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 Pendiente aprobación	8/10/2025	Cambios solicitados por parte de la revisoría fiscal

TABLA DE CONTENIDO

1. OBJETIVO 3

2. DEFINICIONES/GLOSARIO 3

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 5

4. COMPROMISO DE LA ALTA DIRECCIÓN 5

5. ALCANCE DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 6

6. APLICABILIDAD 6

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES YRESPONSABILIDADES) 6

8 POLÍTICAS 8

8.1 POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS 9

8.2 POLÍTICAS DE GESTIÓN DE ACTIVOS 9

8.3 POLÍTICAS DE CONTROL DE ACCESO LÓGICO 9

8.4 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO 10

8.5 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES 10

8.6 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 10

8.7 POLÍTICAS DE RELACIONES CON LOS PROVEEDORES 10

8.8 POLÍTICAS DE GESTIÓN DE INCIDENTES 12

8.8.1 SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO 12

8.9 POLÍTICAS DE CUMPLIMIENTO 13

8.9.1 ACTUALIZACIONES Y DIVULGACION DE LAS POLITICAS DE SEGURIDAD 13

8.9.2 ESCRITORIO LIMPIO: 13

8.9.3 USO ADECUADO DE INTERNET 13

8.9.4 USO ADECUADO DE CORREO ELECTRÓNICO: 14

8.9.5 USO DE USUARIOS Y CONTRASEÑAS: 14

8.9.6 APAGADO DE EQUIPOS EN LA NOCHE 15

8.10 POLÍTICA DE USO DE LA INFORMACIÓN 15

8.11 POLITICA DE BLOQUEO DE USO DE MEDIOS EXTRAIBLES DE ORIGEN FISICO 15

8.12 POLÍTICA DE COPIAS DE RESPALDO (BACKUP) 16

8.13 POLÍTICA DE CIBERSEGURIDAD 16

9 SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN 17

SENSIBILIZACIÓN Y COMUNICACIÓN 17

CAPACITACIONES EN SEGURIDAD 17

10 SANCIONES 18

11 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 18

12 APROBACIÓN Y REVISIONES A LA POLÍTICA 18

13 REFERENCIAS NORMATIVAS 19

1. OBJETIVO

Establecer los lineamientos generales para la seguridad de la información, teniendo en cuenta las demás políticas, normas y procedimientos que hacen parte de los procesos de la entidad, alineados con el contexto del direccionamiento estratégico y de gestión del riesgo garantizando la confidencialidad, integridad y disponibilidad de la información.

2. DEFINICIONES/GLOSARIO

- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Modelo de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Activo:** Todo lo que tiene valor para la entidad: Información, software o programa de cómputo, hardware o equipos de cómputo, servicios.
- **Almacenamiento:** Es un dispositivo que permite conservar los datos y la información de manera independiente y que permite presentarla a diversos sistemas.
- **Cableado estructurado:** consiste en cables de par trenzado protegidos (Shielded Twisted Pair, STP) o no protegidos (Unshielded Twisted Pair, UTP) en el interior de un edificio con el propósito de implantar una red de área local (Local Area Network, LAN).
- **Clave o Contraseña:** Es una forma de autenticación sobre los sistemas informáticos.Debe mantenerse en secreto y debe ser personal e intransferible y es recomendable con cumpla con condiciones de complejidad que garantice la seguridad.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.(CONPES 3701).
- **Confidencialidad**: Hace referencia a que la información no esté disponible o sea revelada a entes no autorizados.
- **Dominio:** Se entiende como un espacio en red que contienen todas las estaciones, y los distintos recursos compartidos administrados de forma centralizada.
- **ERP:** Los sistemas de planificación de recursos empresariales (en inglés ERP, Enterprise Resource Planning) son sistemas de gestión de información que automatizan muchas de

las prácticas de negocio asociadas con los aspectos operativos o productivos de una empresa.

- **Firewall perimetral:** Se define como un elemento o sistema que permite proteger unosperímetros en instalaciones sensibles de ser atacadas por intrusos.
- **IAS Solutions:** Nombre de la herramienta ERP adquirida por el Instituto para apoyar losprocesos financieros, contables, de nómina, recursos humanos y operacionales.
- **Máquina virtual:** Es un software que simula un sistema de computación y puede ejecutarprogramas como si fuese una computadora real.
- **Monitoreo:** Consiste en la observación de uno o más parámetros para detectar eventualesanomalías.
- **Red de Área Local (LAN):** Es la interconexión de varias Computadoras y Periféricos.
- **Roles:** Es una colección de permisos definida dentro de un sistema de información la cual se puede asignar a usuarios específicos en contextos específicos. La combinación de roles y contexto definen la habilidad de un usuario específico para hacer algo dentro de dicho sistema.
- **Servidor:** Es un equipo informático que forma parte de la red y provee servicios a otros equipos cliente.
- **Switch:** Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN)
- **Usuario:** Es una cuenta expedida al funcionario o contratista, la cual le permitirá ingresar a las diferentes plataformas o aplicativos que operan en la entidad.
- **VMWare:** Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un computador, un hardware) con unas características de hardware determinadas.
- **Wireless:** Término relativo a una red de área local (LAN) y ciertos dispositivos que no requieren cables físicos para su interconexión.
- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar el daño a un activo de información, sistema o proceso de la Corporación.
- **Evaluación de Riesgos:** Es el proceso de comparar el riesgo estimado contra un criterio dado, con el objeto de determinar su clasificación de acuerdo con su probabilidad de ocurrencia e impacto causado en caso de materializarse.
- **Evento:** Suceso identificado en una organización, sistema, servicio o estado de la red que indica una posible brecha en la Política de Seguridad de la Información o fallo de los controles, o una situación desconocida que podría ser relevante para la seguridad.
- **Gestión de Riesgos:** Proceso de identificación, medición, clasificación, control y minimización o eliminación, de los riesgos que afecten a la información de la Corporación.
- **Incidente:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad e impacto significativos de comprometer las operaciones del negocio y comprometer la seguridad de sus activos de información.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño de un activo de información. Combinación de la probabilidad de un evento y el impacto de sus consecuencias.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidades también consideradas.

- **Modelo de Gestión de Seguridad de la Información:** Es un proceso sistemático y documentado que ayuda a establecer políticas y procedimientos con relación al cumplimiento de los objetivos de la Corporación, con el objeto de mantener un nivel mínimo de exposición frente a los riesgos de la información, que la organización ha identificado. Este Sistema integra diferentes objetivos de control frente a la información, entre los que se encuentra la tecnología, la seguridad física, la protección legal, la gestión de recursos humanos, temas organizacionales, entre otros.
- **Tratamiento de Riesgos de la información:** Proceso de diseño, implementación y despliegue de controles para la eliminación, reducción, mitigación o transferencia de riesgos asociados a los activos de información de una organización.
- **Acuerdo de Confidencialidad:** Documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de INFIMANIZALES.
- **Backup:** Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Infimanizales entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un modelo de gestión de seguridad de la información buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

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

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, practicantes y terceros.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar el riesgo de todos los procesos de la entidad.
- Mejorar continuamente el modelo de gestión de seguridad de la información.
- Implementar los controles tecnológicos necesarios para la protección de los activos de información de la entidad y para la reducción de los riesgos.

4. COMPROMISO DE LA ALTA DIRECCIÓN

Infimanizales se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del modelo de gestión de seguridad de la información; así mismo, se compromete a revisar el avance de la implementación del modelo de gestión de seguridad de la información de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

5. ALCANCE DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos comprende a todos los procesos de la entidad.

6. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas y terceros de Infimanizales.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad.

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

Infimanizales, define los roles y responsabilidades para la implementación del Modelo de Seguridad y Privacidad de la Información y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos):

ROL / INSTANCIA /DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Consejo Directivo	• Aprobar la política de seguridad de la información y ciberseguridad. • Hacer seguimiento a los informes que se presenten relacionados con las políticas implementadas.
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, las políticas de seguridadde la información y sus actualizaciones.
Profesional Especializado (Planeación)	• Proponer la Política de Seguridad de la información y Ciberseguridad y sus actualizaciones. • Monitorear y verificar el cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información y ciberseguridad.

Profesional TI	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Monitorear y verificar el cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información. • Asesorar a la Gerencia en temas que considere necesarios sobre seguridad de la información y ciberseguridad para que estas últimas puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia. • Definir y gestionar los indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad. • Gestionar la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.
Talento Humano	• Implementar acciones para que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
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.
Secretaria General	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos • 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	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del modelo de gestión de seguridad de la información. • 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. • Participar, presentar y aprobar las capacitaciones que se brinden en materia de Riesgo de seguridad de la información y la ciberseguridad.

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.
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.

8 POLÍTICAS

Infimanizales, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

8.1 POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el modelo de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.
- Todos los usuarios nuevos que ingresan a Infimanizales ya sea como funcionario de planta o contratista y le sean asignados equipos de cómputo y/o hace uso de servicios informáticos de la entidad, debe aceptar las condiciones de confidencialidad, protección de datos y del uso adecuado de los bienes informáticos, así como cumplir y respetar las directrices entregadas en la presente Políticas de Seguridad de la información.
- Es responsabilidad de su jefe inmediato o supervisor de notificar al área de tecnología cuales son funciones en los procesos que va a participar. Con base en esta información se realizará la creación del perfil del nuevo funcionario en la red, como el rol en los sistemas de información y el correo institucional que utilizará para todas sus actividades.

8.2 POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de Infimanizales.
- Los activos dispuestos por Infimanizales para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de Infimanizales.
- Infimanizales identificara, clasificara y gestionara su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.
- Para el uso de los recursos tecnológicos de INFIMANIZALES, todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación.
- La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios de tecnología autorizados por INFIMANIZALES.

8.3 POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Cada usuario es responsable de los mecanismos de control de acceso que les sean proporcionados; esto es, del usuario y contraseña necesario para acceder a la red interna de información y a la infraestructura tecnológica del Instituto, por lo que se deberá mantener de forma confidencial.
- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.

- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- Los usuarios y funcionarios son responsables de todas las actividades realizadas con usuario (ID) y es su jefe inmediato o su supervisor quien debe solicitar la creación de su usuario al área de tecnología, así como también quien debe informar cuando debe ser deshabilitado por algún motivo.

8.4 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- Infimanizales adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- Infimanizales definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.

8.5 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. Infimanizales planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el modelo de gestión de seguridad de la información.

8.6 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- La oficina de servicios corporativos y el profesional universitario TIC, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

8.7 POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- Infimanizales establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

- Gestión de incidentes: Es obligación por parte de los funcionarios de la empresa proveedora el reporte de cualquier anomalía que sea detectada para que su tratamiento sea oportuno y se prevengan incidentes de Seguridad. El reporte debe ser canalizado a través de los diferentes niveles jerárquicos hasta llegar al punto de contacto directo con INFIMANIZALES, quien lo reportará al supervisor del contrato, quien a su vez lo reportará a la Dirección de

Ciberseguridad a través del Procedimiento Gestión De Incidentes.

- Requerimientos de Seguridad de Aplicaciones y/o servicios: Si el proveedor es responsable por aplicaciones o servicios informáticos estos deben cumplir con los requerimientos de protección de la Confidencialidad, Integridad y Disponibilidad definidos por INFIMANIZALES, y que debe demostrar con base en el activo que va a ser manejado con uno o más de los siguientes controles:

✓Monitoreo: Estar en capacidad de brindar los mecanismos para detectar incidentes de seguridad de la información sobre el funcionamiento de la aplicación con el que se presta el servicio a INFIMANIZALES. El nivel de detección se ajustará a los requerimientos del activo involucrado en el servicio.

✓Gestión de Vulnerabilidades: Mantener un proceso de revisión permanente de las posibles vulnerabilidades en las aplicaciones que son responsabilidad del proveedor y establecer el proceso de asesoría hacia INFIMANIZALES, con el fin de mitigar oportunamente los riesgos asociados con las vulnerabilidades identificadas.

✓Control de acceso: Presentar los mecanismos de control de acceso a los servicios y los datos manejados con base en la Política de Control de Acceso de INFIMANIZALES.

✓Gestión de incidentes: Contar con un esquema de identificación, reporte, escalamiento, tratamiento y documentación de los incidentes que se presenten en el funcionamiento de la aplicación o servicio prestado.

✓Soporte: El proveedor debe contar con los expertos idóneos para atender incidentes o eventos de seguridad de la información con base en el modelo de gestión de seguridad de la información de INFIMANIZALES.

✓Redundancia: Si los servicios provistos así lo requieren, el proveedor debe contar con sistemas redundantes que le permitan cumplir con los acuerdos de niveles de servicio acordados con INFIMANIZALES.

- Licenciamiento: Todas las aplicaciones y servicios prestados por el proveedor deben contar con el licenciamiento acorde con el marco legal y regulaciones que apliquen a INFIMANIZALES.

- Requerimientos de Seguridad de la Información de la Empresa Proveedora

INFIMANIZALES exigirá unas condiciones mínimas con respecto a Seguridad de la Información para las empresas proveedoras con las que exista intercambio de información según los niveles de clasificación. Así mismo la que este definida en nivel muy alto para Integridad y Disponibilidad, a saber:

- ✓ Contar con un modelo de gestión de seguridad de la información.
- ✓ Presentar la política de seguridad de la información referente al servicio o producto que se está prestando a INFIMANIZALES.
- ✓ Presentar el soporte para el procedimiento de tratamiento de los incidentes de seguridad de la información que puedan darse en el desarrollo del servicio o el producto entregado.
- ✓ Mostrar sus procedimientos de gestión de vulnerabilidades y diagnóstico de seguridad.
- ✓ Mostrar los planes de contingencia y recuperación donde muestre su capacidad de cumplir con la disponibilidad exigida en los acuerdos de niveles de servicio. Las empresas proveedoras cuyos servicios incluyen aspectos controlados por la legislación o regulaciones vigentes aplicables a INFIMANIZALES, deben asegurar y demostrar su cumplimiento.

- Términos y Condiciones

El proceso de contratación deberá establecer en los contratos las limitaciones necesarias para que el proveedor cumpla las políticas, los procedimientos y los instructivos de la seguridad de la información de INFIMANIZALES.

Todos los contratos, en materia de seguridad de la información, deberán incluir como mínimo lo

siguiente:

- ✓ Cumplimiento de las políticas de seguridad de la información y de la política de protección de datos personales de INFIMANIZALES por parte del tercero.
- ✓ Niveles de servicio y operación.
- ✓ Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
- ✓ Propiedad de la información.
- ✓ Restricciones sobre el software empleado.
- ✓ Normas de seguridad física a ser aplicadas.
- ✓ Procedimientos o instructivos a seguir cuando se encuentre evidencia de alteración o manipulación de equipos o información.
- ✓ Procedimientos o instructivos y controles para la entrega de la información manejada y la destrucción de esta por parte del tercero una vez finalizado el servicio.
- ✓ Documentación de los controles físicos y lógicos empleados por el tercero para proteger la confidencialidad, integridad, disponibilidad de los datos y los equipos.
- ✓ El cumplimiento explícito de la normatividad vigente y aplicable a INFIMANIZALES, en materia de seguridad de la información.
- ✓ Responsabilidades de confidencialidad de la información posteriores a la terminación del contrato.
- ✓ Responsabilidades y sanciones en caso de incumplimiento de los acuerdos respectivos.

8.8 POLÍTICAS DE GESTIÓN DE INCIDENTES

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al área de tecnología por cualquiera de los medios dispuestos para tal fin.
- Sera responsabilidad del área de Tecnología seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.
- Los propietarios de los activos de información deben informar al Profesional Universitario TIC los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
- El Profesional Universitario TIC debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al comité institucional de gestión del desempeño de procesos y procedimientos aquellos en los que se considere pertinente.
- El Comité de desempeño de procesos y procedimientos debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.
- El Profesional Especializado Riesgos debe, con el apoyo con del Profesional Universitario TIC, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
- Los funcionarios de Infimanizales en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, deben notificarlo al superior inmediato para que se registre y se le dé el trámite necesario.

8.8.1 SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- Infimanizales establecerá un plan de continuidad tecnológica donde se debe incluir la

continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.

8.9 POLÍTICAS DE CUMPLIMIENTO

Infimanizales velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

8.9.1 ACTUALIZACIONES Y DIVULGACION DE LAS POLITICAS DE SEGURIDAD

Debido a la evolución de la tecnología, las amenazas en temas de seguridad informática y a los cambios legales en la materia, la entidad se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Políticas serán presentados a la Gerencia para su aprobación.

- Es responsabilidad de cada uno de los colaboradores de INFIMANIZALES la lectura y conocimiento de la Política de Seguridad más reciente. Por lo tanto, el área de tecnología con el apoyo del asesor de comunicaciones de la entidad se encargará de realizar la divulgación y socialización de las presentes políticas.
- La falta de conocimiento de las normas aquí descritas por parte de los funcionarios o contratistas no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

8.9.2 ESCRITORIO LIMPIO:

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).
- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

8.9.3 USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
- El área de tecnología podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.
- Queda prohibido el uso de módems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación por parte de la Gerencia General.
- El uso de Internet está ceñido a las páginas requeridas para realizar las operaciones diarias, es de anotar que cualquier otro tipo de consulta está prohibida. Los usuarios de Internet serán por medio de la presente advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas.
- La información interna puede ser intercambiada a través de Internet, pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad

apropiados.

8.9.4 USO ADECUADO DE CORREO ELECTRÓNICO:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a INFIMANIZALES, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- El área de tecnología podrá verificar el contenido de los buzones de los correos electrónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.
- Formalidad del correo electrónico: Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto, podrá ser supervisada por el superior inmediato del empleado.
- Preferencia por el uso del correo electrónico: Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.
- Uso de correo electrónico: La cuenta de correo asignada es de carácter individual por lo cual ningún empleado en ninguna circunstancia debe usar la cuenta de otro empleado.
- Revisión del correo electrónico: Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo diariamente. Así mismo, es su responsabilidad mantener espacio libre en el buzón.
- Mensajes prohibidos: Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.
- Acciones para frenar el SPAM: En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas.
- Todo buzón de correo debe tener un responsable: Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

8.9.5 USO DE USUARIOS Y CONTRASEÑAS:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números) de una longitud mínima de 12 caracteres para garantizar protección ante ataques de diccionario, fuerza bruta y demás variantes.
- Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

Límite de intentos consecutivos de ingreso al sistema

- El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados:

- Ser suspendido hasta nueva reactivación por parte del administrador;
- Ser temporalmente bloqueado (no menos de 5 minutos);

8.9.6 APAGADO DE EQUIPOS EN LA NOCHE

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina durante la noche.

Tiempo limitado de conexión en aplicaciones de alto riesgo

Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad corto la aplicación deberá cerrar la sesión iniciada por el usuario.

Bloqueo estación de trabajo

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 5 min.

8.10 POLÍTICA DE USO DE LA INFORMACIÓN

Divulgación de la información manejada por los usuarios de INFIMANIZALES

INFIMANIZALES podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal, por solicitud de autoridad judicial o administrativa salvo las excepciones indicadas en este documento y las disposiciones legales de protección de datos personales. Se deja claridad que la información pública proveniente de la función registral es administrada exclusivamente para los fines propios de los registros públicos de acuerdo con las normas legales y reglamentarias vigentes sobre la materia. La información proveniente de las demás funciones de INFIMANIZALES es administrada y conservada, observando las disposiciones propias del régimen de protección de datos personales, garantizando la privacidad de la información, previamente clasificada, salvó autorización del titular de esta para su divulgación.

Transferencia de la custodia de información de un empleado que se retira de INFIMANIZALES

Cuando un empleado se retira de INFIMANIZALES, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

Clasificación de la Información

Todos los activos deben estar claramente identificados, se debe elaborar y mantener un inventario de todos los activos importantes.

Eliminación segura de la Información en Medios Informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por INFIMANIZALES, antes de su entrega se les realizara un proceso de borrado seguro en la información.

Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción.

8.11 POLITICA DE BLOQUEO DE USO DE MEDIOS EXTRAIBLES DE ORIGEN FISICO

Esta política aplica a todos los empleados, contratistas y terceros que acceden a los sistemas y recursos de la organización.

Esta política tiene como objetivo minimizar los riesgos de seguridad asociados con el uso de medios extraíbles físicos en el entorno organizacional, protegiendo la confidencialidad, integridad y disponibilidad de la información. Esta medida refleja nuestro compromiso con las mejores prácticas de ciberseguridad, promoviendo un entorno tecnológico confiable y protegido para nuestra organización.

Restricción de Uso: Queda prohibido el uso de medios extraíbles de origen físico, como unidades USB, discos duros externos y DVDs, en los sistemas y dispositivos de la organización, a menos que se obtenga una autorización explícita por parte de la Jefe de Servicios Corporativos y el Profesional de TI.
Alternativas Seguras: Se fomenta el uso de soluciones alternativas seguras, como el intercambio de archivos a través de plataformas autorizadas y cifradas, para reducir la necesidad de utilizar medios extraíbles.

8.12 POLÍTICA DE COPIAS DE RESPALDO (BACKUP)

- **Período de almacenamiento de registros de auditoría**
  Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.
- **Tipo de datos a los que se les debe hacer backup y con qué frecuencia**
  A toda información sensible y software crítico de INFIMANIZALES residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

8.13 POLÍTICA DE CIBERSEGURIDAD

- **Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos**

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al Profesional de TI o a la Dirección de Ciberseguridad.

- **Detección de intrusos**

Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

- **Toda conexión externa debe estar protegida por el firewall**

Toda conexión a los servidores de INFIMANIZALES proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

- **Toda conexión hacia Internet debe pasar por el Firewall**

El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

- **Firewall debe correr sobre un computador dedicado o appliance**

Todo firewall debe correr sobre un computador dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

- **Inventario de conexiones**

Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo anterior se cumple con el diagrama de red.

- **El sistema interno de direccionamiento de red no debe ser público**

Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

- **Revisión periódica y reautorización de privilegios de usuarios**

Los privilegios otorgados a un usuario deben ser reevaluados una vez al año con el fin de analizar sí los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de sistemas con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios a la Profesional de TI.

- El antivirus siempre debe estar activo y actualizado
- Las Conexiones deben manejarse a través de una VPN adecuada, para proteger la intercepción de estas.
- Deberá ser informado al Profesional TI cualquier observación de comportamiento malicioso de sus equipos de trabajo
- Deberá ser informada al Profesional TI la recepción de correos electrónicos que cumpla uno o más de los siguientes criterios:
    - No estar suscrito a ese sitio web o aplicación y recibir mensajes que inciten a acceder a alguna URL
    - Recibir un mensaje de cobro de un servicio al cual no está suscrito
    - Mensajes de dudoso origen que gramaticalmente no posean un aspecto legitimo
    - Correos que solicitan en algún formulario o por el mismo correo datos personales
- Se deberán validar los siguientes aspectos en la recepción de correos electrónicos que no hayan sido solicitados por el usuario en sus operaciones naturales:
    - Nombre de la cuenta de correo de origen
    - Aspecto de la url la cual debe concordar con el portal oficial del servicio que le está contactando

9 SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

INFIMANIZALES definirá un "**Plan de Comunicación en Seguridad de la Información"** a través de su oficina de comunicación interna y externa y el área de tecnología donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad.

CAPACITACIONES EN SEGURIDAD

INFIMANIZALES a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información.

10 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 la misma. 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.

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

Infimanizales realizará revisiones periódicas al modelo de gestión de seguridad de la información. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el modelo de gestión de seguridad de la información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.

12 APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde la aprobación por el Consejo

Directivo. La revisión de esta política se hará en las siguientes

condiciones:

1. Por lo menos de forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.

13 REFERENCIAS NORMATIVAS

Para la formulación, implementación y mejora continua de la Política General de Seguridad de la Información y Ciberseguridad, Infimanizales se apoya en las siguientes referencias normativas:

- **ISO/IEC 27001:2022** - Tecnologías de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. Esta norma internacional proporciona un marco para establecer, implementar, mantener y mejorar continuamente un modelo de gestión de seguridad de la información.
- **Ley 1581 de 2012 (Ley de Protección de Datos Personales en Colombia)**: Por la cual se dictan disposiciones generales para la protección de datos personales. Esta ley establece el régimen general de protección de datos personales en Colombia, garantizando el derecho de habeas data.
- **Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones)**: En particular, lo referente a la Estrategia de Gobierno Digital (anteriormente Gobierno en Línea) y los lineamientos de seguridad y privacidad de la información para las entidades públicas.
- **CONPES 3701 de 2011 (Política Nacional de Ciberseguridad y Ciberdefensa)**: Documento que establece los lineamientos de política pública para fortalecer la ciberseguridad y la ciberdefensa en Colombia, buscando minimizar el nivel de riesgo ante amenazas y incidentes cibernéticos.
- **Circular Externa 007 de 2018 de la Superintendencia de Industria y Comercio (SIC)**: Imparte instrucciones sobre la implementación del principio de responsabilidad demostrada (Accountability) y la gestión de riesgos en el tratamiento de datos personales.
- **Guías y Modelos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**: Referidas al Modelo de Seguridad y Privacidad de la Información (MSPI) para entidades públicas, que proporcionan directrices y herramientas para la implementación de políticas y controles de seguridad.