POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

INSTITUTO DE FINANCIAMIENTO, PROMOCIÓNY DESARROLLO DE MANIZALES

VERSIÓN	FECHA	CAMBIOS
1.0.0	23/12/2021	Versión inicial del documento
2.0.0		Revisión del cumplimiento de la documentación
3.0.0	26/09/2023	Incluir temas de ciberseguridad y cambio de nombre de la política
4.0.0	14/04/2026	Cambios solicitados por la Revisoría Fiscal y ajustes para fortalecer la alineación del documento con el Modelo de Gestión de Seguridad de la Información.

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los principios, lineamientos y directrices generales para la gestión de la seguridad de la información y la ciberseguridad en Infimanizales, con el fin de proteger la confidencialidad, integridad, disponibilidad y demás atributos de seguridad de los activos de información, en armonía con el direccionamiento estratégico, la gestión del riesgo, la continuidad de la operación y el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

2. DEFINICIONES/GLOSARIO

- Activo de información: Información, datos, sistemas, servicios, software, hardware o recursos que tienen valor para Infimanizales y requieren protección.
- Amenaza: Causa potencial de un incidente no deseado que puede afectar un activo de información.
- Ciberseguridad: Capacidad institucional para prevenir, detectar, responder y recuperarse frente a amenazas e incidentes cibernéticos que puedan afectar los activos de información, los servicios y la operación.
- Confidencialidad: Propiedad de la información de no estar disponible ni ser divulgada a personas, entidades o procesos no autorizados.
- Control: Medida administrativa, técnica, física o legal orientada a prevenir, detectar, corregir o mitigar riesgos.
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando sea requerida por una parte autorizada.
- Evento de seguridad de la información: Suceso identificado en un sistema, servicio o red que indica una posible brecha, falla de control o situación relevante para la seguridad.
- Gestión de riesgos: Proceso de identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos que pueden afectar los activos de información.
- Incidente de seguridad de la información: Evento o conjunto de eventos no deseados que comprometen o pueden comprometer la confidencialidad, integridad o disponibilidad de la información.
- Integridad: Propiedad de salvaguardar la exactitud, completitud y validez de la información.
- Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad y genere afectación sobre un activo de información.
- Seguridad de la información: Preservación de la confidencialidad, integridad, disponibilidad y, cuando aplique, autenticidad, trazabilidad y no repudio de la información.
- Tratamiento del riesgo: Proceso de definir e implementar medidas para evitar, mitigar, transferir o aceptar un riesgo.
- Usuario: Persona interna o externa autorizada para acceder a activos, sistemas o servicios de información de la entidad.
- Vulnerabilidad: Debilidad de un activo, sistema o control que puede ser explotada por una

amenaza.

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Infimanizales reconoce la información y los activos que la soportan como recursos estratégicos para el cumplimiento de su misión institucional y la prestación de sus servicios. En consecuencia, adopta la presente Política General de Seguridad de la Información y Ciberseguridad como marco rector para la protección de la confidencialidad, integridad, disponibilidad y demás atributos de seguridad de la información, así como para la gestión de los riesgos de seguridad de la información y ciberseguridad que puedan afectar sus procesos, servicios, tecnologías, usuarios y terceros relacionados.

La entidad se compromete a implementar, mantener y mejorar continuamente los lineamientos, controles y mecanismos necesarios para prevenir, detectar, responder y recuperarse frente a eventos e incidentes que puedan comprometer la seguridad de la información y la continuidad de la operación, en cumplimiento de los requisitos legales, regulatorios, contractuales e institucionales aplicables.

La gestión de la seguridad de la información y la ciberseguridad en Infimanizales se fundamenta en los siguientes principios:

- protección de los activos de información;
- gestión integral del riesgo;
- cumplimiento normativo y regulatorio;
- responsabilidad compartida;
- mejora continua;
- cultura de seguridad y ciberseguridad;
- seguridad en la relación con terceros y proveedores;
- apoyo a la continuidad de la operación y resiliencia institucional.

Infimanizales en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

4. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

Son objetivos específicos de la política de seguridad de la información los siguientes:

- Establecer el marco general para la gestión de la seguridad de la información y la ciberseguridad en la entidad.
- Fortalecer la cultura institucional de seguridad de la información y ciberseguridad en servidores, contratistas, usuarios y terceros relevantes.
- Definir lineamientos generales para la protección de los activos de información y la gestión de los riesgos asociados.
- Promover la implementación de controles, procedimientos y mecanismos de seguimiento orientados a la prevención, detección, respuesta, recuperación y mejora continua.
- Apoyar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables a la entidad en materia de seguridad de la información, ciberseguridad y protección de datos.

5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de Infimanizales manifiesta su compromiso con la protección de la información, la gestión de la seguridad de la información y la ciberseguridad, así como con el fortalecimiento continuo de los controles, capacidades y recursos necesarios para prevenir, detectar, responder y recuperarse frente a riesgos, eventos e incidentes que puedan afectar los activos de información, los servicios y la operación de la entidad.

En desarrollo de este compromiso, la Alta Dirección promoverá la adopción, cumplimiento, revisión y mejora continua de la presente política y de los documentos que la desarrollan; garantizará la asignación de recursos humanos, técnicos, tecnológicos y financieros razonablemente necesarios; impulsará la gestión de los riesgos de seguridad de la información y ciberseguridad; apoyará las actividades de sensibilización y capacitación; y realizará seguimiento periódico al estado de implementación, desempeño y efectividad del modelo de gestión de seguridad de la información y ciberseguridad.

Los documentos específicos para el desarrollo de la presente política deben ser socializados con la alta dirección y podrán ser adoptados por la gerencia general del Instituto a través de resoluciones de adopción.

6. ALCANCE

La presente Política General de Seguridad de la Información y Ciberseguridad aplica a todos los procesos de Infimanizales y comprende la información en cualquier formato, los activos de información, los sistemas de información, los servicios tecnológicos, la infraestructura tecnológica y de comunicaciones, así como los mecanismos físicos, lógicos y administrativos utilizados para su tratamiento, almacenamiento, transmisión y protección.

7. APLICABILIDAD

La presente Política General de Seguridad de la Información y Ciberseguridad es de obligatorio cumplimiento para todos los servidores públicos, contratistas, practicantes, proveedores, terceros y demás usuarios que, por razón de sus funciones, obligaciones o relación con Infimanizales, tengan acceso a la información, a los activos de información, a los sistemas de información o a la infraestructura tecnológica de la entidad.

La presente política se aplica junto con los manuales, procedimientos, instructivos, lineamientos y demás documentos que la desarrollan o complementan. Su incumplimiento dará lugar a las acciones administrativas, contractuales, disciplinarias, civiles o penales a que haya lugar, de conformidad con la normatividad vigente y las disposiciones internas de la entidad.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

Infimanizales define una estructura de roles y responsabilidades para orientar la gestión, implementación, seguimiento y mejora de la seguridad de la información y la ciberseguridad, con participación de las instancias de dirección, las áreas de apoyo, los líderes de proceso y los usuarios internos y externos que accedan a los activos de información de la entidad.

ROL / INSTANCIA /DEPENDENCIA	RESPONSABILIDADES
Consejo Directivo	• Aprobar la política de seguridad de la información y ciberseguridad. • Hacer seguimiento a los informes que presente la alta dirección relacionados con la implementación de la política.
Gerente General	• Proporcionar los recursos necesarios para la implementación y mantenimiento del modelo de gestión de seguridad de la información (Recursos económicos, humanos, tecnológicos y los que se requieren para la implementación de la política). • Presentar al Consejo Directivo para su aprobación, la política de seguridad de la información y sus actualizaciones. • Adoptar mediante resolución los manuales, procedimientos, instructivos, lineamientos y demás documentos que la desarrollan o complementan la política general.
Profesional Especializado (Planeación)	• Proponer la Política de Seguridad de la información y Ciberseguridad y sus actualizaciones y contribuir con el diseño de los manuales, procedimientos, instructivos, lineamientos y demás documentos que la desarrollan o complementan la política general. • Monitorear y verificar el cumplimiento de la política y de los manuales, procedimientos, instructivos, lineamientos y demás documentos que la desarrollan o complementan.
Profesional Especializado (Riesgos)	• Apoyar la articulación de la seguridad de la información y la ciberseguridad con la gestión institucional del riesgo financiero, el seguimiento y la mejora continua.
Profesional TI	• Implementar y operar los controles técnicos definidos, apoyar la gestión de incidentes, el monitoreo, la administración de plataformas tecnológicas y la ejecución de medidas de protección acordes con los lineamientos institucionales.
Talento Humano	• Incorporar acciones de inducción, reinducción, capacitación y concientización en seguridad de la información y ciberseguridad para servidores, contratistas y demás colaboradores.
Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Asesor de comunicaciones	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.

ROL / INSTANCIA /DEPENDENCIA	RESPONSABILIDADES
Secretaria General	• Incorporar en la gestión contractual y en la relación con terceros los requisitos, obligaciones y controles aplicables en materia de seguridad de la información y ciberseguridad. • Velar por se incluyan en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad, así mismo verificar periódicamente el cumplimiento de las mismas.
Líderes de Proceso	• Aplicar y promover el cumplimiento de la política y de los documentos derivados en sus procesos, identificar riesgos y coordinar la implementación de controles en el ámbito de su responsabilidad. • Participar en el control y mitigación de los riesgos de seguridad de la información y la ciberseguridad a los cuales se encuentran expuestos sus procesos.
Todos los funcionarios y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos de información y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados. • Adoptar una cultura de autocontrol y mitigación de riesgo de seguridad de la información y la ciberseguridad en todas las actividades diarias. • Cumplir las disposiciones establecidas en la política y en sus documentos complementarios, proteger los activos de información bajo su responsabilidad, participar en actividades de sensibilización y reportar oportunamente eventos o incidentes de seguridad
Usuario final	• Mantener la confidencialidad e integridad de los activos de información provistos por la organización para llevar a cabo sus labores. • Reportar cualquier violación, incidente, vulnerabilidad o riesgo potencial que afecte la seguridad de la información de Infimanizales a la Profesional de TI y esta a su vez a quien haga las veces en la Dirección de Ciberseguridad. • Proteger los activos de información de Infimanizales contra cualquier compromiso que pueda afectar la confidencialidad, integridad o disponibilidad de la información. • Cumplir las políticas, procedimientos e instructivos de seguridad de la información establecidos por Infimanizales y apropiar la seguridad de la información como una de sus responsabilidades de trabajo. • Mantener la integridad de la configuración entregada por el área de Informática del equipo asignado para desarrollar sus funciones. • Participar en sesiones de sensibilización frente a temas de seguridad de la Información y ciberseguridad. • Asegurar que la información bajo su cargo tenga copias de seguridad. • Garantizar el cumplimiento de los acuerdos de confidencialidad durante y después de la terminación laboral.

ROL / INSTANCIA /DEPENDENCIA	RESPONSABILIDADES
Dirección de Ciberseguridad	• Asesorar en materia de seguridad de la información y ciberseguridad a la Dirección General y a los procesos que lo solicite. • Gestionar el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento continuo del modelo de gestión de seguridad de la información. • Realizar la actualización de la política de seguridad de la información y los procedimientos e instructivos que la soporta. • Verificar el cumplimiento de la política de seguridad de la información de Infimanizales. • Desarrollar la estrategia de seguridad de la Información de Infimanizales. • Supervisar la implementación de la estrategia de la seguridad de la información. • Monitorear la gestión del riesgo de seguridad de la información sobre los activos de información. • Definir la estrategia de sensibilización, entrenamiento y educación en seguridad de la información en la organización. • Gestionar la divulgación de las políticas y directrices de seguridad de la información definidas por Infimanizales. Así mismo, sensibilizará a los interesados sobre las modificaciones que se efectúen a la Política de Seguridad de la Información. • Evaluar las iniciativas planteadas en función del fortalecimiento del modelo de gestión de seguridad de la información y gestionar su presentación ante la Gerencia General.

9. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Para el desarrollo de la presente Política General de Seguridad de la Información y Ciberseguridad, Infimanizales adoptará y mantendrá documentos complementarios que desarrollen los lineamientos, controles, procedimientos e instructivos aplicables a las diferentes materias de seguridad de la información y ciberseguridad.

Como mínimo, la entidad deberá contar con lineamientos o documentos específicos relacionados con las siguientes materias:

9.1. Seguridad de los recursos humanos

Infimanizales establecerá lineamientos para que los servidores, contratistas y terceros conozcan, asuman y cumplan sus responsabilidades frente a la seguridad de la información y

la ciberseguridad durante su vinculación, permanencia y desvinculación de la entidad.

9.2. Gestión de activos de información

Infimanizales adoptará lineamientos para la identificación, clasificación, uso, custodia, protección y disposición de los activos de información, de acuerdo con su criticidad y valor para la entidad.

9.3. Control de acceso lógico

Infimanizales definirá lineamientos para la gestión de identidades y accesos, con el fin de asegurar que el acceso a la información y a los recursos tecnológicos se otorgue de forma controlada, autorizada y acorde con las funciones de cada usuario.

9.4. Seguridad física y del entorno

Infimanizales implementará medidas orientadas a proteger las instalaciones, áreas, equipos e infraestructura física que soportan la información y los servicios institucionales, frente a accesos no autorizados, daños o interferencias.

9.5. Seguridad en las operaciones

Infimanizales establecerá lineamientos para la operación segura de sus recursos tecnológicos, con el propósito de proteger la información, mantener la estabilidad de los servicios y reducir la exposición a riesgos de seguridad y ciberseguridad.

9.6. Adquisición, desarrollo y mantenimiento de sistemas

Infimanizales incorporará criterios de seguridad de la información y ciberseguridad en la adquisición, desarrollo, implementación, mantenimiento y cambio de sistemas de información y tecnologías asociadas.

9.7. Relaciones con proveedores y terceros

Infimanizales definirá lineamientos para gestionar los riesgos de seguridad de la información y ciberseguridad asociados a proveedores, contratistas y terceros que accedan, procesen, custodien o administren información o servicios de la entidad.

9.8. Gestión de incidentes de seguridad de la información y ciberseguridad

Infimanizales adoptará lineamientos para el reporte, análisis, tratamiento, respuesta, recuperación y aprendizaje frente a eventos e incidentes que puedan afectar la confidencialidad, integridad, disponibilidad o uso adecuado de la información y los servicios tecnológicos.

9.9. Seguridad de la información en la continuidad del negocio

Infimanizales integrará la seguridad de la información y la ciberseguridad en sus estrategias de continuidad y recuperación, con el fin de fortalecer la resiliencia institucional frente a contingencias e incidentes.

9.10. Cumplimiento

Infimanizales promoverá el cumplimiento de los requisitos legales, regulatorios, contractuales e internos aplicables en materia de seguridad de la información, ciberseguridad, protección de datos y uso adecuado de los recursos tecnológicos.

9.11. Uso de la información

Infimanizales establecerá lineamientos para el uso, manejo, intercambio, conservación y disposición de la información, de acuerdo con su clasificación, sensibilidad y finalidad institucional.

9.12. Uso de medios extraíbles

Infimanizales regulará el uso de medios extraíbles y otros mecanismos de almacenamiento o transferencia física de información, con el fin de prevenir la pérdida, fuga, alteración o acceso no autorizado a los datos.

9.13. Copias de respaldo

Infimanizales adoptará lineamientos para la generación, protección, conservación, prueba y recuperación de copias de respaldo de la información y de los sistemas críticos, en concordancia con las necesidades de operación y continuidad.

9.14. Ciberseguridad

Infimanizales establecerá lineamientos orientados a prevenir, detectar, responder y recuperarse frente a amenazas cibernéticas, mediante la implementación de capacidades, controles y mecanismos acordes con su contexto de riesgo y necesidades institucionales.

10. SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Infimanizales promoverá una cultura institucional de seguridad de la información y ciberseguridad mediante actividades de sensibilización, capacitación, comunicación y concientización dirigidas a servidores públicos, contratistas, terceros y demás actores que la entidad considere relevantes, de acuerdo con sus niveles de responsabilidad y exposición al riesgo.

La entidad establecerá y mantendrá mecanismos y planes orientados a divulgar la presente política, fortalecer el conocimiento sobre buenas prácticas de seguridad de la información y ciberseguridad, y fomentar el reporte oportuno de eventos e incidentes que puedan afectar los activos de información y la operación institucional.

Las actividades de sensibilización, capacitación y comunicación deberán realizarse de manera periódica y estarán articuladas con los procesos de inducción, reinducción, formación institucional y gestión del cambio, de conformidad con los lineamientos definidos por la entidad.

11. SANCIONES

- Cualquier violación a las políticas de seguridad de la información de Infimanizales debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

- Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de esta. Las medidas correctivas por comportamientos inadecuados de los usuarios sobre los sistemas de información o por incumplimiento de las políticas establecidas por la organización, serán tomadas por el jefe o director del área responsable de la persona que está incumpliendo. Igualmente, si existe reiteración de los hechos, será informado al área de gestión humana. En el caso de terceros (servicios internos o externos, proveedores o contratistas) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de control pertinentes o autoridades competentes.

12. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Infimanizales realizará seguimiento semestral a la implementación, cumplimiento, desempeño y efectividad de la presente Política General de Seguridad de la Información y Ciberseguridad, así como de los lineamientos, controles y documentos que la desarrollen.

Para tal efecto, la entidad establecerá mecanismos de medición, evaluación y análisis que permitan identificar el nivel de avance del modelo de gestión, el comportamiento de los riesgos, la eficacia de los controles implementados, el estado de las acciones de mejora y las oportunidades de fortalecimiento en materia de seguridad de la información y ciberseguridad.

Los resultados del seguimiento y evaluación servirán de base para la toma de decisiones, la actualización de controles, la formulación de acciones correctivas, preventivas y de mejora, y la revisión periódica de la política y de sus documentos complementarios.

13. APROBACIÓN, VIGENCIA Y REVISIÓN

La presente Política General de Seguridad de la Información y Ciberseguridad será aprobada por el Consejo Directivo de Infimanizales y entrará en vigor a partir de la fecha de su aprobación formal.

La política deberá ser revisada, como mínimo, una vez al año, o antes si se presentan cambios normativos, regulatorios, organizacionales, tecnológicos, contractuales o de riesgo que afecten su pertinencia, suficiencia o efectividad.

También deberá revisarse y, de ser necesario, actualizarse, cuando se presenten incidentes relevantes de seguridad de la información o ciberseguridad, hallazgos de auditoría, resultados de seguimiento, cambios en el contexto institucional o cualquier otra situación que justifique su ajuste.

Toda modificación deberá quedar documentada mediante el respectivo control de cambios, versión y aprobación por la instancia competente.

14. REFERENCIAS NORMATIVAS

Para la formulación, implementación, mantenimiento y mejora continua de la presente Política General de Seguridad de la Información y Ciberseguridad, Infimanizales tendrá en cuenta, según su aplicabilidad, las disposiciones legales, regulatorias, técnicas e institucionales vigentes.

Entre las principales referencias se consideran, entre otras, las siguientes:

- Circular Básica Jurídica de la Superintendencia Financiera de Colombia, en lo relacionado con los requerimientos aplicables en materia de seguridad de la información y ciberseguridad.
- Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia, en cuanto al marco de requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad.
- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto reglamentario aplicable en materia de protección de datos personales y demás normas que lo modifiquen, adicionen o sustituyan.
- ISO/IEC 27001:2022, como marco de referencia para la gestión de la seguridad de la información.
- ISO/IEC 27002, como guía de buenas prácticas para controles de seguridad de la información, cuando resulte aplicable.
- Lineamientos, guías y modelos adoptados institucionalmente en materia de seguridad de la información, ciberseguridad, gestión del riesgo, continuidad del negocio y protección de datos personales.