CONTENIDO

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

1. INTRODUCCIÓN

Uno de los insumos principales para la gestión, el control y la toma de decisiones del INSTITUTO DE FINANCIAMIENTO, PROMOCION Y DESARROLLO DE CALDAS – INFI, es la información que la entidad genera, almacena y administra, por tanto, es primordial establecer políticas claras y contundentes para su recolección, almacenamiento, administración y entrega.

De igual modo, la tecnología es el recurso clave para el buen manejo de dicho activo de la información, la cual se desarrolla, crece y evoluciona de manera rápida y constante, requiriendo establecer lineamientos de seguridad que minimicen la alteración, fuga o indisponibilidad de la información durante las etapas de fabricación, diseño e implementación de las herramientas, incluso durante el uso de estas. Por esta razón el Manual de Políticas de seguridad de la información y ciberseguridad busca i) definir lineamientos, controles, roles perfiles y responsabilidades para la gestión de la información, y ii) gestionar al máximo las amenazas a los sistemas de información, control y gestión y iii) limitar la capacidad de los atacantes para violentar y dar un mal uso a la información.

Por lo anterior, la entidad consolida en el presente documento las políticas en seguridad de la información para garantizar la confidencialidad, integridad, disponibilidad, no repudio y cumplimiento de las obligaciones en materia de tratamiento de datos personales, el buen uso y cuidado de la información y el funcionamiento adecuado de los recursos tecnológicos puestos a disposición de los usuarios.

Dado que la entidad cuenta con un Sistema Integrado de Planeación y Gestión, este documento hace parte integral del mismo, complementando los procedimientos y manuales vigentes del proceso de Tecnologías de la Información, como instrumento para orientar la implementación del Manual de Políticas de Seguridad de la información y ciberseguridad y sensibilizar a los servidores públicos y contratistas acerca de la importancia del buen manejo de la información.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

2. OBJETIVOS

Objetivo general

La declaración del Manual de Políticas de Seguridad de la Información y ciberseguridad Institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión.
El Manual de Políticas de seguridad de la información y ciberseguridad se consolida a través de los procedimientos, guías, instructivos, publicaciones, controles tecnológicos y administrativos, así como en la asignación de roles y responsabilidades.

Objetivos específicos

- Garantizar la confidencialidad e integridad de la información crítica de la entidad e información sensible de terceros para que esta sea solo accesible por las personas autorizadas protegiéndolos de la divulgación no autorizada o modificación no intencionada o fraudulenta.
- Asegurar la disponibilidad y la continuidad de la operación en los procesos críticos de la entidad que están soportados en la infraestructura tecnológica.
- Conservar la confianza de los ciudadanos y contar con el compromiso de los funcionarios, contratistas y demás personal relacionado con el Instituto respecto al adecuado manejo y protección de la información que es gestionada y resguardada por INFICALDAS.
- Generar conciencia entre los funcionarios, contratistas y terceros que tenga vínculos con INFICALDAS sobre el uso adecuado de los activos de información puestos a su disposición para la realización de sus funciones y actividades diarias, garantizando la confidencialidad, privacidad e integridad de la información para identificar, reportar y gestionar los riesgos de seguridad digital mediante acciones de sensibilización y capacitación.
- Implementar, mantener y mejorar anualmente el conjunto de controles de seguridad de la información recomendados por el Modelo de seguridad y privacidad de la información - MSPI mediante la aplicación del Plan de

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

Seguridad y privacidad de la información institucional, para mantener en niveles aceptables los riesgos residuales de seguridad digital.

- Fortalecer continuamente la función institucional mediante la implementación, difusión y mejoramiento continuo del MSPI (Modelo de seguridad y privacidad de la información) para mejorar la confianza de las partes interesadas en el compromiso institucional de preservar adecuadamente la confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de la entidad
- Dar cumplimiento a los lineamientos establecidos por los diversos entes como el MinTIC con su política de Gobierno Digital, la Superintendencia Financiera de Colombia con la circular externa 007 de 2018 y la Función Pública con su Modelo Integrado de Planeación y Gestión (MIPG), en todo lo que esté relacionado con Seguridad de la Información.

3. ALCANCE

El Manual de políticas de seguridad de la información y la ciberseguridad cubre todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas, proveedores, terceros y visitantes que laboren o tengan relación con INFICALDAS, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

Igualmente se aplican a todos los datos, información e infraestructura en propiedad de la entidad los cuales son considerados confidenciales y/o críticos para los objetivos del negocio, los cuales pueden estar almacenados en forma física y/o en digital, durante su ciclo de vida: creación, distribución, almacenamiento y/o eliminación.

4. MARCO NORMATIVO Y/O LEGAL

Norma	vínculo	Título
Ley 1581 de 2012	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981	Protección de datos personales

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

Ley 1712 de 2014	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
Decreto 2573 de 2014	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60596	Estrategia de Gobierno en línea
Decreto 1078 de 2015 (Actualización diciembre 2023)	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 1008 de 2018	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902	establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Conpes 3595 de 2020	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf	Política Nacional de Confianza y Seguridad Digital
Resolución 500 de 2021	https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf	Lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Resolución746 de 2022	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=226870	Adiciona lineamientos y fortalece el Modelo de seguridad y privacidad de la información, sin derogar la Resolución 500 de 2021

Resolución 2277 de 2025	https://www.mintic.gov.co/portal/715/articles-403045_recurso_2.pdf	actualizó el Anexo 1 de la Resolución 500 de 2021 y derogó otras disposiciones relacionadas con la materia.
Decreto 338 de 2022	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866	Lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital.
Decreto 767 de 2022	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766	Lineamientos generales de la Política de Gobierno Digital. estableció los nuevos lineamientos generales de la Política de Gobierno Digital y, en la práctica, derogó y reemplazó las disposiciones del Decreto 1008 de 2018 que se referían a esta política.
Resolución 460 de 2022	https://www.mintic.gov.co/portal/715/articles-179710_recurso_2.pdf	Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital
PARTE I, TÍTULO IV, CAPÍTULO V	https://www.superfinanciera.gov.co/publicaciones/10083444/normativanormativa-generalcircular-basica-juridica-ce-parte-i-instrucciones-generales-aplicables-a-las-entidades-vigiladas-10083444/	Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad
Resolución 2710 de 2017	https://gobiernodigital.mintic.gov.co/692/articles-176070_recurso_2.pdf	Lineamientos para la adopción del protocolo IPv6
Decreto 1126 de 2021	https://gobiernodigital.mintic.gov.co/692/articles-176070_recurso_1.pdf	Modificación de la Resolución 2710 de 2017: Lineamientos para la adopción del protocolo IPv6

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

5. DEFINICIONES

Activo: Todo lo que tiene valor para la entidad: Información, software o programa de cómputo, hardware o equipos de cómputo, servicios.

Activo de Información: recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación).

Almacenamiento: Es un dispositivo que permite conservar los datos y la información de manera independiente y que permite presentarla a diversos sistemas.

Autenticación: mecanismo técnico que permite garantizar que una persona o entidad es la correcta.

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.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

Datos personales sensibles: aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

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 - ERP (en inglés 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.
Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Firewall perimetral: Se define como un elemento o sistema que permite proteger unos perímetros en instalaciones sensibles de ser atacadas por intrusos.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, comprende la identificación, evaluación y el tratamiento de riesgos

IAS Solutions: Nombre de la herramienta ERP adquirida por el Instituto para apoyar los procesos financieros, contables, de nómina, recursos humanos y operacionales.

Impacto: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

Máquina virtual: Es un software que simula un sistema de computación y puede ejecutar programas como si fuese una computadora real.

Monitoreo: Consiste en la observación de uno o más parámetros para detectar eventuales anomalías.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Red de Área Local (LAN): Es la interconexión de varias Computadoras y Periféricos.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

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)

Calle 21 No. 23 – 22 Edificio Seguros Atlas,
pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

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.

6. ROLES Y RESPONSABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

Alta Gerencia	• La revisión y aprobación de la Políticas de Seguridad y Privacidad de la Información • Asegurar los recursos necesarios para implementar y mantener el Sistema de gestión de Seguridad de la Información • Velar por el cumplimiento de los lineamientos establecidos en esta Política General de Seguridad de la Información y el Manual de Políticas de Seguridad y privacidad de la Información. • Apoyar la estrategia institucional en seguridad de la información y ciberseguridad.
Comité Institucional de Gestión y Desempeño	• Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información • Velar por la implementación del Sistema de Gestión de Seguridad de la Información • Revisar y aprobar el Manual de Políticas de Seguridad de la Información y ciberseguridad y los

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

	lineamientos asociados, asegurando que reflejen los controles necesarios para mitigar los riesgos informáticos de INFICALDAS • Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información • Aprobar acciones y mejores prácticas que se orienten en la implementación del Modelo de Seguridad y Privacidad de la Información. • Verificar el cumplimiento de las políticas de seguridad y privacidad de la información de INFICALDAS • Garantizar la divulgación de las políticas y normas de seguridad de la Información a todos los funcionarios, contratistas, proveedores y clientes • Presidir las reuniones requeridas para la toma de decisiones que permitan la gestión y mitigación de riesgos críticos de seguridad de la información • Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información
Oficina de Control interno	• La Oficina de control interno debe realizar auditorías internas para evaluar el cumplimiento del Modelo de Seguridad y Privacidad de la Información. • La Oficina de control interno debe realizar auditorías internas para evaluar el cumplimiento del Sistema de gestión de seguridad de la información • La Oficina de Control interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Modelo de Seguridad y Privacidad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades. • La Oficina de Control interno debe informar a las áreas responsables los hallazgos de las auditorías.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

Oficina jurídica	• Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso. • Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.
Secretaria General	• Velar por el cumplimiento legal del Manual de Políticas de Seguridad de la Información y ciberseguridad en la entidad.
Oficina de sistemas	• Identificar los activos de información de los cuales es responsable y Encargado. • Asesorar a las otras dependencias en los procesos de identificación e implementación de controles. • Implementar y mantener todas las medidas necesarias para proteger nuestros datos, siguiendo las directrices establecidas en las políticas de seguridad y privacidad de la información. • Apoyar al responsable de Seguridad de la Información (o quien cumpla con estas responsabilidades dentro de la Entidad) y del Oficial de Protección de Datos en los temas de su competencia.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

	• Realizar la gestión constante de las tecnologías de la información para dar cumplimiento a la seguridad y privacidad de la información. • Dar cumplimiento a la política de seguridad y privacidad de la información cuando se considere pertinente por cambios normativos, necesidades del servicio, cambios de procesos y procedimientos internos de la entidad y riesgos de seguridad detectados que así lo ameriten • Fomentar una cultura de seguridad de la información mediante actividades de capacitación y sensibilización a todo el personal de la entidad. • Definir, elaborar e implementar las políticas, procedimientos, formatos y demás documentos que sean de su competencia para la operación del modelo de seguridad y privacidad de la información - MSPI. • Liderar la definición de parámetros para el establecimiento de hardware, software y comunicaciones, así como de la arquitectura tecnológica. Sin embargo, la administración de la información en la fase de registro tanto en aplicativos como bases de datos es responsabilidad de cada área, con el fin de evitar modificación no autorizada o intencional o el uso indebido de los activos de la organización • Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de INFICALDAS. • Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información de INFICALDAS. • Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Entidad. •

Responsable de seguridad de la información (Profesional Especializado Sistemas)	• Definir y gestionar la normativa de seguridad y privacidad de la información y seguridad digital. • Participar y reportar la gestión de seguridad y privacidad de la información en los comités institucionales relevantes. • Promover la concientización, capacitación y mejora continua en materia de seguridad y privacidad de la información para todo el personal de la entidad. • Definir, socializar e implementar los procedimientos relacionados con la gestión de seguridad y privacidad de la información al interior de la entidad. • Apoyar activamente en la identificación, evaluación y mitigación de los riesgos de seguridad de la información en la entidad. • Evaluar y verificar e informar semestral la implementación y efectividad de los controles de seguridad de la información. • Coordinar la implementación de acciones preventivas y correctivas sobre la gestión de la seguridad de la información con los respectivos responsables, de acuerdo con los resultados de las auditorías internas o externas. • Asesorar y acompañar a las diferentes áreas de la entidad en la gestión de activos de información, riesgos, implementación de controles y definición de actividades de planes de tratamiento para mejorar la postura de seguridad en la entidad.
Oficial de cumplimiento de protección de datos personales	• Analizar y comprobar la conformidad de la normativa de las actividades de tratamiento • Recabar información para determinar las actividades de tratamiento • Servir de enlace coordinar con las demás áreas de la organización para asegurar una implementación transversal del programa integral de gestión de datos personales • Registrar las bases de datos de la organización en el registro nacional de bases de datos y analizar el

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

	reporte atendiendo a las instrucciones que sobre el particular emita la superintendencia de industria y comercio cuando aplique • Analizar la responsabilidad de cada cargo de la organización para diseñar un programa de entrenamiento o protección de datos personales específico para cada uno de ellos • Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización • Coordinar la definición e implementación de los controles del que apunten a la gestión de datos personales programa integral de gestión de datos personales • Supervisar y asegurar que se implementen medidas de seguridad adecuadas para proteger los datos personales, así como Garantizar su confidencialidad, integridad y disponibilidad • Evaluar y gestionar los riesgos asociados al tratamiento de datos personales y proponer las medidas necesarias para mitigar dichos riesgos
Oficina de Riesgos	• Definir los instrumentos, metodologías y procedimientos para gestionar de manera efectiva los riesgos de seguridad de la información, acorde con los lineamientos de la Función Pública y alineados con las mejores prácticas. • Monitorear los riesgos asociados a la de seguridad de la información y proponer las medidas necesarias para mitigar dichos riesgos. • Proporcional apoyo a la Gerencia y lideres de áreas y/o procesos sobre los riesgos de seguridad de la información para la toma de decisiones. • Colaborar con el diseño del Manual de política de seguridad y privacidad de la información.

Líder proceso de Gestión del Talento humano:	• Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información. • Implementar procesos de selección que incluyan verificación de antecedentes y evaluaciones de confiabilidad con criterios de seguridad de la información. • Garantizar la firma de acuerdos de confidencialidad y compromiso con la protección de datos desde la vinculación. • Integrar el entrenamiento en seguridad de la información dentro del proceso de inducción y reinducción del personal • Apoyar en la implementación del plan de concientización y sensibilización en seguridad y privacidad de la información. •
Propietarios de la información	Son propietarios de la información cada uno de los líderes de área donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades. • Valorar y clasificar el activo de información según su sensibilidad y criticidad para establecer controles de acceso para protegerla, garantizando que solo el personal autorizado pueda consultarla, modificarla o crearla. • Determinar en conjunto con Tecnico Administrativo de Gestión Documental, los tiempos de retención y las medidas de protección de la información, alineados con las normativas vigentes. • Almacenar el activo de información en los recursos proporcionados por la entidad. La Oficina de sistemas no se responsabiliza por la pérdida de datos causada por fallas del hardware, software o errores humanos.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

	• Participar en el control y mitigación de los riesgos de seguridad de la información a los cuales se encuentren expuestos los datos dentro de su proceso. • Realizar evaluaciones periódicas de los riesgos asociados a la información y de la efectividad de los controles de acceso. Comunicar de manera oportuna cualquier hallazgo o mejora a los usuarios y responsables de la información
Funcionarios, contratistas y terceros usuarios de la información	• Todos los colaboradores que realicen labores para INFICALDAS tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad y privacidad de la información. • Rendir cuentas por el uso y protección de tal información, mientras que esté bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio, de la misma manera proteger la información a la cual acceden y procesen, para evitar su pérdida, alteración, destrucción o uso indebido. • Aplicar y el cumplir con el presente Manual de Política.

7. LINEAMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD INSTITUCIONAL

7.1 Seguridad de los recursos humanos

Dentro del proceso de selección del personal ya sea de planta o por prestación de servicios (contratistas) se deben verificar antecedentes disciplinarios, judiciales y fiscales, firmar acuerdos de confidencial protección de datos personales, así mismo durante su periodo contractual con INFICALDAS se deben hacer inducciones y reinducciones para llevar a cabo la socialización del Manual de Política de seguridad y privacidad de la información y política protección de datos personales, así como capacitación en temas relacionados con la seguridad de la información y

ciberseguridad; Sí ocurre un cambio de empleo dentro de la misma institución se debe informar a todo el personal sobre el cambio, y al finalizar el contrato se deben revocar los permisos y realizar la devolución de los activos una vez finalizada la relación contractual o al ocurrir un cambio de empleo y se debe diligenciar **1100-F-74 ACTA DE ENTREGA FUNCIONARIO.**

7.2 Gestión de activos

Toda información ya sea física o digital que se produzca al interior de INFICALDAS por cada uno de sus funcionarios bien sea de planta, contratistas o proveedores y que hagan uso de los recursos tecnológicos dispuestos por la entidad, se catalogan como activos de información propiedad de INFICALDAS, para dicho control se establece la **POLÍTICA DE PROPIEDAD INTELECTUAL.**

Toda la información o activos de información serán identificados y clasificados de acuerdo con las directrices y lineamientos orientados desde el Archivo General de la Nación – AGN y los procedimientos internos de la entidad, para lo cual se puede hacer referencia al **1140-F-12 Inventario y Clasificación de Activos de información** que se encuentra publicado en la página web oficial de INFICALDAS y para para los activos tecnológicos de igual manera se clasifican de acuerdo a su valor e importancia para determinar su nivel de protección, este inventario se encuentra en **1500-F-18 INVENTARIO DE EQUIPOS DE COMPUTO – ADMINISTRACION DE LA PLATAFORMA TECNOLOGICA**

Retención y destrucción final de la información

Se deben establecer los procedimientos y directrices para el manejo de la información durante su ciclo de vida, es decir desde su creación hasta su eliminación dando así cumplimiento a ley 1581 de 2012 (Protección de datos) y la Ley 594 de 2000 (Ley General de Archivos).

La directriz debe incluir los plazos de retención, la conservación segura y la eliminación final y definitiva de los datos e información, tanto en formato físico como digital. Se debe consultar el Programa de retención documental de INFICALDAS (PRD).

Calle 21 No. 23 – 22 Edificio Seguros Atlas,
pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

Inventario y propiedad de los activos informáticos.

Se deben identificar y clasificar los activos de información que pueden ser considerados como sensibles o críticos para INFICALDAS y que deben ser protegidos con las mejores prácticas de seguridad de la información, así mismo, asignar responsabilidades claras para esta protección, teniendo en cuenta los lineamientos orientados por MINTIC para el inventario de activos de información que puede ser consultada en **1140-F-12 Inventario y Clasificación de Activos de información**

Mantenimiento de Equipos tecnológicos:

Se debe asegurar que todos los dispositivos de la entidad funcionen de manera óptima y estén protegidos de vulnerabilidades, para esto el Oficina de sistemas coordinara el servicio de mantenimiento preventivo o correctivo de los equipos de cómputo de la entidad, de acuerdo con el **1500-D-2 CRONOGRAMA DE MANTENIMIENTO INFRAESTRUCTURA TECNOLOGICA** El mantenimiento preventivo se ejecuta por el personal a cargo de soporte técnico dentro de la entidad o en caso contrario bajo el contrato con proveedor especializado vigente y estos deben ser registrados en el formato de **1500-F-15 REGISTRO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS DE CÓMPUTO** o conservar la evidencia con el soporte de mantenimiento realizado por los proveedores. El mantenimiento correctivo se realiza a demanda de acuerdo con las solicitudes de los funcionarios.

Pérdida y/o daño de dispositivos:

El funcionario que tenga bajo su responsabilidad o se le haya asignado algún equipo de cómputo para la ejecución de sus funciones, será responsable de su uso y custodia; en consecuencia, atenderá lo acordado en la **1500-F-02 ASIGNACIÓN DE EQUIPO DE COMPUTO,** conforme al acuerdo y cumplimiento del manifiesto de este documento.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

7.3 Controles de acceso

Se deberán asumir responsabilidades sobre los accesos a la información ya sea de manera física o digital para mitigar los riesgos asociados a accesos no autorizados dando cumplimiento a la confidencialidad, integridad y disponibilidad de la información.

Dentro del **1500-D-05 LINEAMIENTO DE CONTROLES DE ACCESO** se especifican los principios para tener en cuenta para una óptima gestión de los accesos para: Usuarios con privilegios de administrador, usuarios nuevos y retiro de usuarios, Accesos remotos, realizando la solicitud de accesos o revocación de estos por medio de los canales autorizados para formalizar la solicitud.

7.4 Seguridad física y del entorno

Se deben adoptar las medidas necesarias que controlen los accesos físicos a las instalaciones y áreas seguras para mitigar los riesgos asociados a la afectación de la integridad y disponibilidad de la información.

Todas las áreas destinadas al procesamiento de la información según los niveles de clasificación establecidos por la entidad deben contar con protecciones físicas o perímetros de seguridad (tales como paredes, puertas de acceso controlado y personal a la entrada de los diferentes pisos), éstas deben cubrir con las necesidades en cuanto a: controles de entradas físicas, seguridad de oficinas, espacios y medios, protección contra amenazas externas y ambientales. Dentro del documento: **1500-D-08 LINEAMIENTO DE SEGURIDAD FÍSICA Y AMBIENTAL**, se describen las condiciones para mantener áreas seguras.

7.5 Seguridad en las operaciones

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación de la entidad. INFICALDAS planea, gestiona, respalda y monitorea la infraestructura tecnológica con el fin de establecer los controles de seguridad pertinentes que permitan proteger la confidencialidad, integridad y

disponibilidad de la información siguiendo los lineamientos referenciados en los procedimientos establecidos para el SGSI.

- **Protección Malware**: Tener instalado licenciamiento de software Antivirus y antimalware en todos los equipos de cómputo de la entidad para brindar protección de software malicioso como virus, troyanos, spyware y Ransomware y demas disposiciones descritos en **1500-D-04 LINEAMIENTOS CONTRA VIRUS O SOFTWARE MALICIOSO**

- **Copias de seguridad:** Realizar las copias de seguridad de manera periódica para toda la información crítica y bases de datos. Se deberá mantener copias de seguridad de los equipos de cómputo, servidores críticos de las entidad y servidores de datos, de manera recurrente y deberán permanecer actualizadas y sincronizadas con el equipo de cómputo, además de hacer uso de software de gestión para copias de seguridad para la automatización de esta actividad. Para esto se cuenta con el **1500-F-07 PROCEDIMIENTO PARA REALIZAR Y RESTAURAR BACKUPS** contiene la especificación de la ejecución de las copias de seguridad de la entidad.

- **Control de instalación de software**: Se deben describir los lineamientos para el uso e instalación de software en los equipos de cómputo de los funcionarios para garantizar la seguridad de la información en INFICALDAS, por esta razón es necesario contar con restricciones frente a la instalación de software**.** Es necesario hacer uso de los medios autorizados para realizar la solicitud de instalación de software tal como se indica en **1500-F-02 ASIGNACION DE EQUIPO DE COMPUTO V4**

- **Gestión del cambio:** Se debe establecer un procedimiento formal para definir el control de las solicitudes de cambios de tecnología para evaluar, aprobar e implementar cualquier cambio en las plataformas de infraestructura tecnológica y sistemas de información. Se debe hacer uso del **1500-F-04 FORMATO SOLICITUD CAMBIOS** y tener en cuenta el **1500-PR-05 PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS TECNOLÓGICOS**

- **Gestión de la capacidad:** Hacer la gestión y seguimiento de la capacidad de todos los activos críticos de la entidad para garantizar su disponibilidad y rendimiento óptimo de la infraestructura tecnológica y así prevenir interrupciones del servicio o la degradación de configuraciones de seguridad.

El Oficina de sistemas deberá tener en cuenta esta información para gestionar la capacidad y asegurar los recursos de hardware, software y red para proyectar demandas futuras en almacenamiento, rendimiento de los sistemas de información críticos, eliminación de datos innecesarios, obsolescencia tecnológica, entre otros.

- **Registro y monitoreo de eventos:** Realizar el seguimiento a los registros de actividad en la red recopilando y analizando la información para la detección temprana de eventos que amenacen la seguridad de la información de INFICALDAS, por medio de las herramientas especializadas o recopilando información de registros de plataformas de seguridad para analizar y tomar decisiones de mejora o cambios en las configuraciones de los sistemas que puedan estar afectados de acuerdo como se indica en **1500-PR-09 PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES**. Así mismo se realiza la revisión del funcionamiento de los diferentes servidores físicos y virtuales para conocer cuál es el estado de funcionalidad y estado de sistemas operativos y software de operación con control en **1500-F-18 CHECKLIST DIARIO DE REVISIÓN DE INFRAESTRUCTURA INFICALDAS**

- **Trabajo remoto:** El área de recursos humanos debe establecer las directrices y condiciones de trabajo asegurando el cumplimiento de los acuerdos de confidencialidad, el área de Salud y Seguridad en el Trabajo – SST de definir las condiciones seguras de trabajo, y la oficina de sistemas debe proporcionar el soporte y las herramientas necesarias para facilitar el acceso a las aplicaciones e información por medio de conexiones seguras (VPN) desde el lugar destinado para trabajo.

7.6 Seguridad de las comunicaciones

Se deben establecer controles para el acceso lógico y protección de las redes de INFICALDAS, con el fin de asegurar y cumplir con el servicio de comunicaciones que sean establecidos para el acceso a los servicios tecnológicos y que deberán ser acordados con la Gerencia.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

INFICALDAS definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la confidencialidad e integridad de la información.

Se debe establecer lineamientos para el uso y acceso apropiado de internet y correo electrónico en donde se establezcan las directrices para la utilización de estas herramientas como uso exclusivo para el desempeño de sus funciones y cargo en el Instituto y no para propósitos personales, garantizando la disponibilidad del acceso.

7.7 Adquisición, desarrollo y mantenimiento de Software

Se debe describir como se realiza la gestión de la seguridad de la información en los sistemas adquiridos con un tercero, verificando que se garantice la confidencialidad, integridad y disponibilidad de la información de la entidad. Todos los contratos con proveedores de software deben incluir cláusulas de seguridad y privacidad de la información que especifiquen de manera clara las responsabilidades de cada parte y los controles que el proveedor debe implementar para proteger la información de INFICALDAS de acuerdo con **1500-D-07 LINEAMIENTO DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE.**

7.8 Relación con los proveedores

INFICALDAS cuenta con procedimientos para la selección y evaluación de los proveedores, estos lineamientos están directamente relacionados con la Función Pública, dada la naturaleza de la entidad. Para este caso, se entenderá como proveedores aquellas personas naturales o jurídicas que presten servicios de tecnología (servicios, consultoría, implementaciones) y que dentro de sus labores tenga acceso a la información de la entidad: estos, deberán dar cumplimiento a los acuerdos contractuales que se orienten de acuerdo con los servicios contratados y a su vez deben firmar el **1500-F-12 COMPROMISOS DE CONFIDENCIALIDAD-Y-NO DIVULGACION DE LA INFORMACION** para garantizar la reserva, integridad y uso adecuado de la información a la que se tenga acceso en desarrollo de su relación con INFICALDAS.

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

NOTA: Si dado el caso que se realicen pruebas o muestra de servicios y se requiera acceder a la información de la entidad sin tener un contrato, igualmente el profesional o empresa a cargo de la actividad, debe formar el compromiso de confidencialidad.

7.9 Administración de la información y propiedad intelectual

Cada usuario y funcionario son responsables de los mecanismos de control de acceso a la información que tiene acceso y genera en el cumplimiento de sus funciones en la entidad. Igualmente, la información generada por los funcionarios o contratistas en el desarrollo de sus funciones y objeto del contrato es propiedad de la entidad.

Todo funcionario de INFICALDAS al hacer uso de los recursos informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje e igualmente de la información que reciba para el cumplimiento de sus funciones.

Para dar cumplimiento, se ha estipulado la **POLITICA DE PROPIEDAD INTELCTUAL**

7.10 Escritorio y pantalla limpia

Se deberán plantear los lineamientos para la protección de los activos físicos y digitales, que haya sido clasificados por la entidad como sensible o confidencial, estas reglas deben ser atendidas por todos los funcionarios con el fin de prevenir accesos no autorizados, robo, perdida o daño de dichos datos e información, cuando los espacios de trabajo no se encuentran supervisados. En el **1500-D-06 LINEAMIENTO DE ESCRITORIO Y PANTALLA LIMPIA** se pueden consultar estas reglas a seguir.

8. PLAN DE CONTINGENCIA ANTE DESASTRES

Se debe contemplar un plan de contingencia con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión

crítica y las operaciones informáticas que soportan los servicios críticos de la Institución, ante el evento de un incidente o catástrofe parcial y/o total se hace necesario de la disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica del negocio en los tiempos esperados y acordados

Estos deben prepararse de cara a futuros sucesos y los funcionarios deben ser conocedores y tener claro cuál es el proceso para seguir, dicho procedimiento está definido en el **1500-P-03 PLAN DE CONTINGENCIAS Y CONTINUIDAD**

9. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Se deberá contar con un plan de gestión de incidentes de INFICALDAS que defina una hoja de ruta de los procedimientos para identificar, gestionar, contener y recuperarse de un incidente de seguridad y así minimizar el daño e impacto ante un incidente.

Los funcionarios deben ser conocedores y tener claro cuál es el proceso para seguir, dicho procedimiento está definido en el **1500-PR-09 PROCEDIMIENTO PARA LA GESTION DE INCIDENTES**

10. CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

El Oficina de sistemas tiene como una de sus funciones la de proponer, revisar y capacitar en el cumplimiento de políticas y lineamientos de seguridad, que garanticen acciones preventivas y correctivas para salvaguardar equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

El Manual de Políticas de Seguridad y privacidad de la información son de obligatorio cumplimiento para los funcionarios, contratistas y terceros que tienen vínculos con la entidad y para ambos genera consecuencias ya sea disciplinarias y legales en caso de contratos de servicio.

El no acatamiento de las políticas aquí descritas puede hacer vulnerable el sistema organizacional exponiendo a la empresa a pérdidas financieras, de imagen y credibilidad ante sus clientes, socios y entes reguladores, por esto el cabal cumplimiento de estas hace parte de las responsabilidades de cada uno de los empleados y/o usuarios de los recursos informáticos que interactúan con los sistemas de información de la empresa.

Dado el caso en el que el Manual de Políticas de Seguridad y privacidad de la información no se cumplan, el Instituto tomará las medidas disciplinarias y/o legales que correspondan, pudiendo ser causal de terminación y/o cancelación de contratos laborales y/o comerciales (cualquier vínculo contractual) al que dé lugar, exigiendo la indemnización asociada al daño o perjuicio del que se vio afectada.

11. ACTUALIZACIONES Y DIVULGACION DEL MANUAL DE POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Manual de Políticas de seguridad de la información y ciberseguridad se revisan y actualizan anualmente con el fin de garantizar su vigencia y pertinencia para el cumplimiento de los objetivos institucionales. De la misma forma se revisan cuando se presenten situaciones como: cambios organizacionales, culturales o del entorno interno o externo, cambios operativos o normativos que afecten a la entidad, cuando ocurren incidentes de seguridad de la información que obliguen al fortalecimiento de controles o lineamientos, o de acuerdo con los resultados de la gestión de riesgos institucionales. De igual manera, se implementan mediante lineamientos, procedimientos o controles que especifican los detalles técnicos de su operación.

Los cambios realizados en el presente documento serán presentados al comité de gestión y desempeño, para luego ser llevados a Consejo Directivo para su aprobación.

Es responsabilidad de la entidad mantener disponible el presente documento para que sea de acceso público a todos los funcionarios de la entidad y a externos como partes interesadas, de igual manera la Oficina de sistemas con el apoyo de comunicaciones de la entidad se encargará de realizar la divulgación y socialización. Es responsabilidad de cada uno de los colaboradores de INFICALDAS la lectura y conocimiento del Manual de Políticas de seguridad y privacidad de la información más reciente.

12. PROCESOS DISCIPLINARIOS

El incumplimiento al Manual de las políticas de seguridad de la información y ciberseguridad y los lineamientos descritos en este documento se trata mediante el procedimiento de incidentes de seguridad de la información, de acuerdo con la naturaleza del incidente y los resultados de su tratamiento e investigación y los responsables de los procesos institucionales, evalúan la necesidad de adelantar procesos disciplinarios o legales.

La entidad debe firmar el Compromiso de confidencialidad y no divulgación de la información con todos los funcionarios, persona jurídica o natural que tenga acceso a los datos e información de INFICALDAS.

Cuando los incidentes de seguridad de la información correspondan a delitos informáticos calificados como tales por la normatividad vigente, el equipo de riesgos formulará la recomendación a la Secretaria General de la entidad para iniciar las acciones legales ante la respectiva autoridad competente. Cuando el incidente de seguridad de la información no esté calificado como un delito informático, las acciones disciplinarias o legales se adelantan de acuerdo con la competencia del código de procedimiento disciplinario en el caso de servidores públicos o mediante los criterios definidos en los contratos de prestación de servicios en el caso de contratistas.

Los servidores públicos de INFI que ocasionen algún incidente de seguridad de la información por realizar acciones que contravengan o incumplan alguna de las disposiciones descritas en el presente documento, serán reportados por correo electrónico al Jefe inmediato, al Jefe de la Oficina Asesora de Planeación, al Coordinador del Grupo de Gestión Humana y Jefe de la Oficina de Control Interno, para la revisión del caso y la adopción de las medidas respectivas de acuerdo con las políticas aplicables en la entidad.

Respecto a los contratistas, estos serán reportados al supervisor del contrato, para la revisión del caso y tomar las medidas respectivas.

Calle 21 No. 23 – 22 Edificio Seguros Atlas,
pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64

@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co

PROYECTÓ	John Jairo Giraldo Villa KAVANTIK	**REVISÓ Y APROBÓ**	Consejo Directivo
CARGO	Profesional Especializado Sistemas Contratista KAVANTIC SAS	**Acuerdo**	15
FECHA	20/11/2025	**FECHA**	26/11/2025

Calle 21 No. 23 – 22 Edificio Seguros Atlas, pisos 3 y 4 – Manizales, Caldas
PBX: +57 (606) 898 30 64
@Inficaldas
atencionalciudadano@inficaldas.gov.co
www.inficaldas.gov.co