceso formal de autorización del Patrocinador de la Información. En general los usuarios con privilegios especiales deben usar métodos de acceso y comunicación seguros que autentiquen de manera fuerte al usuario y que garanticen la confidencialidad del acceso.

- **Prohibición a la suplantación de usuarios**

Está prohibida la suplantación, el enmascaramiento o la firma por otros usuarios de cualquier sistema de información de la Federación.

Los usuarios deben usar siempre su cuenta de usuario para acceder a los recursos informáticos de la Federación, incluso si deben hacerlo desde una estación diferente a la asignada.

4.8. CONTROL Y ADMINISTRACIÓN DEL ACCESO DE LA INFORMACIÓN

El uso de la información presente en los sistemas y archivos digitales de la federación debe ser controlado para prevenir accesos no autorizados. los privilegios sobre la información deben ser mantenidos en concordancia con las necesidades del negocio, limitando el acceso solamente a lo que es requerido.

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información de acuerdo con su clasificación se mantengan protegidos de una manera consistente con su valor para el negocio y de acuerdo con los riesgos de pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Acceso a la información**

Los controles de acceso a la información deben ser los definidos y documentados por el Propietario de la Información y deben estar basados en requerimientos específicos del negocio, quien además debe en conjunto con el Administrador del Sistema de Información mantener vigente la información de personas y privilegios autorizados para acceder al sistema.

- **Controles de acceso lógico**

Con el objeto de prevenir el acceso no autorizado a la información contenida en los recursos informáticos de la Federación, se deben establecer controles de acceso lógico que permitan acceso únicamente a los usuarios autorizados. Los recursos informáticos deben:

a) Controlar los accesos de usuarios a los datos, conforme a la clasificación de la información definida por la Federación.

b) Proveer la protección contra el acceso no autorizado a cualquiera de las herramientas del software operativo o de soporte de los aplicativos que sea capaz de modificar los parámetros del sistema o de la aplicación.

c) Evitar comprometer la seguridad de recursos informáticos que sean compartidos con otras aplicaciones.

- **Definición de perfiles acordes al rol**

Se deben crear perfiles de acceso asociados a roles que tienen responsabilidades y cumplen con actividades comunes; estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios.

- **Definición de perfiles de usuario**

Los permisos de acceso a los aplicativos de la Federación deben ser garantizados de manera preferente a grupos de usuarios y no a individuos. Se deben otorgar permisos de acceso a los recursos informáticos en función de grupos. Estos grupos deben ser conformados por individuos cuyo rol, responsabilidad y actividades sean equivalentes. Cada grupo debe ser asociado a un perfil de acceso autorizado por el Propietario de la Información y los usuarios a quienes sea asignado un mismo perfil contarán con los mismos privilegios.

- **Asignación de accesos basados en los perfiles de usuario aprobados**

Los Administradores de Sistemas de Información deben asignar a los usuarios los privilegios de acceso a la información con base en los perfiles de usuario aprobados por el Propietario de la Información y no basados en requerimientos individuales. Se deben realizar revisiones periódicas de los privilegios asignados a los usuarios.

- **Solicitud de accesos a sistemas de información o red de datos**

La solicitud de acceso a Sistemas de Información y/o red de Datos para colaboradores o terceros solo podrá ser realizada como mínimo por un Jefe de Oficina o persona de cargo similar o superior. La aprobación de la solicitud de usuarios de los Sistemas de información solo podrá ser realizada por el Administrador o Usuario Líder de cada sistema.

- **Perfiles de Auditoría**

Siempre que el sistema/herramienta lo ofrezca, se debe contar con perfiles especiales para ser usados por la función de auditoría. Los auditores deben tener privilegios para

ver la información del negocio acorde con su clasificación y no puedan realizar ningún tipo de modificación. Los accesos a través de estos perfiles deben tener un carácter temporal cuya vigencia debe definir el Propietario de la Información de acuerdo con la actividad de auditoría realizada.

- **Novedades de estado contractual de colaboradores**

Todas las novedades sobre retiros y cambios del personal en la organización deberán ser reportadas inmediatamente a los Administradores de los Sistemas de Información para que los privilegios de acceso sobre la información sean consistentes con las funciones asignadas a cada cargo y el estado contractual del colaborador correspondiente, tomando las acciones necesarias.

- **Actualización de los privilegios de acceso a la información**

Se deben deshabilitar o actualizar los privilegios de acceso a los recursos informáticos inmediatamente se presente la novedad correspondiente o cuando se genere un cambio de privilegios en un rol o perfil.

Cuando un colaborador o un usuario externo deja la organización o cambia de cargo, los Administradores de los Sistemas de Información respectivos deben validar, eliminar o reasignar sus privilegios de acceso a los recursos informáticos de la Federación de manera inmediata, de acuerdo con la novedad y atendiendo los requerimientos para el desarrollo de la nueva función.

- **Manejo centralizado de privilegios**

Los privilegios de los usuarios de los recursos informáticos deben ser manejados y controlados centralizadamente por los Usuarios líderes o Administradores de los Sistemas de Información.

- **Verificación del nivel de acceso real de los usuarios**

El Usuario Líder del Sistema de Información debe realizar una comparación periódica entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que realmente cuentan, y verificar que los usuarios que efectivamente acceden a la información corresponden a los autorizados previamente por él, reflejando una adecuada segregación de funciones; en caso de no hallar concordancia, deberá realizar el correspondiente ajuste.

- **Restricciones de acceso a la información**

El acceso a los recursos informáticos de la Federación y sus datos debe ser otorgado de acuerdo con el Manual de Administración de Información de Grupos de Interés. El acceso a la información debe estar basado en los requerimientos individuales de cada aplicación y otorgando los menores privilegios posibles.

La aplicación de los siguientes controles debe ser considerada para soportar los requerimientos de acceso:

a) Proporcionar menús para controlar el acceso de los usuarios a las funciones de los aplicativos.

b) Restringir la divulgación de datos o funciones de los recursos informáticos que los usuarios no están autorizados a acceder.

c) Controlar las capacidades de acceso de los usuarios mediante el uso de perfiles y/o grupos de perfiles.

d) Asegurar que las salidas de los aplicativos que manejan datos confidenciales contengan únicamente los que son relevantes para el uso de la salida y se envíen exclusivamente a los usuarios y/o equipos autorizados.

- **Restricción de accesos del personal a los diferentes ambientes informáticos**

En la medida en que la planta de empleados lo permita y la segregación de funciones sea posible, el personal que realiza funciones asociadas a un ambiente específico (desarrollo, pruebas y producción) debe contar con perfiles de acceso que limiten sus actividades exclusivamente al ambiente en el que trabajan. El personal de desarrollo no debe tener acceso al ambiente de pruebas y por ningún motivo al ambiente de producción. De igual manera, el personal que realiza pruebas sólo debe tener acceso a los ambientes de pruebas. Por otra parte, los usuarios por ningún motivo deben tener acceso a programas fuente, a utilitarios propios del ambiente de desarrollo ni a líneas de comando que puedan colocar en riesgo los activos de información de la Federación.

- **Acceso a los datos de producción sólo a través de aplicativos**

Los aplicativos deben ser el único vehículo para acceder a los datos de producción de la organización. Se deben utilizar los aplicativos de la organización siempre que se quiera acceder a los activos críticos de información. En esta categoría deben entenderse incluidas las interfaces autorizadas por el Propietario de la Información que estén construidas a partir de herramientas de integración de aplicativos. En caso de

requerirse un acceso a los datos, diferente al existente en el aplicativo oficial, se debe justificar y autorizar por parte del Propietario de la Información, informando a la Oficina de GR y contando con el apoyo de la Oficina TI.

- **Usuarios funcionales administradores**

Los usuarios privilegiados de los recursos informáticos deben ser los autorizados por el Propietario de la Información. Los usuarios funcionales, privilegiados como administradores del sistema o de bases de datos de la organización, deben ser los que el Propietario de la Información ha dispuesto y/o autorizado para tal fin. Desde el punto de vista técnico, la Oficina de TI es la administradora de las bases de datos organizacionales, que son alimentadas por los sistemas de información de la Federación.

- **Usuarios de emergencia y/o encargos**

Cada usuario líder de sistema de información debe establecer un programa de administración de usuarios de emergencia o encargos, para aplicarlo en el momento en que los titulares de los roles se encuentren ausentes, para garantizar la continuidad de las funciones que se surten en cada sistema. Estas asignaciones deben quedar registradas y ser trazables por medio de un mecanismo administrado por el Usuario Líder.

- **Usuarios para procesos especiales o automáticos (cuentas de "servicio")**

Para la ejecución de procesos especiales o automáticos se deberán usar códigos / nombres de usuario especiales cuya utilización será únicamente para la ejecución de dichos procesos, reconociéndose estas cuentas de usuario como cuentas de servicio con características particulares que les permita garantizar el correcto funcionamiento de los procesos mencionados. La Oficina de TI debe asegurar la confidencialidad y custodia de estas credenciales.

- **Restricción en el uso de utilitarios / herramientas**

El conocimiento y utilización de utilitarios/ herramientas fuera del catálogo de software base, debe ser restringido a usuarios privilegiados que por su rol requieran su aplicación. En cualquier caso, su uso debe ser avalado por TI.

4.9. Seguridad informática en los procesos de administración de sistemas

Las áreas que participan en los procesos de la administración de sistemas de la federación son soporte en el modelo de seguridad informática.

Procedimientos y responsabilidades en seguridad informática deben ser incluidos dentro de cada uno los procesos de administración de sistemas de la Federación, para lograr el cumplimiento del sistema de seguridad y riesgo informático. Las áreas que hacen parte de la administración de sistemas deben crear y mantener una metodología que controle el ciclo completo de seguridad en el desarrollo y mantenimiento de sistemas e infraestructura tecnológica.

Los requerimientos de seguridad de la información deben ser identificados previo al diseño de los sistemas de tecnología de la información. Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas y si una modificación es requerida, ésta debe cumplir estrictamente con los requerimientos de seguridad informática que han sido previamente establecidos. El nivel de seguridad de la información de un sistema no puede verse disminuido, por lo que la información y los sistemas productivos no deberán ser utilizados para desarrollo, prueba o mantenimiento de aplicaciones.

La implantación de un sistema nuevo o cambio significativo a los existentes debe estar alineada a las Políticas de Seguridad de la Información y de Seguridad y Riesgo Informático.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Introducción de nuevos recursos informáticos a la Federación**

Se deben configurar los parámetros de seguridad a todo nuevo recurso informático que se implante en la Federación, de acuerdo con la normatividad establecida. No se pueden implementar nuevos componentes tecnológicos sin que previamente se incluyan todas las medidas de seguridad requeridas. Para ello se deben implantar las facilidades disponibles en el equipo, en cuanto a seguridad se refiere y adaptarlas en función de los procedimientos y los estándares definidos. Cualquier cambio a la plataforma tecnológica debe ser aprobado a través del procedimiento de control de cambios de TI (Change Advisory Board - CAB), establecido en la Políticas de Prestación y Uso de los Servicios de TI.

- **Estándares de plataforma**

Se debe definir un estándar de configuración de opciones y parámetros por plataforma que considere los requerimientos de operación segura para los recursos informáticos de la Federación.

- **Implantación de estándares de plataforma**

Todo recurso informático de la Federación debe ser configurado de acuerdo con el estándar establecido para la correspondiente plataforma.

- **Adquisición y mantenimiento de software aplicativo**

La adquisición y mantenimiento del software debe incluir los controles de seguridad informática que garanticen que cumpla las políticas y lineamientos de seguridad de la información de la Federación.

- **Actividades de desarrollo y mantenimiento de software por personal interno o terceros**

Los desarrollos y actividades de mantenimiento de software realizadas por personal interno o por terceros deben cumplir las políticas, procedimientos y estándares de desarrollo de software establecidos por la Federación. La Oficina de TI, debe asegurarse de que todas las actividades de desarrollo de software realizadas por personal interno o terceros cumplen las convenciones de desarrollo de software establecido por la Federación.

- **Actualización de sistemas de información**

Todos los terceros que desarrollen y/o suministren sistemas de información para la Federación tendrán la obligación de suministrar periódicamente actualizaciones para sus sistemas con el fin de garantizar su seguridad y disponibilidad de acuerdo con lo establecido en las obligaciones contractuales que deben cubrir este aspecto.

- **Desarrollo de aplicaciones seguras**

Los requerimientos de seguridad de la información deben ser cumplidos durante todo el ciclo de desarrollo y mantenimiento de software, y éstos deben ser integrados desde el principio como parte de la solución.

- **Liberación de nuevos desarrollos**

La puesta en producción de nuevos desarrollos o modificación de aplicativos es permitida únicamente si estos cuentan con la seguridad mínima establecida en las políticas, procedimientos, lineamientos y estándares de seguridad para el desarrollo de aplicaciones y la formalización de dicha implementación a través del Comité de Cambios. La implantación de nuevos aplicativos que no contemplen los mecanismos mínimos de seguridad sólo se puede realizar mediante un proceso formal de

excepción, a través de la aceptación formal del riesgo por parte del Propietario de la Información, siempre y cuando los niveles de riesgo se encuentren dentro del apetito de riesgo definido por las Juntas Directivas de Fedepalma y Cenipalma, caso en el cual se debe formalizar dicha implementación a través del Comité de Cambios.

En caso de que el Comité de Cambios identifique una situación asociada a nuevos desarrollos que involucre un nivel de riesgo superior al apetito de riesgo, deberá ser reportado a la Oficina de Gestión de Riesgo.

- **Documentación del software**

Toda adquisición, desarrollo o modificación de software debe incluir el suministro o actualización de la documentación técnica correspondiente del producto. Es responsabilidad de TI contar con dicha documentación al amparo del proceso formal de cambios.

- **Separación de ambientes**

Los ambientes de desarrollo, pruebas y producción de los recursos informáticos de la Federación deben estar separados lógicamente. Se deben definir controles necesarios para garantizar esta separación de ambientes.

- **Información de producción en desarrollo o pruebas**

Para resguardar su confidencialidad a efecto de no vulnerar las condiciones de seguridad de acuerdo con su clasificación, la información que está en producción no debe ser utilizada para desarrollo o pruebas, o de ser necesario dicha información deberá ser sometida a un proceso de despersonalización (mezcla de datos) previo a su utilización en ambientes distintos al de producción.

- **Paso de aplicativos a producción**

Los sistemas aplicativos de la Federación deben haber pasado por un proceso completo de pruebas y validación antes de ser liberados a producción en un ambiente dedicado para tal fin. Cualquier paso de aplicativos a producción debe ser aprobado a través del procedimiento de control de cambios, así mismo se debe mantener un control de versiones sobre el mismo.

- **Actualización simultánea de registros**

Debe existir protección contra la actualización simultánea de un registro buscando que se mantenga la integridad de los datos. Durante la actualización de archivos o bases

de datos, el registro afectado debe ser protegido para que ningún otro programa lo modifique.

- **Integridad referencial en bases de datos**

Todos los modelos de datos deben manejar integridad referencial para asegurar que cualquier cambio en un dato sea integrado en todo el modelo de datos en forma automática.

- **Mecanismos para la preservación de la integridad en los aplicativos**

Las aplicaciones por sí solas deben asegurar que la información que se procesa mantenga su integridad. En el diseño de aplicaciones se debe considerar la existencia de validaciones para el ingreso correcto de la información, mecanismos de verificación que aseguren su correcto procesamiento, especialmente cuando se realizan cálculos y alertas que comuniquen desviaciones críticas o de alto impacto.

- **Confiabilidad de los datos**

Todos los Usuarios de Sistemas de Información de la organización serán responsables por la validez y veracidad de la información que ingresan en los mismos.

- **Divulgación de información sobre recursos informáticos**

No se podrá dar información sobre los recursos informáticos como respuesta a encuestas por cualquier medio no autorizado y publicado expresamente por TI. La solicitud de esta información se debe hacer por medios formales y autorizados protegiendo esta información con acuerdos de confidencialidad cuando se requiera.

4.10. Terceros que acceden a sistemas de la federación local o remotamente

Los terceros que utilizan local o remotamente sistemas de información de la federación deben cumplir con la política de seguridad informática.

El uso y acceso local o remoto a los sistemas de información de la Federación por terceros y empresas relacionadas, debe ser formalizado por medio de acuerdos que hagan obligatorio el cumplimiento de la presente Política. Estos terceros deben surtir la respectiva validación y aprobación de las áreas encargadas por la Federación, que se realiza en el proceso de Adquisición de Bienes y Servicios.

Cada relación con un tercero o empresa relacionada de la Federación debe tener un representante o supervisor de contrato dentro de la Federación, que vele por el

correcto uso y la protección adecuada de la información del negocio de acuerdo con su clasificación. Éste será responsable por las actividades realizadas o servicios prestados por el tercero de durante la vigencia del contrato.

En caso de ser necesario para el desarrollo del objeto contratado, los terceros deberán adherirse a las normas de seguridad emitidas por los entes regulatorios con los que interactúa La Federación.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Acuerdos de cuidado de la información con entes externos**

En el contrato de servicios se debe incluir un acuerdo o cláusula de confidencialidad alineadas con el Manual de Administración de Información de los Grupos de Interés de la Federación, que detalle sus compromisos en el cuidado de la misma y las penas a que estarían sujetos en caso de incumplirlos.

- **Inclusión de cláusulas de seguridad de la información en contratos con entes externos**

Se deben incluir cláusulas de seguridad de información en los contratos firmados con entes externos relacionados con los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información.

- **Control de acceso a terceros**

El acceso de entes externos a los servicios informáticos de la Federación y sus datos debe ser otorgado de acuerdo con las políticas internas para acceso a la información y debe contemplar las siguientes condiciones:

a) Está basado en los requerimientos específicos del Propietario de la Información.

b) Evaluar los requisitos legales previos a la realización de cualquier autorización de acceso al tercero.

c) Tener identificado claramente a los terceros mediante la asignación de códigos / nombres de usuario únicos para el acceso a los recursos informáticos.

d) Asignar los perfiles siguiendo un proceso específico de autorización de acceso a los recursos requeridos y sustentar una necesidad legítima del negocio.

e) Definir una lista de individuos autorizados para la utilización de los servicios con los respectivos privilegios y derechos con respecto a cada uso, cuando surja la necesidad.

f) Establecer el acceso a información estrictamente necesaria para el cumplimiento del servicio por parte del tercero.

g) Implementar los procedimientos de supervisión y control de las actividades del tercero, por parte del área responsable de éste.

h) Validar los recursos informáticos empleados por el tercero en el suministro del servicio a la Federación.

i) Socializar con los terceros las Políticas de Prestación y Uso de los Servicios de Tecnología Informática y Telecomunicaciones, además de las políticas descritas en el presente documento dejando constancia de lo anterior en la respectiva acta de compromiso.

j) Establecer un tiempo finito de vigencia del usuario y perfiles asignados al tercero.

- **Información de infraestructura tecnológica.**

No se podrá dar información sobre la infraestructura tecnológica como respuesta a encuestas por cualquier medio no autorizado y publicado expresamente. La solicitud de esta información se debe hacer por medios formales y autorizados protegiendo esta información con acuerdos de confidencialidad cuando se requiera.

4.11. Recuperación de TI.

Todos los recursos informáticos y los procesos asociados deben contar con un plan de continuidad de ti y estar preparados para los ataques contra la seguridad de la información de estos.

La información debe estar disponible para su uso autorizado cuando la Federación la requiera en la ejecución de sus tareas regulares. En caso de que los activos de información críticos en custodia de TI sufran alguna situación que lleve a la falla en su disponibilidad, se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo, sin disminuir los niveles de seguridad establecidos.

La Federación, por intermedio de la Oficina de TI, establecerá medidas de reacción inmediata que permitan detectar y mitigar los efectos de ataques contra la seguridad

informática como son los de denegación de servicios, ingreso de código no autorizado o ataques de fuerza bruta. Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informada a la Federación de la existencia de estas amenazas, detectar los ataques de manera oportuna y ejecutar las acciones consiguientes.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Plan de recuperación de desastres TI**

La Federación deberá garantizar la existencia de un plan de recuperación de desastres de TI, incluido un servicio de contingencia alterno, sobre los recursos informáticos críticos del negocio y la operación que garantice la continuidad de los procesos de la Federación ante eventos catastróficos.

- **Respaldo de información crítica**

Las copias de respaldo de la información crítica de la Federación deben ser realizadas en forma periódica de modo que se garantice su disponibilidad. Se deberá definir la periodicidad de la ejecución de los procesos de respaldo de la información crítica de la Federación. Esta periodicidad se debe adherir a las mejores prácticas de la industria.

- **Custodia de los medios de respaldo de la información de misión crítica**

Los medios de respaldo de la información de misión crítica de la Federación se deben almacenar en localidades alternas y seguras.

- **Pruebas de restauración de información crítica**

Se deben realizar pruebas periódicas de los medios que contienen copias de respaldo de información crítica que incluyan la restauración y verificación de la información. La solicitud de restauración de la información solo podrá ser realizada por el Propietario de la misma o por aquel que él designe.

- **Control de código malicioso y virus informáticos**

Debe existir protección contra código malicioso, a nivel institucional, en los equipos de la Federación. Esta debe contemplar:

a) El acceso y uso de repositorios de software (File Server) y recursos informáticos de producción que limite el acceso a los sistemas y programas, y el uso de las funciones en los sistemas para disminuir el riesgo de las infecciones por virus.

b) La detección de infecciones por virus, malware, phishing, spam, etc. con el empleo regular de software y hardware apropiado que mantenga el registro, lleve estadísticas, verifique cambios a objetos ejecutables y permanezca alerta ante sucesos inesperados.

c) La actualización permanente del software y hardware elegido por la Oficina de TI para salvaguardar los recursos informáticos de la Federación.

- **Erradicación de código malicioso por expertos**

Los usuarios no deben intentar erradicar el código malicioso de los recursos informáticos por sus propios medios. Si un usuario sospecha que un recurso informático está bajo los efectos de un código malicioso, debe dejar de usarlo inmediatamente y solicitar asistencia a la Oficina de TI mediante los canales establecidos.

4.12. Seguridad física

Todas las áreas físicas del negocio deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas. la información confidencial o sensible al negocio debe mantenerse en lugares con acceso restringido cuando no es utilizada.

Los recursos informáticos de la Federación deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de negocio.

La información clasificada como confidencial no se dejará desatendida o sin control, por lo que la Federación desarrollará estrategias que permitan prevenir el acceso no autorizado a este tipo de información.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Acceso a áreas críticas (data center o cuartos de cómputo).**

El acceso de personal debe ser circunscrito a los miembros de la Sección de Operaciones TI y al Jefe de la Oficina de Tecnología Informática. Por tanto, solamente ellos podrán autorizar el ingreso de personal adicional.

TI debe llevar un registro permanente del tráfico de personal en los cuartos de cómputo de la Federación.

Las Oficinas de Tecnología y Servicios Administrativos deben proveer la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

El acceso a las áreas críticas de TI bajo condiciones de emergencia o de situaciones de urgencia manifiesta, debe ser autorizado por el Jefe de TI o su Responsable de Operaciones. En su ausencia, dicho aval lo puede entregar el Jefe de Servicios Administrativos.

- **Protección de medios de almacenamiento**

Los medios de almacenamiento de la Federación que contienen copias de respaldo de información deben protegerse en concordancia con la clasificación de la información que almacenan. Una copia adicional de estos medios debe estar guardada en una locación alterna al centro de cómputo bajo condiciones ambientales que garanticen su conservación. Esto debe estar contemplado en los procedimientos para administración de copias de respaldo de TI.

- **Custodia de información técnica de las herramientas tecnológicas**

La documentación, los manuales, los programas fuente, los medios y cualquier otro tipo de información técnica de las herramientas tecnológicas deben residir bajo la responsabilidad de la Oficina de TI; además debe reservarse una segunda copia en un lugar de acceso restringido para casos de contingencia o catástrofe.

Las áreas donde se encuentran recursos informáticos que contienen activos de información crítica de la Federación deben contar con equipos de seguridad ambiental, procedimientos formales para su uso y controles periódicos de verificación de su estado.

- **Circuitos alternos y equipos de respaldo para el suministro de energía**

Las áreas de procesamiento de información crítica y las indispensables para la operación del negocio deben contar con circuitos alternos y equipo de respaldo para suministro de energía.

- **Acceso de visitantes a áreas de acceso restringido de TI**

Deben existir controles específicos y de obligatorio cumplimiento para el acceso de visitantes a áreas de TI con acceso restringido. Para dichas áreas, únicamente el personal de la Federación formalmente autorizado puede accederlas en función de las

actividades que desarrolla. En el caso que los colaboradores y/o entes externos requieran ingresar a estas áreas, deben estar acompañados por el personal autorizado de la Oficina de TI.

- **Obras civiles en áreas de TI con acceso restringido**

Todos los cambios estructurales dentro de los lugares destinados al procesamiento de datos y/o almacenamiento de recursos informáticos críticos deben estar avalados por la Oficina de TI, con el fin de evaluar, antes de la realización de estos, los posibles impactos sobre el área afectada.

- **Consumo de alimentos y cigarrillos en áreas que contienen recursos informáticos**

Está prohibido fumar y consumir alimentos en las áreas de acceso restringido que contienen recursos informáticos críticos de la Federación.

- **Control de acceso a los equipos de cómputo**

Todos y cada uno de los recursos informáticos deben ser asignados a un responsable, por lo que es de su competencia hacer buen uso de estos.

El usuario está en la obligación de bloquear su equipo de cómputo cada vez que se levante de su puesto. Como medida complementaria, la Oficina de TI establecerá una política de bloqueo de sesión automático por inactividad.

Al utilizar cualquier equipo de cómputo de la Federación, el colaborador debe utilizar sus credenciales de acceso, para establecer una sesión que le otorgue los privilegios asociados a su perfil.

4.13. No repudio

La autenticidad de un negocio o transacción electrónica que realice la federación debe ser asegurada.

La Federación se apoya día a día en los medios electrónicos para realizar sus actividades. Por lo tanto, para cualquier negocio o transacción que se haga por estos medios, la Federación debe asegurar la autenticidad de cada parte que interviene y evitar que alguna de ellas niegue su participación (no repudio).

Al realizar negocios electrónicos se deben generar rastros que le permitan a la Federación resolver conflictos cuando alguna de las partes niegue su participación.

Estos se deben generar, guardar y ser accedidos acorde con las políticas internas de la Federación y la normatividad aplicable.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Certificación de transacciones**

Con el fin de garantizar la aceptación en la realización de transacciones efectuadas entre la Federación y los clientes, se deben establecer mecanismos de certificación de las transacciones realizadas.

- **Certificación en todo el ciclo de la transacción**

Se deben incluir servicios de certificación en todo el ciclo de las transacciones que por su nivel de riesgo requieren de este mecanismo de control. Se debe contar con servicios de certificación en los siguientes puntos de la transacción:

a) Requerimiento del servicio

b) Evidencia de la generación

c) Evidencia de la transferencia y almacenamiento de información

d) Evidencia de la verificación

e) Solución de la disputa

- **Certificación de transacciones que afectan datos**

Se requiere hacer uso de servicios de certificación para toda comunicación entre las organizaciones que componen la Federación, así como entre la Federación y otros grupos de interés en la que se actualicen o transmitan bases de datos de terceros por medio de transacciones efectuadas por los sistemas de información. En general la transmisión y actualización de información crítica debe utilizar servicios de certificación.

- **Interfaces para los servicios de certificación**

El acceso a los servicios de certificación debe ser realizado mediante la incorporación de rutinas estándar en las aplicaciones.

- **Controles en reenvío de transacciones**

En caso de requerirse el reenvío de transacciones por parte de la Federación, se deben conservar las medidas de seguridad existentes en las transacciones originales. Las transacciones que fueron rechazadas, una vez que son reenviadas, deben sujetarse a los procedimientos habituales de seguridad y validación.

- **Grabación de transacciones rechazadas**

Todas las transacciones que sean rechazadas se deben almacenar en un archivo o base de datos de inconsistencias con el fin de verificar posteriormente si la transacción concluyó consistentemente en todos los aplicativos que involucró.

- **Responsabilidad del emisor con la custodia del certificado digital**

Es absoluta responsabilidad del emisor de una transacción la custodia y uso que se dé al certificado digital suministrado para la realización de transacciones electrónicas. El emisor de la transacción electrónica debe conocer y asumir la responsabilidad que implica el uso del certificado digital y los cuidados que debe tener para mantener su confidencialidad.

- **Responsabilidad del receptor**

Es responsabilidad del receptor de una transacción electrónica verificar la información de control y almacenarla adecuadamente. El receptor de la transacción debe verificar que el emisor es un ente autorizado para generar transacciones y validar todos los datos de control de la transacción. Si el receptor encuentra alguna anomalía debe rechazar la transacción y reportar el incidente.

- **Aspectos legales de la certificación**

Los participantes en transacciones comerciales deben aprobar y documentar las normas de operación de transacciones comerciales certificadas. Se debe establecer en el contrato los compromisos entre las partes involucradas en la transacción comercial realizada electrónicamente.

4.14. Administración de alertas

La Oficina de Ti debe ser alertada en el mismo instante en que existan violaciones a la política de seguridad informática.

Las situaciones o acciones que violen las políticas, responsabilidades y procedimientos de Seguridad informática deben ser detectadas, registradas e informadas a la Oficina de TI de manera inmediata (alertas). La Oficina de TI debe realizar el respectivo manejo de los incidentes, dando prioridad a dichas alertas y resolverlos conforme a la criticidad de la información que puede estar asociada a estos. El objetivo es atender estas y otras situaciones que la Oficina de TI considere como críticas.

La administración de los incidentes de seguridad informática estará a cargo de la Oficina de Tecnología Informática y se alinea con lo establecido en el Manual de Administración de Información de los Grupos de Interés de la Federación.

La administración de los incidentes de seguridad de la información estará a cargo de la Oficina de Gestión de Riesgo Corporativo.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Registro de alertas**

Se deben implementar herramientas donde se puedan registrar las alertas y que permitan evidenciar el ciclo del tratamiento de estas. Ej. Herramienta de Gestión de Casos TI.

- **Generación de alertas**

Los recursos informáticos deben disponer de mecanismos que alerten sobre eventos que comprometan su integridad y confidencialidad. Deben existir herramientas de generación de alertas a nivel de hardware, sistema operativo y software de seguridad, las cuales deben ser habilitadas en concordancia con la clasificación y criticidad del recurso informático.

- **Monitoreo de alertas**

Se deben implantar mecanismos para el monitoreo de alertas que faciliten su detección, notificación y seguimiento. Los mecanismos de monitoreo deben detectar posibles incidentes de seguridad informática.

- **Registros de alertas en logs de auditoría**

Se deben utilizar herramientas y software que permitan el registro de alertas, para su posterior análisis y el desarrollo de una gestión eficiente de verificación, control y seguimiento, siempre que sea requerido.

En cuanto al hardware, el tiempo de retención de los logs, variará dependiendo de las capacidades ofrecidas por cada dispositivo.

En cuanto al software, el tiempo de retención de los logs, variará dependiendo de la configuración ofrecida por el software estándar de industria o por las necesidades de cada Usuario Líder de los Sistemas de Información.

- **Responsabilidad de reporte de desviaciones o vulnerabilidades**

Todos los colaboradores son responsables por reportar en forma inmediata cualquier condición anormal o vulnerabilidad que detecte en el uso los recursos informáticos de la Federación mediante los mecanismos destinados para tal fin.

- **Reserva de la información sobre vulnerabilidades**

La información específica sobre las vulnerabilidades o condiciones anormales de seguridad informática tiene carácter confidencial.

- **Estructura de comunicación de incidentes**

La Federación debe establecer y mantener un procedimiento formal de reporte de incidentes de seguridad informática, que le permita a los usuarios informar acerca de éstos cuando se presenten o se tenga sospecha de su ocurrencia.

- **Seguimiento de incidentes**

Todo incidente o alerta de seguridad debe ser tratado de principio a fin mediante el procedimiento de tratamiento de incidentes de la Oficina de TI, que gestione el análisis, investigación, documentación, solución completa y seguimiento a cualquier incidente de seguridad.

4.15. Auditabilidad de los controles de seguridad informática

Los controles asociados a la seguridad informática de la Federación deben ser revisados periódicamente para asegurar el cumplimiento del modelo de gestión de riesgo

La Oficina de TI debe llevar a cabo revisiones periódicas del estado general de seguridad y riesgo informático, mediante la ejecución de pruebas de vulnerabilidad (hacking ético), que generen los respectivos análisis de brechas.

La Oficina de TI debe generar y ejecutar un plan de mitigación asociado a las vulnerabilidades detectadas y entregadas en el análisis. Para la ejecución de dichas mitigaciones, la Federación debe contar con los recursos del caso para llevarlas a cabo, sean humanos o económicos, siempre con el respaldo de la Alta Dirección.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Registros de Auditoría**

En la medida de lo posible, los recursos informáticos deben incluir registros de auditoría que involucren cualquier evento susceptible de verificación posterior.

- **Disponibilidad de información de Auditoría**

La información de auditoría de la Federación debe estar disponible para su uso por las personas autorizadas para tal fin.

- **Evaluación del informe de vulnerabilidades y ejecución de acciones de remediación**

La información generada como resultado del Ethical Hacking debe ser consolidada en un Análisis de Brechas (Gap Analysis). Este documento debe ser evaluado por la Oficina de TI y se debe preparar y ejecutar el respectivo plan de mitigación.

- **Registro de usuarios privilegiados**

Se debe registrar el acceso y/o actividades de usuarios privilegiados como los administradores de recursos informáticos y administradores de control de acceso lógico (usuarios líderes).

- **Sincronización de relojes**

La fecha y la hora deberán estar sincronizadas en todos los recursos informáticos de acuerdo con un estándar, para asegurar que los registros reflejan el tiempo exacto de ocurrencia. En el caso de que se trate de recursos informáticos ubicados en el exterior, se deben tener en cuenta las diferencias horarias (puede tomarse como referencia la hora legal colombiana del Instituto Nacional de Metrología).

4.16. Conectividad

Todas las conexiones a redes públicas deben ser autenticadas para prevenir que la información sea revelada o alterada.

Las conexiones a la red interna (LAN) de la Federación deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad de la información trasmitida sobre dicha red. Igualmente, todos los accesos de salida a otras empresas deben realizarse sobre redes previamente aprobadas por la Federación.

Los usuarios que se conecten a la red interna deben cumplir con la presente política antes de que se realice la conexión. Esto aplica igualmente a cualquier conexión actual o futura en la red de la Federación, que utilice medios públicos para integrar lugares que estén geográficamente dispersos.

Se requiere la aprobación del Propietario de la Información para poder accederla remotamente, y dichos accesos deben cumplir con lo estipulado en el numeral 4.8 de esta política.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Segregación de redes**

Se deben definir zonas separadas que agrupen lógicamente los recursos informáticos de la Federación de acuerdo con la criticidad de los activos de información que manejan.

- **Uso de los firewalls de la Federación como únicos puntos de acceso a redes externas**

En las sedes corporativas, el (los) Firewall(s) es (son) el único punto autorizado por la Federación para el establecimiento de conexiones de cualquier recurso informático de la organización con redes externas. En ninguna circunstancia se deben establecer conexiones directas hacia redes externas desde los recursos informáticos de la Federación.

- **Confidencialidad de la información técnica de la red**

La información técnica de la red interna de la Federación (direcciones internas, configuración y diseño de la red) debe estar restringida al personal autorizado que tenga necesidad legítima de conocerla y con una autorización explícita del Propietario de la Información. Toda la información mencionada tiene carácter de confidencial y debe recibir el tratamiento definido para este nivel de criticidad.

- **Controles de enrutamiento**

Se debe contar con mecanismos que controlen el enrutamiento en la red. El acceso a los recursos informáticos de la Federación desde redes externas o internas requiere que se verifique y controle que el acceso sea realizado exclusivamente sobre los recursos informáticos objeto de la autorización.

- **Control de acceso entre zonas de red**

Todas las zonas deben considerar los mecanismos de control de acceso consecuentes con el nivel de confidencialidad de la información que allí reside. TI podrá aislar o desconectar de la red de datos uno o más recursos informáticos que representen un riesgo o comprometan la seguridad de la información corporativa entre zonas de red.

- **Autenticación de conexiones remotas**

Los accesos desde puntos remotos o redes específicas externas deben contar con mecanismos de autenticación de la conexión que prevengan de posibles accesos no autorizados.

- **Acceso remoto hacia redes de la Federación**

El acceso remoto a las redes de la Federación debe ser tramitado a través de la Oficina de TI, previa evaluación de una razón justificada del negocio y la validación con el Propietario de la Información; adicionalmente, la Oficina de TI reportará las solicitudes de acceso remoto a las redes de la Federación a la Oficina de Gestión de Riesgo Corporativo.

Los permisos del usuario que accede remotamente a la red deben estar restringidos específicamente a la actividad particular a realizar.

Los equipos desde los que se accede deben estar validados por la Federación. Las direcciones de red, cuentas de usuario y contraseñas que son usados para este acceso son de carácter confidencial.

Deben considerarse los controles que limiten el acceso a la información y operaciones autorizadas. Algunos controles para tener en cuenta son:

a) Obligar el paso de toda comunicación remota a través de los componentes de seguridad perimetral definidos por la Oficina de TI.

b) Incorporar mecanismos de autenticación de la conexión que prevengan accesos no autorizados.

c) Ofrecer los mecanismos para que las áreas encargadas puedan definir el trabajo permitido, las horas de trabajo, la clasificación de la información que puede ser accedida, los sistemas internos y servicios que el usuario que ingresa remotamente está autorizado a acceder.

d) Registrar en el log de auditoría de las actividades realizadas mediante esta conexión.

- **Acceso remoto a redes externas desde la entidad**

El acceso remoto desde la Federación a otras redes externas debe realizarse por razones estrictas de negocio y desde equipos autorizados por la Oficina de TI.

- **Información confidencial en la red**

La información confidencial de la Federación a ser transmitida sobre cualquier red debe ser cifrada (mediante la utilización de mecanismos de encripción).

- **Integridad de la información en la red**

Se deben considerar en la arquitectura de la red los mecanismos apropiados que minimicen la probabilidad de que la información que fluye en la red pueda ser alterada.

- **Restricción de envío de información hacia redes externas.**

Únicamente con autorización del propietario de la Información, cuando exista una razón justificada de negocio y cuando se adhiera al Manual de Administración de Información de Grupos de Interés, se pueden realizar transferencias de datos y archivos hacia redes externas, incluida internet. Lo anterior, queda sujeto a la validación por parte de la Oficina de TI y la Oficina de Gestión de Riesgo Corporativo.

- **Acceso restringido a servicios de internet**

El acceso de colaboradores o terceros a los servicios de internet debe obedecer a propósitos legítimos del negocio, y este debe impedir la navegación a páginas no autorizadas, de acuerdo con los lineamientos de la Federación.

4.17. Uso de los activos o recursos informáticos del negocio

Los recursos informáticos son provistos a los usuarios exclusivamente para propósitos organizacionales.

Los recursos informáticos de la Federación son exclusivamente para propósitos del negocio y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Usuarios que intenten acceder a información para la que no tienen autorización, están violando la presente Política.

La Federación se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Uso y cuidado de recursos informáticos**

Es responsabilidad de los usuarios la conservación y uso correcto de los recursos informáticos. Los usuarios deben dar un tratamiento cuidadoso a los recursos informáticos que la Federación ha dispuesto para que realicen sus actividades laborales. De igual forma, el colaborador que se retire de la Federación deberá hacer entrega formal de los recursos informáticos asignados para su labor.

- **Uso de recursos informáticos de la Federación sólo en actividades propias del negocio**

Los recursos informáticos de la Federación deben ser utilizados únicamente para fines corporativos aprobados por la organización. Por lo tanto, tampoco se autoriza la conexión de recursos particulares a la red corporativa. La Federación, como proveedora de los recursos, tendrá la facultad de monitorear su uso por parte de los usuarios.

- **Ingreso y uso de información ajena para propósitos de negocio en la Federación**

Sin importar la fuente de donde provenga, la información que ingrese mediante medios electrónicos a la Federación y su utilización está supeditada a propósitos exclusivos del negocio y debe estar explícitamente autorizada por el Propietario de la Información.

- **Uso de recursos informáticos de seguridad autorizados**

Solamente los recursos informáticos de seguridad suministrados y/o autorizados por la Federación a través de la Oficina de TI, se deben utilizar en la protección de los activos de información.

- **Uso restringido de herramientas propias de la gestión de seguridad informática**

Únicamente los usuarios de la Oficina de TI o a quien esta delegue, están facultados por la Federación para utilizar herramientas propias de la gestión de seguridad informática, por lo tanto y a menos que esté explícitamente autorizado por el jefe de TI, éstas no pueden ser utilizadas por otros usuarios.

- **Restricción en el uso de privilegios**

Está prohibido intentar sobrepasar los controles de seguridad de los recursos informáticos, buscar vulnerabilidades de seguridad y/o examinar los recursos informáticos en busca de información, sin la autorización expresa de la Oficina de TI. Los usuarios sólo deben ingresar a las funciones u opciones de los aplicativos inherentes a su cargo, así le sean asignados permisos o privilegios adicionales por deficiencias en los sistemas de control de acceso lógico o por error en la definición de su perfil.

- **Cumplimiento de las políticas y los procedimientos de seguridad en el uso de los servicios de Internet e Intranet**

Todo usuario debe ser consciente y cumplir las políticas y el procedimiento de seguridad informática de la Federación cuando hace uso de los servicios de Internet e Intranet. Los usuarios autorizados por la Federación para acceder a servicios de Internet e Intranet son absolutamente responsables de la utilización que hagan de dichos servicios y por las consecuencias que se deriven de su utilización.

- **Replicación de mensajes de divulgación general y/o advertencias provenientes de fuentes externas a la organización.**

Está prohibida la replicación de mensajes de divulgación general o de advertencias públicas relacionados con temas de seguridad Informática hacia otros usuarios sin la autorización explícita de la Oficina TI o quienes ellos deleguen; solo ellos están autorizados para el envío de mensajes de divulgación general o de advertencias públicas relacionadas con seguridad informática provenientes de fuentes externas a la Federación.

- **Prohibición del envío de mensajes en cadenas, bromas y advertencias de virus**

Está prohibido el envío de mensajes cadena, bromas y advertencias de virus. El uso de los recursos informáticos de la Federación para el reenvío de correos con mensajes cadena o advertencias de virus no está permitido. Todo correo recibido con alertas sobre un supuesto virus o la existencia de código dañino dentro de la Federación debe ser verificado con la Oficina de TI.

- **Desconexión de recursos Informáticos que son fuente de riesgo**

La Oficina de TI podrá aislar o desconectar de la red de datos uno o más recursos informáticos que representen un riesgo o comprometan la seguridad de la información corporativa.

- **Monitoreo del uso de los recursos**

La Federación, a través de la Oficina de TI, como proveedora de los recursos informáticos, podrá realizar el monitoreo de su uso por parte de los usuarios.

- **Realización de investigaciones**

La Federación, a través de la Oficina de TI, como proveedora de los recursos informáticos podrá llevar a cabo investigaciones de seguridad sobre los recursos proveídos con el fin de establecer la responsabilidad de las acciones realizadas sobre los mismos.

- **Uso de medios removibles**

La utilización de elementos removibles de almacenamiento (memorias USB/Flash, CD/DVDs re escribibles, discos duros portátiles, celulares, PDAs, entre otros) por parte de los usuarios, deberá cumplir estrictamente los lineamientos establecidos por la Oficina de TI.
El colaborador que los utilice con la autorización respectiva deberá buscar en todo momento preservar la confidencialidad de la información almacenada en este y evitar el contagio de código malicioso (virus, troyanos, Spyware, etc.) en la red.

4.18. Mantenimiento de los niveles de seguridad informática

Los niveles de seguridad deben mantenerse o mejorarse en el tiempo.

Es responsabilidad de la Oficina de TI establecer y mantener niveles de seguridad que cumplan con el Manual de Administración de Información de Grupos de Interés de la Federación. También se debe tener en cuenta niveles de seguridad informática en casos de adquisición, desarrollo y mantenimiento de sistemas de información y/o cumplimiento de requerimientos legales.

Para el cumplimiento de la presente política se deben aplicar los siguientes aspectos:

- **Elementos de seguridad informática**

Los elementos de seguridad informática deben mantenerse actualizados de manera que el nivel de seguridad sea mantenido y mejorado en el tiempo.

- **Aseguramiento de la seguridad en la infraestructura y los sistemas de información**

La oficina de TI debe asegurar que la infraestructura y los sistemas de información implementados en la Federación cumplan con los niveles adecuados de seguridad informática de acuerdo con los requerimientos establecidos para la administración de la seguridad de la información. Para este propósito se deben realizar ejercicios de búsqueda y explotación de vulnerabilidades, así como su respectiva estrategia de remediación.

5. VIGENCIA DE LA POLÍTICA

Se espera que las Políticas en Seguridad Informática se preserven en el tiempo, por lo cual deberán ser revisadas periódicamente con el fin de establecer su actualización, vigencia y ajuste de acuerdo con los requerimientos del negocio y ante nuevas necesidades, con el fin de garantizar que sigan siendo adecuadas, suficientes y eficaces.

Cualquier colaborador de la Federación puede identificar la necesidad de modificar la presente Política. Dichas inquietudes y sugerencias deben ser comunicadas al Jefe de TI, responsable por el mantenimiento de ésta. Es responsabilidad de todos los colaboradores consultar el presente documento, así como sus modificaciones cada vez que estas sean informadas por la Oficina de TI.

Esta política entra en vigor a partir del momento de su publicación. El desconocimiento de la misma, de ninguna manera exime de su cumplimiento.