| | |
|---|---|
| FONAVIEMCALI *De tu mano hacia el futuro* | **Fondo de Empleados, trabajadore pensionados de las Empresas Munic FONAVIEMCALI.** |
| | **POLITICA GENERAL DE SEGUR INFORMACIÓN Resolución No.012 de 2020 Acta de Junt** |

FONAVIEMCALI
*De tu mano hacia el futuro*

2020

# POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

**APROBADO POR LA JUNTA DIRECTIVA DE FONAVIEMCALI**

**2020-10-12**

**Contenido**

# POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE FONAVIEMCALI.

## Política Corporativa de Seguridad de la Información

**FONAVIEMCALI** reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, bases de conocimiento, manuales, estudios internos, códigos fuente de aplicaciones, estrategia, gestión, y otros conceptos; sabemos que la información es un activo fundamental para la prestación de nuestros servicios, comercialización de nuestros productos y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de nuestra parte en la protección de la información como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad de la información.

Lo anterior se implementa con el fin de identificar y minimizar los riesgos a los cuales se expone la información, ayudando a la reducción de costos operativos, financieros, y establecer una cultura de seguridad lo cual garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

### 1. PROPOSITO DE ESTA POLITICA

Es el propósito de este documento definir la política Institucional con respecto al uso responsable de los sistemas de información de **FONAVIEMCALI,** entendiendo por uso responsable el seguimiento de normas, políticas y buenas prácticas que salvaguarden la seguridad de la información, sistemas de información y recursos tecnológicos Institucionales.

### 2. ALCANCE Y OBJETIVOS

La Política de Seguridad de la Información de **FONAVIEMCALI** aplica a los consultores, proveedores, colaboradores, estudiantes en práctica,

aprendices y a cualquier otra persona natural o jurídica que tenga acceso a los sistemas de información del Fondo.

La Política de Seguridad de la Información como instrumento fundamental del Modelo de Seguridad y Privacidad de la Información de **FONAVIEMCALI** tiene como objetivos los siguientes:

## 3. OBJETIVOS:

- Minimizar el riesgo en los procesos del Fondo.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de protección de datos personales alineándose al cumplimiento de la ley 1581 de 2012.
- Mantener la confianza de los colaboradores, contratistas, proveedores, aliados estratégicos y otros terceros.
- Apoyar la innovación tecnológica en el Fondo.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores y contratistas.
- Garantizar la continuidad del negocio frente a incidentes.

## 4. TÉRMINOS/DEFINICIONES. Para los propósitos de esta política se aplicarán las siguientes definiciones:

**Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
**Amenaza**: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o al Fondo.
**Análisis de riesgos**: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
**Anonimización del dato**: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.
**Ciberseguridad**: capacidad de minimizar el nivel de riesgo al que están expuestos los usuarios, ante amenazas o incidentes de naturaleza cibernética.
**Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).
**Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

**Análisis de riesgos de seguridad de la información:** proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

**Comunicaciones electrónicas**: Incluyen todo uso de los sistemas de información para comunicar, publicar material y contenido por medio de servicios como correo electrónico, chat, páginas HTML, o alguna herramienta similar.

**Contraseña o Password**: Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

**Control Acceso Lógico:** El control de acceso lógico a sistemas y aplicaciones es la primera barrera que superar por parte de un atacante para el acceso no autorizado a un equipo y a la información que contiene.

**Copias de Respaldo:** Una copia de seguridad, respaldo, copia de respaldo, copia de reserva (del inglés *backup*) es una copia de los datos originales fuera de la infraestructura que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales; etc.

**Exploits**: Es un método concreto de uso de un error de algún programa (bug) para entrar en un Sistema informático. Generalmente, un exploit suele ser un programa que se aprovecha de algún Error del sistema operativo, por ejemplo: obtener los privilegios del administrador y así tener un control total sobre el sistema.

**ID**: La palabra" id", es la abreviatura del vocablo inglés "Identification", que traducido al idioma español significa "identificación". La "id" sirve para dar un nombre de usuario dentro de un correo, portal, servicio, juego online o cualquier otro tipo de sitio en Internet que nos pida un registro.

Esta identificación servirá para que entremos en este sitio con un perfil prediseñado por nosotros mismo, que además también llevará consigo una clave de acceso para que podamos tenerlo adaptado. Esta identificación también suele ser llamada por el nombre de Nick, mucho más popular.

**Material no permitido**: Incluye la transmisión, distribución o almacenamiento de todo material Que viole cualquier normatividad aplicable. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial, secreto

comercial u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización, así como material que resulte obsceno, difamatorio o ilegal de acuerdo con el ordenamiento jurídico nacional.
**Red Institucional**: Es el conjunto de recursos de conectividad computacionales que permite la comunicación de datos e información a través de toda el Fondo incluyendo Internet.
**Redes**: Incluye cualquier sistema de cableado o equipos físicos como enrutadores, switches, además de varios sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.
**Sistemas de información**: Incluye cualquier sistema o aplicación de software que sea administrado por el Fondo y de los cuales ella es responsable, como lo son las aplicaciones de servidores, escritorio, sistemas operativos y aplicaciones de Internet.
**Spoofing:** Es el procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente para engañar al programa o sistema que protege la red contra intrusos (firewall).
**Terceros:** todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
**Usuario(s)**: Incluye toda persona, no necesariamente vinculada directamente con el Fondo que tenga interacción con el uso de los recursos y servicios de sistemas de información de la empresa, ya sean (personal administrativo, directivos, Consultores, practicantes, proveedores, clientes, etc.).

## 5. COMPROMISO DEL COMITÉ ESTRATÉGICO

El Comité Estratégico de **FONAVIEMCALI** aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

El Comité Estratégico de la entidad demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los colaboradores de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas

**FONAVIEMCALI** establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Organización. Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de

plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

## 6. NORMAS QUE RIGEN PARA LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

### 6.1. Normas dirigidas a: COMITÉ ESTRATÉGICO

- Debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- Debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- Debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.
- Debe promover activamente una cultura de seguridad de la información en el instituto.
- Debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.
- Debe asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la empresa.

### 6.2. Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- El Comité de Seguridad de la Información debe actualizar y presentar ante la presidencia las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

### 6.3. Normas dirigidas a: OFICINA DE GESTIÓN DE CALIDAD

- La Oficina de Gestión de Calidad debe liderar la generación de lineamientos para gestionar la seguridad de la información de **FONAVIEMCALI** y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- La Oficina de Gestión de Calidad debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

### 6.4. Normas dirigidas al: ÁREA DE SISTEMAS

- El área de sistemas debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información del **FONAVIEMCALI** a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- El área de sistemas debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- El área de sistemas debe informar a las áreas responsables los hallazgos de las auditorías.
- La jefatura de Sistemas debe asignar las funciones, roles y responsabilidades, a sus colaboradores para la operación y administración de la plataforma tecnológica del Fondo. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

### 6.5. Normas dirigidas a: TODOS LOS USUARIOS

- Los colaboradores y personal provisto por terceras partes que realicen labores en o para **FONAVIEMCALI**, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

## 7. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

**FONAVIEMCALI** ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión del Fondo en cuanto a la protección de sus activos de Información:

1. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de **FONAVIEMCALI,** siendo posible tener un aliado estratégico externo para conformar este comité.
2. Los activos de información de **FONAVIEMCALI**, serán identificados y clasificados para establecer los mecanismos de protección necesarios.
3. **FONAVIEMCALI** definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.
4. Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de **FONAVIEMCALI.**
6. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por el Fondo.
7. Es responsabilidad de todos los colaboradores y contratistas de **FONAVIEMCALI** reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
8. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.
9. **FONAVIEMCALI** contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales. Adicionalmente **FONAVIEMCALI** cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

## 8. POLÍTICAS ESPECÍFICAS Y COMPLEMENTARIAS:

### 8.1. Acuerdos de confidencialidad

Todos los colaboradores de FONAVIEMCALI y/o terceros deben aceptar los **acuerdos de confidencialidad** definidos por el Fondo, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella. Lo anterior soportados en la política de protección de datos de la organización.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de **FONAVIEMCALI** a personas o entidades externas. Estos acuerdos deben aceptarse por cada uno de ellos como **parte del proceso de contratación**, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

### 8.2. Segregación de funciones - [ISO/IEC 27002:2015 A.6.1.2]

Toda tarea en la cual los colaboradores tengan acceso a la infraestructura tecnológica y a los sistemas de información debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

En concordancia:

- Todos los sistemas de disponibilidad crítica o media de la Institución deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

- El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Deben estar claramente segregadas las funciones de soporte técnico, planificadores y operadores.

### 8.3. Uso aceptable de los activos - [ISO/IEC 27002:2015 A.8.1.3]

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los colaboradores y contratistas determinadas por el Comité Estratégico, Gerencias y Jefaturas de Área o Dependencia.
Todos los colaboradores y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "**acuerdo de confidencialidad de la información**", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerada como un "incidente de seguridad".

Además, en caso de existir un acto por parte de cualquier tercero definido por la ley como delito informático, éste se llevará a las instancias judiciales que se requieran basados en la ley 1273 de Delitos Informáticos en la jurisprudencia colombiana; o la que rija en el país donde se encuentre alguna sucursal de **FONAVIEMCALI**, todo en pro de la protección de la integridad de la organización frente a actos malintencionados con la información del Fondo.

### 8.4. Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de FONAVIEMCALI, es por eso por lo que este proceso debe hacerse desde una estación debidamente registrada y/o autorizada por el área de sistemas, es decir, el computador debe estar registrado dentro del DNS (Domain Name Server) primario del Fondo y/o estar localizado con una dirección IP legítima.

Con base en lo anterior, el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

**a) No está permitido:**

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, YouTube, y paginas no corporativas que tengan como objetivo crear

comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de **FONAVIEMCALI**

- El intercambio no autorizado de información de propiedad de **FONAVIEMCALI**, de sus clientes y/o de sus funcionarios, con terceros.
  La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica consideradas herramientas de (hacking), entre otros.
- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la jefatura de Sistemas, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

### 8.5. Gestión de medios removibles - [ISO/IEC 27002:2015 A.8.3.1]

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de **FONAVIEMCALI**, estará autorizado para aquellos colaboradores cuyo perfil del cargo y funciones lo requiera.
La jefatura de Sistemas es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de **FONAVIEMCALI** sólo los colaboradores autorizados pueden hacer uso de los medios de almacenamiento removibles.
Así mismo, el colaborador se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de **FONAVIEMCALI** que éste contiene.

Para los funcionarios que estén autorizados a tener en sus equipos con uso de dispositivos removibles estos estarán habilitados con el conocimiento del jefe del área y las implicaciones que tiene el mal uso de este recurso en conocimiento del funcionario, asumiendo este la responsabilidad de los eventos de seguridad que se presenten con el dispositivo en casos de uso inadecuado o eventos de seguridad por negligencia o descuido.

Para determinar los usuarios que cuentan con el permiso se cuenta con una Matriz de usuarios VIP donde se referencia el usuario, el cargo, la actividad a desempeñar y la justificación del permiso.
Los funcionarios que no cuenten con esta autorización no podrán tener acceso a leer o escribir información en dispositivos de uso extraíble por lo cual deberán usar otros recursos como correo electrónico o los sistemas de almacenamiento en la nube que están aprobados por el área de sistemas y puestos a su disposición.

### 8.6. Gestión de acceso de usuario - [ISO/IEC 27002:2015 A.9.2]

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de **FONAVIEMCALI** debe ser asignado de acuerdo con la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Institución, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información. Los responsables de la administración de la infraestructura tecnológica de **FONAVIEMCALI** asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo con procesos formales de autorización los cuales deben ser revisados de manera periódica por el área encargada de **FONAVIEMCALI.**

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los colaboradores y terceros e implementada por La jefatura de Sistemas. Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de **FONAVIEMCALI,** sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

### 8.7. Gestión de contraseñas de usuario - [ISO/IEC 27002:2015 A.9.4.3]

Todos los recursos de información críticos de **FONAVIEMCALI** tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por La jefatura de Sistemas.

Todo funcionario o tercero que requiera tener acceso a los sistemas de información de **FONAVIEMCALI** debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (Password) asignado por la organización. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas. Como política de contraseñas estas deberán tener como mínimo 12 caracteres mayúsculos, minúsculos y caracteres especiales acompañados de números y no deberán tener relación alguna con la persona como tal. La asignación de estas contraseñas será una responsabilidad directa del usuario y en casos de eventos de seguridad si este se presenta por causa de una contraseña débil esta responsabilidad será imputada al funcionario que no acató la política respectiva.

### 8.8. Correo electrónico

Los colaboradores y terceros autorizados a quienes **FONAVIEMCALI** les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

**a)** La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de **FONAVIEMCALI**, así mismo podrá ser

utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

**b)** Los mensajes y la información contenida en los buzones de correo, así como los adjuntos son propiedad de **FONAVIEMCALI** y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones laborales.

**c)** El tamaño de los buzones de correo es determinado, según las políticas de buzón definidas por la administración de la plataforma OF365 por parte de Tecnología de la información, previa definición estándar de la plataforma correspondiente.

**d)** El tamaño de envío y recepción de mensajes, sus contenidos y demás características propias de estos deberán ser definidos e implementados por el área Tecnología de la información.

**e) No es permitido:**

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes con datos sensibles que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- No es permitido cadenas de correos con datos personales que evidencien intercambio de estos de manera irresponsable o con fines no permitidos en la organización o que no sean válidos para dar formal cumplimiento con lo estipulado en la ley 1581 de protección de datos personales y que no estén alineados con la política interna de protección de datos personales de **FONAVIEMCALI.**
- Utilizar la dirección de correo electrónico de **FONAVIEMCALI** como punto de contacto en comunidades interactivas de contacto social, tales como Facebook y/o MySpace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y la jefatura de Sistemas.

**f)** El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que **FONAVIEMCALI** proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

**g)** El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Oficina respectiva de Comunicaciones, mercadeo o medios de comunicación y la autorización de La jefatura de Sistemas. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser

eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

**h)** Toda información de **FONAVIEMCALI** generada con los diferentes programas computacionales (Ej. Office365, Project, Access, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables usando tecnologías como **cifrado de datos**, utilizando las características de seguridad que brindan las herramientas proporcionadas por el Área Tecnología de la Información. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

**i)** Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por **FONAVIEMCALI** y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

### 8.9. Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por **FONAVIEMCALI** a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de **FONAVIEMCALI** es responsabilidad del Área Tecnología de la Información, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por **FONAVIEMCALI** a través de esta Gerencia.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por el Área Tecnología de la Información.

c) El área de sistemas de la Información con sus responsables en cabeza de La jefatura de Sistemas debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Los colaboradores y terceros autorizados por La jefatura de Sistemas, o los que posean la posibilidad de acceso controlado de usuario y contraseña deberán dar uso adecuado a los recursos de la red inalámbrica de **FONAVIEMCALI,** está prohibido realizar cualquier tipo de actividad ilícita o de bloqueo de los puntos de acceso que pueda poner en riesgo, afectar o detener de manera provocada o malintencionada el servicio inalámbrico de la red de **FONAVIEMCALI.**

e) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de **FONAVIEMCALI,** deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por La jefatura de Sistemas.
f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de **FONAVIEMCALI;** las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por La jefatura de Sistemas.
g) La sincronización de dispositivos móviles, tales como PDAs, smartphones, tablets, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con La jefatura de Sistemas y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.
h) Cada colaborador del Fondo será responsable de los recursos tecnológicos físicos, como computadores, impresoras, discos, y cualquier equipo informático que quede a su cargo desde el momento de ingresar a el Fondo, y en caso de pérdida, robo o deterioro intencional o por negligencia comprobada deberá responder por el recurso asignado, y será labor de la presidencia determinar la forma de cómo se debe restituir en dinero o en especie este recurso.

### 8.10. Áreas Seguras- [ISO/IEC 27002:2015 A.11.1]

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en **FONAVIEMCALI,** deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad del Área de Sistemas del fondo y las dependencias propietarias del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre **FONAVIEMCALI** y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad de la jefatura de Sistemas garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con el comité estratégico o el nivel gerencial del que dependa esta área de Sistemas, establecer estos aspectos con las obligaciones contractuales específicas.

### 8.11. Control de acceso físico - [ISO/IEC 27002:2015 A.11.1.2]

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, y confidencial de la empresa, así como aquellas en las que se encuentren

los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

### 8.12. Seguridad de los equipos - [ISO/IEC 27002:2015 A.11.2]

Los equipos que hacen parte de la infraestructura tecnológica de **FONAVIEMCALI** tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de **FONAVIEMCALI** no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

**FONAVIEMCALI** mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

### 8.13. Ubicación y Protección de los Equipos- [ISO/IEC 27002:2015 A.11.2.1]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de **FONAVIEMCALI** deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general.

Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata. Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5)

minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

### 8.14. Controles contra Códigos Maliciosos - [ISO/IEC 27002:2015 A.12.2.1]

**FONAVIEMCALI** establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware, Cifradores y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la jefatura de Sistemas autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados en ninguna circunstancia, así como de su actualización permanente.

Así mismo, **FONAVIEMCALI** define los siguientes lineamientos:

**No está permitido:**

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por **FONAVIEMCALI.**
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por la jefatura de Sistemas.

### 8.15. Respaldo de la información - [ISO/IEC 27002:2015 A.12.3.1]

**FONAVIEMCALI** debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la jefatura de Sistemas y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la organización, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El área encargada del proceso tecnológico en conjunto con su aliado estratégico prestador de servicios tecnológicos establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca

del traslado, frecuencia, identificación y definirá juntamente con las dependencias los períodos de retención de esta.

Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada. Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta.

El sitio externo donde se resguardan dichas copias debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados. Así mismo todo acuerdo contractual con el tercero que administre la seguridad de los respaldos deberá exigir que este deberá cumplir con lo estipulado en la ley 1581 de protección de datos personales actuando como encargado de la información si es un ente distinto a funcionarios de la organización en caso de no existir reglamentaciones de protección de datos en el documento contractual vigente en el momento del servicio.

### 8.16. Controles de Auditoria de los sistemas de Información - [ISO/IEC 27002:2015 A.12.7.1]

El área de sistemas de la empresa **FONAVIEMCALI** ha identificado los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga. Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos. Estos procesos de aceptación deberán realizarse y controlarse por medio de formatos establecidos para la actividad realizada por cada tercero.

### 8.17. Separación de las Redes - [ISO/IEC 27002:2015 A.13.1.3]

La plataforma tecnológica de **FONAVIEMCALI** que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La jefatura de Sistemas es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

### 8.18. Transferencia de información - [ISO/IEC 27002:2015 A.13.2]

**FONAVIEMCALI** firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar

información restringida o confidencial de la Institución. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información. Así mismo se requerirá para el intercambio de información que se tengan en cuenta los aspectos legales alineados con ley 1581 para lo cual se deben tener los mensajes de privacidad respectivos y las autorizaciones de los titulares en caso de que sean datos personales. Así mismo este aparte deberá ser tratado principalmente y de manera más detallada en la política interna de **FONAVIEMCALI** relacionada con la protección de datos personales.

Todo colaborador de **FONAVIEMCALI** es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

### 8.19. Política Para Uso De Dispositivos Móviles.

**FONAVIEMCALI** proveerá las condiciones para el manejo de los dispositivos móviles (portátiles, teléfonos inteligentes y tabletas, entre otros) corporativos que hagan uso de servicios de FONAVIEMCALI. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por el Fondo.

### 8.20. Política de Seguridad de Teletrabajo o Home Office.

**FONAVIEMCALI** cuenta con las aplicaciones CORE de su negocio en ambientes web como son ERP, Correo electrónico y repositorios de datos de usuarios entre otros; es muy importante para la seguridad de la labor de los funcionarios del Fondo que se tengan en cuenta medidas mínimas de seguridad de la información, para así cumplir con el objetivo de mantener disponibilidad, confidencialidad e integridad de la información de FONAVIEMCALI.

En los casos que se requiera que un funcionario este en modo teletrabajo es importante que éste trabaje con el equipo local y activo del Fondo y solo en casos especiales sea aprobado trabajar con equipos que no son del Fondo siendo un requisito que estos cumplan con las medidas de seguridad mínimas que esta política contempla.

Para que un funcionario este en modo teletrabajo es un requisito que se tengan las mínimas medidas de seguridad para estar protegido frente a las principales amenazas de Internet, estas son:

- Disponer de un antivirus licenciado y actualizado.
- Utilizar un equipo con sistema operativo legal licenciado y actualizado
- Utilizar contraseñas robustas en todos sus accesos requeridos basados en la política de contraseñas del Fondo.
- Verificar que en el acceso a los servidores corporativos se utilicen certificados reconocidos por la red del Fondo, un usuario del dominio del Fondo y que los sitios web a los que accede tengan el “candado” de la conexión SSL.

Para prácticamente cualquier otro tipo de conexión que requiera acceso a la red interna de la organización, lo más importante es activar una conexión VPN, con un usuario y clave válida dentro de la red de FONAVIEMCALI, así como contar con los permisos respectivos de su líder de área.

Para casos especiales cuando el funcionario no puede usar un equipo del Fondo, éste permiso deberá ser avalado por un directivo de la misma y este funcionario deberá firmar un documento de responsabilidad para el cumplimiento de la política en cuanto a que el equipo a usar no debe ni puede tener menos de las medidas de seguridad descritas en esta política y que la responsabilidad de los eventos de seguridad que pasen en la infraestructura por el incumplimiento de la misma será su responsabilidad.

Normas para uso de dispositivos móviles Normas dirigidas a:

**AREA DE TECNOLOGIA DE LA INFORMACIÓN**

- Gestionar las opciones de protección de los dispositivos móviles corporativos que hagan uso de los servicios autorizados por FONAVIEMCALI.
- Establecer las configuraciones requeridas y permitidas para los dispositivos móviles corporativos que hagan uso de los servicios autorizados por FONAVIEMCALI.
- Todos los dispositivos móviles con línea corporativa deben tener configurado un bloqueo de acceso de seguridad (contraseña, biometría, patrones gráficos, u otras opciones).
- Aplicar a los dispositivos móviles corporativos que cumple funciones corporativas, los controles de protección contra código malicioso.
- Aplicar los controles de seguridad que eviten el uso de las SIM Card de las líneas móviles corporativos en equipos diferentes a los autorizados y registrados por FONAVIEMCALI.
- Implementar los controles tecnológicos que impidan la conexión a redes y servicios de FONAVIEMCALI de equipos móviles con sistemas operacionales con modificaciones consideradas inseguras (Jailbreack, rooting, entre otros).

**NORMAS DIRIGIDAS A: TODOS LOS USUARIOS**

- No dar uso al dispositivo en actividades que no sean exclusivamente relacionadas con sus actividades de carácter laboral.
- Informar al área de tecnología todos los inconvenientes que presente el dispositivo y no tomará acciones de soporte correctivo en lugares distintos al área de tecnología de la empresa.
- Informará al área de tecnología todos los mensajes o eventos que se presenten y que dentro de su percepción detecte que hacen referencia a mensajes o eventos de seguridad o que atenten contra la seguridad de la información institucional que posee el dispositivo.
- No prestará el dispositivo a ninguna persona a no ser que este dispositivo sea solicitado por un jefe o el área de sistemas del Fondo con el debido procedimiento y de manera personal.
- No instalará ningún tipo de programa o aplicación que no sea aprobada por el área de sistemas
- Para quienes tengan autorizado el uso de dispositivos móviles personales para tener acceso a la información institucional se suscribe un acuerdo de usuario final de dispositivos móvil que incluye la renuncia a la propiedad de los datos y el borrado remoto en caso de incidentes con el dispositivo. En todo caso se preserva el derecho a la privacidad del propietario del dispositivo.
- Evitar usar dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad físicas necesarias para evitar pérdida o robo de estos.
- No modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Evitar la instalación de programas desde fuentes desconocidas; instalar aplicaciones en los dispositivos móviles únicamente desde repositorios seguro y previa consulta al área de tecnología del Fondo.
- Evitar hacer uso de redes inalámbricas de uso público inseguras para transmitir información institucional, así como conectar los dispositivos a equipos de uso compartido público (Cafés internet, hoteles, aeropuertos, computadores personales no institucionales).
- No almacenar videos, fotografías, o información de tipo personal en los dispositivos móviles institucionales asignados.
- Preservando el derecho fundamental a la intimidad, las actividades realizadas con los dispositivos móviles institucionales o los activos de información institucionales podrán ser monitoreados siguiendo los procedimientos del Fondo o los definidos por la normatividad vigente.

## 9. NOTIFICACIÓN.

Con el fin de dar cumplimiento a la **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE FONAVIEMCALI**, el área de Talento Humano establecerá un acta de compromiso o un Otro Sí al Contrato de trabajo que firmarán todos los colaboradores al momento de recibir la identificación personal.

## 10. APLICACIÓN Y CUMPLIMIENTO

Cualquier usuario definido en el alcance del presente documento que viole las **POLÍTICAS DE SEGURIDAD DE INFORMACIÓN DE FONAVIEMCALI** será objeto de las acciones legales pertinentes. Esta política aplica desde el momento de su publicación en los medios de comunicación oficiales del Fondo.

**Original firmado**

**MILTON RUFINO ORDOÑEZ**
Presidente Junta Directiva

**JULIO CESAR VILLOTA**
Secretario Junta Directiva

**CONTROL DE CAMBIOS**

| Páginas | Descripción del cambio | Fecha y Acta de aprobación Junta Directiva |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |