



**MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN
(SISTEMAS DE INFORMACIÓN)**

FONDO DE FOMENTO PANELERO

Versión No. 04 año 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 2 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

INDICE

1. INTRODUCCIÓN	4
1.1. Objetivo General	4
1.2. Objetivos Específicos	4
1.3. Alcance	5
1.4. Utilización	5
1.5. Actualización	5
1.6. Vigencia	6
2. DEFINICIONES	7
3. POLÍTICAS Y LINEAMIENTOS	10
3.1. Política para los activos de la información	10
3.1.1. Procedimientos de seguridad	10
3.2. Política de redes sociales	17
3.3. Políticas en el proceso de vinculación o desvinculación del personal	17
3.4. Política de contraseñas seguras	17
3.5. Política de escritorio limpio	18
3.6. Política de uso de Internet	18
3.7. Política de equipos personales	18
3.8. Política de uso de dispositivos móviles (institucionales y no institucionales)	19
3.8.1. Alcance	19
3.8.2. Dispositivos móviles institucionales	19
3.8.3. Dispositivos móviles no institucionales	19
3.8.4. Transferencia y manejo de información	20
3.8.5. Responsabilidades del usuario	20
3.9. Política de medios extraíbles	20
3.10. Política de conexión remota a los equipos	20
3.10.1. Alcance	20
3.10.2. Condiciones de acceso remoto	21
3.10.3. Controles de seguridad	21

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 3 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

3.10.4.	Restricciones	21
3.10.5.	Responsabilidades	21
3.10.6.	Monitoreo y control	21
3.11.	Política de uso de correo electrónico	22
3.12.	Política de control de acceso a los recursos de la Red	23
3.13.	Política de creación y administración de usuarios y roles, y gestión de información física	23
3.14.	Política de uso de equipos corporativos.	24
3.15.	Política para administradores y funcionarios de tecnología	24
3.16.	Política de gestión de incidentes de seguridad de la información	24
3.16.1.	Clasificación de los incidentes de seguridad	25
3.16.2.	Responsabilidades	25
3.16.3.	Tiempos de respuesta	25
3.16.4.	Procedimiento de gestión de incidentes	25
3.16.5.	Procedimiento de notificación	26
3.16.6.	Seguimiento y mejora continua	26
3.17.	Plan de respuesta a emergencias en caso de pérdida de información	26
3.18.	Planificación de la continuidad del negocio	27
CONTROL DE CAMBIOS		28

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

AREA SISTEMAS DE INFORMACIÓN

FONDO DE FOMENTO PANELERO

VERSIÓN:03

Página 4 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

1. INTRODUCCIÓN

El Fondo de Fomento Panelero, ha consolidado la seguridad de la información como un componente estratégico para garantizar la transparencia, la eficiencia y la confianza en todas sus actividades institucionales, ya que la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes.

Este **Manual Interno de Seguridad de la Información** establece las definiciones, lineamientos, políticas y buenas prácticas necesarias para proteger los activos que hacen parte de la institución y datos manejados, tanto a nivel interno, como en sus relaciones con productores, gremios, entidades gubernamentales y aliados del sector panelero.

La información gestionada, desde registros de productores, estudios técnicos, bases de datos y documentación administrativa, hasta informes estratégicos, representa un activo crítico para la institución y para la sostenibilidad del sector panelero colombiano. Su protección adecuada es indispensable para prevenir riesgos, dar cumplimiento a las normas legales vigentes y asegurar la continuidad de las operaciones.

En base a lo anterior, el objetivo principal de este manual es orientar a todos los colaboradores, directivos, contratistas y demás actores vinculados al Fondo de Fomento Panelero en el manejo responsable, seguro y ético de la información, para la promoción de una cultura organizacional basada en la prevención, la confidencialidad, la integridad y la disponibilidad de la información.

1.1. Objetivo General

Establecer el marco normativo, técnico y organizacional a través de procedimientos y políticas que permitan proteger de manera efectiva la información administrada por el Fondo de Fomento Panelero, garantizando su confidencialidad, integridad y disponibilidad.

1.2. Objetivos Específicos

- Establecer los lineamientos institucionales en materia de seguridad de la información con la finalidad de proteger los datos, programas y equipos de cómputo institucionales, para mantener la disponibilidad, integridad y confiabilidad de la información de todos los servicios de Infraestructura TI, y en especial de aplicaciones críticas y bases de datos.
- Definir las políticas y procedimientos para la protección de los activos de información del Fondo de Fomento Panelero, incluyendo datos físicos y digitales, sistemas, infraestructuras tecnológicas y procesos operativos.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

AREA SISTEMAS DE INFORMACIÓN

FONDO DE FOMENTO PANELERO

VERSIÓN:03

Página 5 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

- Promover la concientización y formación continua de los colaboradores del Fondo de Fomento Panelero en temas de seguridad de la información, divulgando las políticas establecidas para el tratamiento de la información física y digital, y realizando sensibilizaciones sobre la correcta gestión de los activos de información, uso responsable de internet y recursos tecnológicos, y prevención de incidentes de seguridad.
- Mantener accesos restringidos a la información confidencial y acceso según el rol en la red interna de la compañía.
- Mantener control según el perfil del acceso a las aplicaciones más importantes de la empresa, en especial si tiene información sensible o confidencial.
- Garantizar el cumplimiento de la normatividad legal vigente y de la confidencialidad de la información, velando por su estricto cumplimiento.
- Fortalecer una cultura organizacional basada en la responsabilidad y la protección de los datos estratégicos del sector panelero colombiano.
- Proveer directrices claras para la gestión de incidentes de seguridad, incluyendo la notificación, contención, análisis, documentación y recuperación ante eventos que comprometan la información institucional.
- Identificar, clasificar y gestionar los riesgos asociados al manejo de la información, estableciendo controles preventivos, correctivos y de detección para minimizar el impacto de posibles incidentes.

1.3. Alcance

Las disposiciones de la presente serán de obligatorio cumplimiento para todos los miembros colaboradores del Fondo de Fomento Panelero.

1.4. Utilización

Este manual es de uso RESTRINGIDO, de acuerdo con los objetivos establecidos. En consecuencia, queda PROHIBIDO retirarlo de las instalaciones de la entidad, así como su reproducción para fines diferentes a los fijados, sin autorización previa del Gerente General de FEDEPANELA, quien ejerce sus funciones como ente administrador del FONDO DE FOMENTO PANELERO.

1.5. Actualización

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025

	MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN AREA SISTEMAS DE INFORMACIÓN FONDO DE FOMENTO PANELERO	VERSIÓN:03	Página 6 de 28 FECHA DE APROBACIÓN MANUAL: DICIEMBRE 2024
---	---	------------	---

Todas las modificaciones a su contenido incluyendo su actualización serán realizadas por el Área de Sistemas de Información.

1.6. Vigencia

El presente manual tiene vigencia a partir de la fecha de su expedición

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 7 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

2. DEFINICIONES

- 2.1. Activo:** Componente del proceso de negocios. Los activos pueden incluir, gente, edificios, sistemas computacionales, redes, registros en papel, faxes, etc.
- 2.2. Activo de Información:** Cualquier elemento que tenga valor para el Fondo de Fomento Panelero y que requiera protección. Puede incluir datos digitales, documentos impresos, sistemas informáticos, bases de datos, correos electrónicos, equipos tecnológicos, entre otros.
- 2.3. Análisis de Causa Raíz:** Proceso mediante el cual se identifican las causas fundamentales que originaron un incidente de seguridad, con el fin de implementar acciones correctivas y evitar su recurrencia.
- 2.4. Antivirus:** son programas cuyo objetivo es detectar y eliminar virus informáticos.
- 2.5. Archivos:** Es aquel donde reposan las hojas de vida de los Usuarios activos e inactivos y donde se encuentra la información de uso cotidiano y en curso.
- 2.6. Backup (Copia de seguridad):** Duplicado de información almacenada en un medio alternativo con el fin de poder recuperarla en caso de una eventual pérdida de datos, daño o incidente de seguridad.
- 2.7. Borrado Seguro:** Proceso mediante el cual se elimina de manera definitiva e irrecuperable la información almacenada en un dispositivo, utilizando métodos que previenen su recuperación posterior.
- 2.8. Clasificación de la Información:** Proceso mediante el cual se asigna un nivel de sensibilidad o criticidad a la información, con el fin de aplicar medidas de protección adecuadas según su importancia (por ejemplo: pública, interna, confidencial, restringida).
- 2.9. Cliente:** Receptor de un servicio, normalmente servicio al cliente es responsable del costo del servicio, ya sea de manera directa a través de la transferencia de costos o indirectamente en términos de las necesidades del negocio.
- 2.10. Confidencialidad:** Propiedad de la información que garantiza que solo las personas autorizadas pueden acceder a ella. Su objetivo es evitar la divulgación no autorizada de datos sensibles o estratégicos.
- 2.11. Contención de Incidentes:** Conjunto de acciones inmediatas orientadas a limitar el impacto de un incidente de seguridad y evitar su propagación a otros sistemas o activos.
- 2.12. Contraseña Segura:** Clave de acceso que cumple con criterios establecidos de longitud, complejidad y periodicidad de cambio, diseñada para proteger cuentas y sistemas contra accesos no autorizados.
- 2.13. Control de Acceso:** Mecanismos físicos o lógicos que permiten limitar el acceso a la información o a los sistemas, garantizando que solo los usuarios autorizados puedan ingresar, consultar o modificar los datos.
- 2.14. Datos Personales/Sensibles:** Información que permite identificar o hacer identificable a una persona, incluyendo datos confidenciales.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 8 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

- 2.15. Disponibilidad:** Condición que garantiza que la información y los sistemas que la procesan estén accesibles y operativos cuando sean requeridos por los usuarios autorizados.
- 2.16. Disposición Final:** Actividad mediante la cual se da de baja definitiva un activo, garantizando la destrucción segura de la información.
- 2.17. Dispositivo Móvil:** Equipo tecnológico portátil con capacidad de procesamiento y conexión a redes, como teléfonos inteligentes, tabletas o dispositivos similares, utilizados para acceder a información institucional.
- 2.18. Erradicación de Incidentes:** Proceso de eliminación definitiva de la causa que originó un incidente de seguridad, una vez ha sido identificado y contenido.
- 2.19. Incidente:** Cualquier evento que no forma parte usual o normal de la operación diaria del proceso de negocio, que causa o puede causar una interrupción o reducción en la calidad del servicio.
- 2.20. Incidente Crítico:** Evento de seguridad clasificado como de alto impacto que afecta significativamente la operación, compromete información sensible o genera incumplimientos legales o contractuales.
- 2.21. Incidente de seguridad:** Evento que compromete, o tiene el potencial de comprometer, la confidencialidad, integridad o disponibilidad de la información.
- 2.22. Infraestructura de TI:** La suma de los activos de la organización de TI como; hardware, software, facilidades de telecomunicación de datos, procedimientos y documentación.
- 2.23. Integridad:** Cualidad que asegura que la información no ha sido alterada de manera indebida, manteniéndose completa, coherente y exacta desde su creación hasta su almacenamiento o transmisión.
- 2.24. Interfaz:** Interacción física o funcional en los límites entre elementos de la configuración.
- 2.25. Malware:** Software malicioso diseñado para infiltrarse, dañar o interrumpir sistemas informáticos, incluyendo virus, troyanos, ransomware y spyware.
- 2.26. Monitoreo:** es el proceso sistemático de recolectar, analizar y utilizar información para hacer seguimiento a un progreso.
- 2.27. Notificación de Incidentes:** Proceso mediante el cual se comunica la ocurrencia de un incidente de seguridad a las partes responsables, la alta dirección o entidades externas, según corresponda.
- 2.28. Plan de Continuidad del Negocio (PCN):** Conjunto de estrategias y procedimientos establecidos para asegurar que las funciones críticas de la organización puedan continuar operando durante y después de una interrupción significativa.
- 2.29. Políticas de Seguridad:** Directrices y normas formales emitidas por la organización para establecer cómo debe protegerse la información y cómo deben actuar los usuarios frente a los riesgos informáticos.
- 2.30. Respuesta a Incidentes:** Conjunto de actividades ejecutadas para gestionar un incidente de seguridad, incluyendo contención, análisis, erradicación y recuperación.
- 2.31. Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza aproveche una vulnerabilidad en un activo de información, causando un impacto negativo para la organización.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 9 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

- 2.32. Seguridad de la Información:** Conjunto de prácticas, políticas y procedimientos destinados a proteger la confidencialidad, integridad y disponibilidad de la información, garantizando que solo las personas autorizadas tengan acceso a los datos, que estos se mantengan completos y precisos, y que estén disponibles cuando se necesiten.
- 2.33. SaaS (Software as a Service):** modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicaciones, donde se accede vía internet desde un cliente.
- 2.34. Tiempo de Recuperación:** Tiempo máximo permitido para restablecer un sistema o servicio después de un incidente, garantizando la continuidad del negocio.
- 2.35. Tiempo de Respuesta:** Intervalo de tiempo transcurrido desde la detección o reporte de un incidente hasta el inicio de las acciones de atención por parte del área responsable.
- 2.36. Usuario Autorizado:** Persona que ha sido identificada y cuenta con los permisos necesarios para acceder a determinados recursos o información dentro de los sistemas del Fondo de Fomento Panelero.
- 2.37. VPN (Virtual Private Network):** Tecnología que permite establecer una conexión segura y cifrada a través de redes públicas, garantizando la confidencialidad de la información transmitida.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

AREA SISTEMAS DE INFORMACIÓN

FONDO DE FOMENTO PANELERO

VERSIÓN:03

Página 10 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

3. POLÍTICAS Y LINEAMIENTOS

3.1. Política para los activos de la información.

FONDO DE FOMENTO PANELERO protegerá y garantizará la confidencialidad, integridad, disponibilidad, auditabilidad y privacidad de la información mediante la aplicación del presente documento y las políticas de protección de datos vigentes.

Para dar cumplimiento a las labores contratadas se realizará la asignación y utilización de la información entregada o suministrada por los beneficiarios desde la formalización de la inscripción del beneficiario a los responsables de los activos de información en el aplicativo SIPA.

En casos en donde a los colaboradores se les suministre recursos informáticos y/o credenciales de acceso a su infraestructura para el desarrollo de la actividad contratada, el colaborador será el responsable directo del recurso y lo utilizará únicamente para el cumplimiento de las actividades asignadas, sin realizar instalaciones de software o aplicativos en los mismos. En el caso de la información de accesos, el colaborador se abstendrá de obtener, modificar, acceder y en general efectuar cualquier acto sobre la información, sin la previa autorización digital por parte del director del sistema de información.

3.1.1. Procedimientos de seguridad.

3.1.1.1. Control de accesos a la red/correo electrónico

El acceso debe gestionarse conforme al principio de mínimo privilegio, asegurando que cada usuario tenga exclusivamente los permisos necesarios para desempeñar sus funciones. Además, se deben mantener controles efectivos sobre los accesos privilegiados mediante registros detallados, revisiones periódicas (al menos trimestrales) enfocadas en la detección de actividades anómalas o indebidas. La desactivación de cuentas inactivas debe realizarse automáticamente tras un periodo definido de inactividad (180 días).

3.1.1.2. Protección de Datos

Se debe aplicar una política de clasificación de la información que defina claramente los niveles de sensibilidad de la información y los controles asociados a cada uno. Las políticas de retención y destrucción segura de datos deben ser consistentes con el plan de gestión documental del Fondo de Fomento Panelero.

3.1.1.3. Vinculación de proveedores

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 11 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

Todo proveedor con acceso a información sensible o a sistemas críticos debe ser evaluado previamente desde el punto de vista de seguridad. Esto incluye análisis de cumplimiento normativo, capacidades técnicas, y madurez en gestión de riesgos. Los contratos deben contener cláusulas explícitas sobre cumplimiento de políticas de seguridad y confidencialidad. A lo largo de la ejecución contractual se evaluará la continuidad de los controles y su alineación con los niveles de servicio y seguridad pactados.

3.1.1.4. Respaldo y Recuperación

Los sistemas cuentan con respaldos automatizados y manuales, realizados al menos diariamente y mensualmente, respectivamente. Estos cuentan con retención suficiente para asegurar la recuperación ante eventos de pérdida o corrupción de datos (30 días de información).

3.1.1.5. Control Físico y Ambiental

El acceso físico a centros de datos y áreas con infraestructura crítica se encuentra limitado a personal autorizado. Estas áreas se encuentran protegidas mediante sistemas de videovigilancia (CCTV). Además, se cuenta con sistemas redundantes de alimentación eléctrica (UPS y generadores) que se encienden automáticamente ante la eventualidad de una falla de energía eléctrica.

3.1.1.6. Control de acceso y Borrado Seguro de la Información para la reutilización y/o baja de activos tecnológicos

En este procedimiento se establecen los lineamientos para controlar el acceso a la información contenida en activos tecnológicos institucionales durante su fase de reutilización o baja definitiva, y garantizar la eliminación segura de los datos almacenados, previniendo accesos no autorizados y posibles filtraciones de información personal, sensible o confidencial.

Los activos tecnológicos institucionales abarcan los computadores PCs, portátiles, memorias USB, equipos móviles, servidores y dispositivos de almacenamiento pertenecientes al Fondo de Fomento Panelero. Este procedimiento establece los lineamientos cuando estos equipos son destinados a reutilización interna, reasignación a otro usuario, donación, reciclaje o disposición final.

A continuación, se presentan las actividades del procedimiento que ejecutará el soporte técnico del área de sistemas de información, teniendo en cuenta que los usuarios finales de los activos son los encargados de entregar los equipos en condiciones apropiadas, y de informar sobre la existencia de datos críticos dentro del equipo.

Nota:

La baja definitiva de los activos tecnológicos del Fondo de Fomento Panelero (FFP) estará sujeta a la

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 12 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

aprobación previa de la Junta Directiva del Fondo, conforme a los lineamientos administrativos y de control de activos vigentes. Ningún equipo podrá ser dado de baja de manera definitiva sin contar con dicha autorización formal, la cual deberá quedar documentada y anexada al acta correspondiente de baja del activo.

3.1.1.6.1. Solicitud de reutilización o baja del activo, y registro en acta correspondiente.

El área de sistemas de información recibe la solicitud de reutilización o baja del activo, por parte del coordinador o profesional autorizado del área donde se encuentra el equipo.

De acuerdo con el inventario vigente de activos de información, se registra en el acta de reutilización o baja de activos tecnológicos la información del equipo: tipo de equipo y especificaciones, área y usuario asignado, estado funcional y destino previsto (reutilización o baja).

3.1.1.6.2. Control de acceso.

Previo a la ejecución de las actividades de borrado o transferencia de información, se deben aplicar lo siguientes controles:

3.1.1.6.2.1. Bloqueo de cuentas y acceso lógico.

- Deshabilitar accesos locales, contraseñas guardadas, tokens o certificados digitales.
- En caso de acceso remoto, eliminar el dispositivo de las plataformas (VPN, correo, sistemas internos, etc.).
- Verificar que la cuenta del usuario asignado inicialmente haya sido desactivada en el equipo.

3.1.1.6.2.2. Cifrado de datos (si aplica).

- Validar si el disco del equipo estuvo cifrado (BitLocker, VeraCrypt u otro). Documentar estado en el acta correspondiente.
- Si el disco no estuvo cifrado y contiene información sensible, priorizar el uso de sobreescritura múltiple.

3.1.1.6.2.3. Evaluación del riesgo.

- Determinar si el equipo contiene información pública, personal, sensible, confidencial institucional o clasificada.
- Registrar los tipos de datos que contiene el equipo en el acta correspondiente.

3.1.1.6.3. Borrado seguro de la información

3.1.1.6.3.1. Revisión y respaldo autorizado (si aplica).

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025

	MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN AREA SISTEMAS DE INFORMACIÓN FONDO DE FOMENTO PANELERO	VERSIÓN:03	Página 13 de 28
		FECHA DE APROBACIÓN MANUAL: DICIEMBRE 2024	

En caso de que se requiera conservar parte de la información (por razones legales o administrativas), debe hacerse un respaldo cifrado con herramientas autorizadas, y registrar el destino del respaldo y responsable.

Es prohibido realizar copias no autorizadas o almacenar información confidencial en medios personales.

3.1.1.6.3.2. Selección del método de borrado, según tipo de dispositivo o soporte físico de almacenamiento de información.

Según el tipo de dispositivo se define el método de borrado seguro, ya que las tecnologías de almacenamiento almacenan, gestionan y recuperan los datos de forma diferente.

Tipo de dispositivo o soporte físico de almacenamiento de información	Descripción	Ejemplos	Método de borrado seguro recomendado
Disco duro mecánico (HDD)	Medio de almacenamiento magnético tradicional. Tiene platos giratorios internos.	Discos de 500GB o 1TB en equipos antiguos o de escritorio.	Sobre escritura múltiple con herramientas como DBAN, Eraser, o comandos shred/dd en Linux (mínimo 3 pasadas).
Unidad de estado sólido (SSD)	Medio de almacenamiento basado en memoria flash. Es más rápido, pero el borrado es más complejo por la forma en que almacena los datos.	SSD SATA o NVMe instalados en portátiles modernos.	Comando “Secure Erase” del fabricante o herramientas específicas (como Samsung Magician, Intel Toolbox o Parted Magic).
Dispositivos USB / Flash	Almacenamiento portátil y removible. Utiliza memoria flash.	Memorias USB, tarjetas SD, microSD.	Formateo completo + sobreescritura (mínimo 3 pasadas).
Discos externos	HDD o SSD conectados por USB, usados para respaldo o transporte de información.	Western Digital, Seagate, etc.	Definir de acuerdo con el tipo de disco.
Equipos móviles	Dispositivos que tienen memoria interna o extraíble donde se	Teléfonos inteligentes, tabletas.	Restablecimiento de fábrica + encriptación previa del dispositivo.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 14 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

almacenan datos.

En el caso de que el tipo de dispositivo sea un servidor, correspondiente a un equipo empresarial con múltiples discos configurados para alta disponibilidad, tal y como data centers o servidores corporativos, se debe en primer lugar identificar el tipo de almacenamiento del servidor:

Característica	Consideraciones
Configuración con RAID	Si tiene RAID, se debe deshabilitar o desmontar el arreglo antes del borrado.
Tipo de discos empleados	Verificar si los discos son HDD, SSD, o mixtos.
Virtualización	Si hay máquinas virtuales, eliminar imágenes, snapshots y discos virtuales.
Almacenamiento externo	Revisar si el servidor está conectado a una SAN o NAS.

Previo al borrado de la información y si es necesario, se debe respaldar la autorización, previa autorización del director del área responsable de la información. Según los tipos de discos que contiene el servidor, se define el método de borrado seguro:

Tipo de almacenamiento	Método recomendado	Herramienta sugerida
HDD en servidores (RAID o no)	- Desmontar el RAID. - Aplicar sobreescritura múltiple (mínimo 3 pasadas).	DBAN, shred (Linux), Blancco Drive Eraser, MHDD, Nwipe
SSD en servidores	- Ejecutar "Secure Erase" validado por el fabricante. - O utilizar software especializado con soporte SSD.	Parted Magic, Blancco SSD Eraser, herramientas del fabricante (Samsung Magician, Intel SSD Toolbox, etc.)
Arreglos RAID completos	- Desmontar el arreglo. - Borrar cada disco individualmente (nunca desde el RAID activo). - O destruir físicamente los discos si están dañados.	Requiere acceso físico o remoto a los discos fuera del RAID.
Máquinas virtuales (VM)	- Eliminar archivos .vmdk, .vhd, .img, etc. y snapshots. - Aplicar sobreescritura en el datastore si está en disco físico.	sdelete (Windows), shred, wipe, o destruir el almacenamiento virtual con herramientas de hipervisor.
Almacenamiento en red (SAN/NAS)	- Eliminar volúmenes lógicos y aplicar sobreescritura o formato seguro desde el sistema host.	Herramientas propias del almacenamiento o del sistema operativo.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 15 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

3.1.1.6.3.3. Ejecución del borrado seguro y documentación.

El técnico del área de sistemas realiza el proceso de borrado seguro y lo documenta en el acta correspondiente, especificando el tipo de dispositivo tratado, método de borrado utilizado, herramienta empleada y validación del resultado (con evidencia fotográfica si aplica).

3.1.1.6.3.4. Verificación del procedimiento realizado.

El técnico del área de sistemas verifica a través del uso de herramientas de análisis forense o recuperación (tales como Recuva, Photorec, FTK Imager, etc) que la información no es recuperable.

3.1.1.6.4. Borrado seguro de la información reforzado (para equipos con datos personales o confidenciales).

Cuando se identifique que el tipo de dispositivo de almacenamiento de información contiene información clasificada como personal, sensible o confidencial institucional, se deben ejecutar medidas adicionales a las enunciadas en el punto 3.1.1.6.3. que refuercen el procedimiento de borrado seguro de la información. Estas incluyen:

3.1.1.6.4.1. Aislamiento del equipo.

- Retirar el equipo de la red institucional.
- Desactivar conexiones inalámbricas (Wi-Fi, Bluetooth, etc.).
- Restringir el acceso físico al equipo (guardar en lugar seguro hasta ejecutar el proceso).

3.1.1.6.4.2. Borrado seguro con método avanzado.

Se selecciona el método de eliminación de la información más seguro, de acuerdo con el tipo de dispositivo:

Tipo de dispositivo o soporte físico de almacenamiento de información	Método reforzado recomendado
Disco duro mecánico (HDD)	DBAN con mínimo 3 pasadas (según estándar DoD 5220.22-M) o equivalente.
Unidad de estado sólido (SSD)	Secure Erase validado por el fabricante + comprobación con herramienta forense.
Dispositivos USB / Flash	Múltiples pasadas con herramientas como Eraser o shred en Linux.
Equipos móviles	Cifrado previo + restablecimiento de fábrica + eliminación remota si aplica.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 16 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

Si el medio presenta fallas que impidan garantizar el borrado seguro, debe procederse a su destrucción física controlada, como la trituración industrial, desmagnetización certificada o perforación física, y dejar evidencia del procedimiento realizado.

3.1.1.6.5. Reutilización del equipo.

Si el equipo será reasignado a un nuevo usuario, se realizan las siguientes actividades:

- Instalar una imagen limpia y autorizada del sistema operativo.
- Aplicar parches de seguridad y software institucional.
- Actualizar el inventario y reasignar el equipo con control de acceso reconfigurado (nuevo usuario y permisos, cifrados si aplica).
- Dejar constancia del procedimiento en el acta correspondiente.

3.1.1.6.6. Baja y disposición final.

Previo a la ejecución de la baja definitiva del activo, se deberá contar con la aprobación formal de la Junta Directiva del Fondo de Fomento Panelero (FFP). Esta aprobación deberá estar debidamente documentada y anexarse al acta de baja del activo tecnológico.

Si el equipo será dado de baja, se realizan las siguientes actividades:

- Dejar constancia del procedimiento en el acta correspondiente.
- Si el equipo será donado o transferido a una entidad externa al FFP, se debe dejar constancia de los datos de la entidad a la que será transferido.
- Disposición final según políticas ambientales, garantizando que no se exponga ningún componente con datos.

3.1.1.6.7. Medidas complementarias de seguridad.

Se tomarán medidas correctivas en caso de detectar accesos no controlados o eliminación no segura. Se mantendrá evidencia del proceso de borrado seguro realizado como respaldo en caso de auditorías.

Si el equipo se entrega a terceros (proveedor de destrucción, reciclaje, donación), se debe ejecutar el borrado antes la salida de las instalaciones del FFP.

Todos los colaboradores del FFP serán sensibilizados en la importancia de eliminar adecuadamente la información antes de la entrega de equipos.

3.1.1.6.8. Anexos.

Formato de acta de reutilización o baja de activos tecnológicos.

Procedimiento FFP-DAF-013 Baja de activos – Dirección Administrativa y Financiera

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

AREA SISTEMAS DE INFORMACIÓN

FONDO DE FOMENTO PANELERO

VERSIÓN:03

Página 17 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

3.2. Política de redes sociales

Ningún colaborador ni contratista del **FONDO DE FOMENTO PANELERO** se encuentran autorizado para participar en redes sociales a nombre del **FONDO DE FOMENTO PANELERO**, en actividades, proyectos, clientes, beneficiarios, personas naturales o jurídicas ni realizar algún tipo de publicación de información en medios de comunicación masiva sin la autorización expresa y digital del departamento de comunicaciones.

Se deben acatar los lineamientos establecidos en las políticas del departamento de comunicaciones del FONDO DE FOMENTO PANELERO.

3.3. Políticas en el proceso de vinculación o desvinculación del personal

FONDO DE FOMENTO PANELERO reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos sociales y comerciales del FONDO DE FOMENTO PANELERO, por tal razón reconoce la importancia de contratar colaboradores y contratistas idóneos que guarden principios de confidencialidad de la información, por tal razón establece los parámetros que se encuentran los contratos y órdenes de servicio establecidos con personas naturales y jurídicas.

3.4. Política de contraseñas seguras

Los colaboradores de **FONDO DE FOMENTO PANELERO** utilizan los computadores como única y exclusiva herramienta de conexión a las diferentes aplicaciones del Core del negocio.

El área de sistema de información es la responsable de realizar la entrega de credenciales, usuarios y contraseñas de acuerdo con el manual de procedimientos del área, utilizando los canales institucionales dispuestos para tal fin.

Se recomienda nunca copiar o divulgar los datos de acceso o los que les son provistos temporal o permanentemente para la ejecución de las actividades, no dejar anotadas las credenciales cerca de la computadora portátil, ni dentro de su estuche o funda. Así mismo, se recomienda el uso de contraseñas fuertes y que no coincidan con hijos o familiares cercanos

Solo para procesos de auditoría externa, interna y soporte técnico el colaborador debe suministrar las credenciales de accesos local o dispositivos entregados por la compañía y una vez finalizada la tarea el colaborador debe actualizar su contraseña.

Se recomienda no utilizar la opción de auto relleno en el navegador, y por el contrario escribir la contraseña cada vez que necesite abrir una sesión, es una regla simple y no perderá mucho tiempo haciendo esto.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 18 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

Para crear contraseñas seguras, se recomienda: usar una contraseña distinta para cada cuenta importante, realizar la modificación de las contraseñas de manera semestral, usar una contraseña formada por la combinación de letras, números y símbolos, y no usar información personal o palabras comunes como contraseñas.

3.5. Política de escritorio limpio

Los colaboradores no deberán almacenar ningún tipo de archivo en el escritorio de la computadora asignada para el desarrollo de sus actividades del **FONDO DE FOMENTO PANELERO**.

Una vez asignado por parte del responsable la computadora como recurso tecnológico, el colaborador debe garantizar que la información se almacene en el recurso compartido (servidor) asignado para tal fin.

3.6. Política de uso de Internet.

FONDO DE FOMENTO PANELERO provee herramienta de conexión para uso con fines corporativos y por lo tanto realiza recomendaciones frente a las restricciones de acceso a Internet.

Para los colaboradores existen cláusulas de confidencialidad de la información, las cuales se encuentran incluidas en el contrato laboral, garantizando el uso adecuado de los activos de la información.

Cuando se realizan bloqueos específicos, estos son realizados a través de dispositivo de seguridad y de privilegios de acuerdo con el rol del colaborador dentro de la compañía.

En la ejecución de actividades laborales:

- Está prohibido el uso de internet con fines de ocio y juegos.
- El uso de herramientas de comunicación es con fines de trabajo y propiamente corporativos.
- Se prohíbe la manipulación de páginas de enmascaramientos de URL para el acceso a las páginas prohibidas por el FONDO DE FOMENTO PANELERO.
- Se restringe el acceso a páginas con contenido inapropiado y no permitido.
- Se prohíbe Utilizar los medios de comunicación o herramientas corporativas para obtener lucro personal o acceso remoto a aplicaciones no corporativas.

3.7. Política de equipos personales

El **FONDO DE FOMENTO PANELERO** prohíbe el uso de equipos personales de cómputo dentro de las instalaciones de la compañía y el acceso a la red de la compañía, a excepción de aquellos colaboradores que en el ejercicio de sus actividades así lo requieran y cuenten con la autorización por parte del área a la que se encuentran vinculados y al área de sistemas de información.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 19 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

3.8. Política de uso de dispositivos móviles (institucionales y no institucionales)

El Fondo de Fomento Panelero reconoce que el uso de dispositivos móviles representa un riesgo potencial para la seguridad de la información, por lo cual establece los siguientes lineamientos para garantizar la protección de los activos de información:

3.8.1. Alcance

Aplica a todos los colaboradores, contratistas y terceros que accedan a información institucional mediante dispositivos móviles, ya sean institucionales o personales.

3.8.2. Dispositivos móviles institucionales

Se consideran dispositivos móviles institucionales aquellos asignados por el Fondo (teléfonos inteligentes, tabletas u otros dispositivos portátiles).

Lineamientos:

- Los dispositivos deben ser utilizados exclusivamente para fines laborales.
- Deben contar con mecanismos de seguridad obligatorios:
 - Bloqueo por contraseña, PIN, patrón o biometría
 - Cifrado de almacenamiento (cuando aplique)
 - Software antivirus o de seguridad actualizado
- Solo el área de Sistemas de Información podrá autorizar la instalación de aplicaciones.
- Está prohibido:
 - Instalar aplicaciones no autorizadas
 - Realizar configuraciones que comprometan la seguridad (root, jailbreak, etc.)
- En caso de pérdida o robo:
 - El usuario debe reportar inmediatamente al área de Sistemas
 - Se podrán aplicar medidas como bloqueo remoto o borrado de la información

3.8.3. Dispositivos móviles no institucionales

El uso de dispositivos personales para acceder a información del Fondo está restringido y solo será permitido bajo autorización expresa del área de Sistemas de Información.

Condiciones de uso:

- El dispositivo debe cumplir con controles mínimos de seguridad:
 - Sistema operativo actualizado
 - Bloqueo de pantalla activo
 - No estar comprometido (sin root o jailbreak)
- El acceso a la información institucional se realizará únicamente a través de:
 - Plataformas autorizadas (correo corporativo, herramientas en la nube)

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

AREA SISTEMAS DE INFORMACIÓN

FONDO DE FOMENTO PANELERO

VERSIÓN:03

Página 20 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

- Está prohibido:
 - Almacenar información institucional sensible de forma local
 - Compartir información corporativa a través de aplicaciones personales no autorizadas
- El Fondo podrá:
 - Revocar el acceso en cualquier momento
 - Solicitar la eliminación de información institucional del dispositivo

3.8.4. Transferencia y manejo de información

Toda transferencia de información desde o hacia dispositivos móviles debe cumplir con las políticas de clasificación de la información.

- La información sensible o confidencial deberá:
 - Ser cifrada
 - No almacenarse permanentemente en dispositivos móviles
- Se prohíbe el uso de redes Wi-Fi públicas sin mecanismos de protección (VPN o cifrado).

3.8.5. Responsabilidades del usuario

- Custodiar el dispositivo asignado o autorizado
- Reportar incidentes de seguridad de forma inmediata
- Cumplir las políticas de seguridad de la información vigentes

3.9. Política de medios extraíbles

El uso de medios extraíbles (USB, discos duros externos, tarjetas de memoria, entre otros) queda restringido exclusivamente a funciones justificadas y previamente autorizadas por el área de Sistemas de Información. Si las necesidades propias requeridas para el desarrollo de las actividades de los colaboradores del Fondo de Fomento Panelero requieren del uso de medios extraíbles, su asignación debe realizarse a través del área de sistemas de información, área que se encargará de que cualquier transferencia de información mediante medios extraíbles cumpla con los controles establecidos de protección de datos.

3.10. Política de conexión remota a los equipos

En concordancia con la validación del área jurídica, el Fondo de Fomento Panelero no adopta un modelo formal de teletrabajo. Sin embargo, se permite la conexión remota a los equipos institucionales bajo condiciones controladas.

3.10.1. Alcance

Aplica a todos los colaboradores y contratistas que requieran acceso remoto a los sistemas, equipos o recursos tecnológicos del Fondo.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

AREA SISTEMAS DE INFORMACIÓN

FONDO DE FOMENTO PANELERO

VERSIÓN:03

Página 21 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

3.10.2. Condiciones de acceso remoto

- La configuración del acceso remoto al computador de la oficina debe ser:
 - Autorizado previamente por el área de Sistemas de Información
 - Justificado por necesidades operativas
- Se realizará únicamente mediante herramientas seguras definidas por la entidad (VPN, escritorio remoto u otras soluciones autorizadas).
- Todo acceso remoto debe estar asociado a un usuario identificado y autenticado.

3.10.3. Controles de seguridad

El acceso remoto deberá cumplir con los siguientes controles:

- Autenticación segura (usuario y contraseña robusta)
- Uso de conexiones cifradas
- Registro y monitoreo de accesos (logs)
- Restricción de acceso según perfil y rol
- Desconexión automática por inactividad

3.10.4. Restricciones

- Está prohibido el acceso remoto desde:
 - Equipos públicos o compartidos
 - Dispositivos no seguros o comprometidos
- No se permite:
 - Descargar información sensible en equipos personales
 - Compartir credenciales de acceso
- El acceso remoto será suspendido cuando:
 - Finalice la relación contractual
 - No exista justificación operativa

3.10.5. Responsabilidades

- Área de Sistemas de Información:
 - Autorizar, configurar y monitorear accesos remotos
 - Garantizar la seguridad de las conexiones
- Usuarios:
 - Usar el acceso remoto únicamente para fines laborales
 - Proteger sus credenciales
 - Reportar cualquier actividad sospechosa
 - No exista justificación operativa

3.10.6. Monitoreo y control

El Área de Sistemas de Información del Fondo de Fomento Panelero podrá monitorear y auditar las sesiones remotas con el fin de garantizar el cumplimiento de las políticas de seguridad de la información

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 22 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

3.11. Política de uso de correo electrónico

El uso del correo electrónico corporativo debe ser solo con fines del desarrollo de las labores propias de las funciones empresariales por lo tanto el sistema de e-mail no debe ser utilizado para enviar contenido inapropiado como:

- Bases de datos de personas naturales o información sensible a personal no autorizado o correos personales; el correo destinado para la recolección de la información, vía formularios web, es el siguiente: gestionspd@gmail.com.
- Correos que puedan considerarse difamatorios o que puedan causar perjuicios a FONDO DE FOMENTO PANELERO
- Enviar contenido inapropiado como: pornografía, comentarios ofensivos (por temas de género, religión, orientación sexual, ideología, etc.), relacionados con actividades terroristas, cultos, apuestas o actividades ilegales.
- Mensajes que puedan considerarse como acoso de cualquier índole.
- Mensajes o contenidos que puedan afectar la reputación del FONDO DE FOMENTO PANELERO tales como acoso, actividades delictivas, cadenas con comentarios ofensivos (por temas de género, religión, orientación sexual, ideología, etc.), relacionados con actividades terroristas, cultos, apuestas o actividades ilegales.
- Contenido que infrinja las leyes de derechos de autor
- Correos de cadenas o mensajes de humor. Estos contenidos muchas veces no son adecuados en el ambiente laboral y saturan las bandejas de entrada.

Recomendaciones generales:

- Se recomienda solo usar la marcación del correo como “alta prioridad” de forma esporádica y para mensajes realmente urgentes
- Se recomienda ser prudente en el momento de enviar mensajes a grupos de personas y enviar los correos a quienes realmente encontrarán el mensaje relevante y útil
- Se recomienda usar el campo “CCo” (copia oculta) para el envío de correos de divulgación o interés general.
- Revisar previamente que los destinatarios sí son los adecuados para el envío de la información del email.
- Si se recibe un email que considere inapropiado se debe reportar inmediatamente al responsable de la administración del correo electrónico para su respectiva gestión o en su defecto, eliminarlo.
- El correo electrónico no es un medio seguro de comunicación, por lo tanto, debe enviar el contenido confidencial o sensible de manera cifrada, haciendo uso de otros mecanismos de cifrado.
- Los usuarios de email no deben abrir archivos adjuntos de correos provenientes de fuentes desconocidas. Pueden ser peligrosos y contener virus, troyanos o cualquier aplicación maliciosa.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 23 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

- Las comunicaciones hechas a través del correo corporativo tienen una copia de seguridad y hacen parte de los archivos de la empresa. La compañía podrá monitorear o investigar las comunicaciones que se hagan a través de dicha herramienta.
- El correo es considerado como una herramienta personal, por lo tanto y por ningún motivo se debe hacer uso de un correo de otro funcionario, esta actividad legalmente está contemplada como una suplantación de identidad.
- No enviar correos masivos a funcionarios externos de la empresa, y si no existe otra opción, verificar que los datos de destinatario sean enviados en copia oculta.

3.12. Política de control de acceso a los recursos de la Red

FONDO DE FOMENTO PANELERO hace uso de aplicaciones específicas para el desarrollo de sus funciones tales como el sistema de información contable, SIPA, y el servidor del Fondo de Fomento Panelero para la disposición de información digital; estas aplicaciones a su vez establecen los criterios de seguridad para el acceso identificado y controlado a la información.

Por lo anterior a cada usuario se le realizará la entrega de un usuario y contraseña, quien se compromete a su gestión estableciendo los criterios de las políticas de contraseñas seguras, así, todo usuario, servicio o dispositivo que requiera conectividad deberá ser identificado, autenticado y autorizado antes de interactuar con cualquier recurso de la red corporativa. Adicionalmente, todo cambio en las reglas de acceso deberá estar justificado, documentado y aprobado por el área de Sistemas de Información.

FONDO DE FOMENTO PANELERO debe asegurar que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.

Cualquier dispositivo que se conecte o deseen conectarse a las redes de datos deben cumplir con todos los requisitos o controles de autenticación y únicamente podrán realizar las tareas para las que fueron autorizados.

3.13. Política de creación y administración de usuarios y roles, y gestión de información física

La generación y administración de roles para la gestión de información electrónica se realiza con base en el manual de funciones del Fondo de Fomento Panelero, garantizando el acceso de forma adecuada y contralada a los recursos compartidos, donde se encuentra la información de FONDO DE FOMENTO PANELERO.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 24 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

El programa de gestión documental del FONDO DE FOMENTO PANELERO es el área responsable de la gestión, seguimiento y control del archivo físico de la organización. La custodia y protección del archivo físico se realiza en cada una de las áreas productoras, y el archivo central se mantiene en espacios físicos bajo llave; las solicitudes de la información física, se deben realizar a través del correo electrónico gestiondocumental@fedepanela.org.co y registrar en el “Formato de Control de Consulta y Préstamo Documental”, siguiendo los lineamientos del Instructivo de consultas y préstamo de información.

3.14. Política de uso de equipos corporativos.

Los equipos corporativos solo deben ser utilizados con los fines del desarrollo de sus labores empresariales, no con fines personales o delictivos.

Los colaboradores no deben instalar programas en sus equipos asignados, diferentes a los aprobados por la compañía para el desarrollo de las actividades de cada rol y el inventario de licenciamiento oficial.

Los colaboradores se deben comprometer al cuidado físico del mismo aceptando su responsabilidad firmada en el acta de entrega de los equipos.

3.15. Política para administradores y funcionarios de tecnología

Las plataformas tecnológicas deben ser operadas y administradas en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dicha plataforma y servicios.

El **FONDO DE FOMENTO PANELERO** debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

La clave de administrador solo debe ser usada para casos específicos, se deben crear usuarios con privilegios de administración en los que se permita el monitoreo de sus actividades.

3.16. Política de gestión de incidentes de seguridad de la información

El Fondo de Fomento Panelero establece la presente política con el fin de garantizar la gestión oportuna, controlada y documentada de los incidentes de seguridad de la información, minimizando su impacto sobre la operación, los activos de información y el cumplimiento normativo.

Todos los incidentes de seguridad de la información, reales o sospechados, deben ser reportados de forma inmediata al área de Sistemas de Información mediante los canales definidos.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

AREA SISTEMAS DE INFORMACIÓN

FONDO DE FOMENTO PANELERO

VERSIÓN:03

Página 25 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

Se entiende como incidente cualquier evento que comprometa, o tenga el potencial de comprometer, la confidencialidad, integridad o disponibilidad de la información.

3.16.1. Clasificación de los incidentes de seguridad

Los incidentes de seguridad se clasificarán según su nivel de impacto:

Nivel	Descripción	Ejemplos
Alto (Crítico)	Impacto severo en la operación, pérdida de información crítica o incumplimiento legal	Ransomware, fuga de datos sensibles, caída total de sistemas
Medio	Afectación parcial de servicios o riesgo controlado	Accesos no autorizados detectados, malware contenido
Bajo	Incidentes sin impacto significativo o fácilmente controlables	Intentos fallidos de acceso, errores de configuración sin impacto

3.16.2. Responsabilidades

Área de Sistemas de Información:

- Recibir, gestionar y coordinar la atención de incidentes
- Clasificar el incidente según su criticidad
- Ejecutar acciones de contención, análisis, erradicación y recuperación
- Documentar el incidente y generar reportes
- Escalar incidentes críticos a la Dirección

Director del Área de Sistemas:

- Supervisar la gestión de incidentes
- Aprobar acciones correctivas mayores
- Informar a la alta dirección cuando aplique

Usuarios / Colaboradores / Contratistas:

- Reportar inmediatamente cualquier incidente o evento sospechoso
- No manipular evidencias
- Seguir las instrucciones del área de Sistemas

3.16.3. Tiempos de respuesta

Los tiempos de atención se establecerán según la criticidad del incidente:

Nivel	Tiempo de respuesta inicial	Tiempo de atención
Alto (Crítico)	Inmediato (máx. 1 hora)	≤ 24 horas
Medio	≤ 4 horas	≤ 48 horas
Bajo	≤ 8 horas	≤ 5 días hábiles

3.16.4. Procedimiento de gestión de incidentes

La gestión de incidentes seguirá el siguiente ciclo:

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 26 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

- **Identificación:** Detección del incidente por parte de usuarios o sistemas de monitoreo
- **Registro:** Documentación inicial del evento (fecha, usuario, sistema afectado, descripción)
- **Clasificación:** Determinación del nivel de criticidad (alto, medio, bajo)
- **Contención:** Acciones inmediatas para limitar el impacto
- **Análisis:** Identificación de causa raíz
- **Erradicación:** Eliminación de la causa del incidente
- **Recuperación:** Restauración de servicios e información
- **Lecciones aprendidas:** Documentación y mejora de controles

3.16.5. Procedimiento de notificación

- Todo incidente debe ser reportado a través de:
 - Correo institucional
 - Comunicación directa al área de Sistemas
- Para incidentes críticos:
 - Se notificará de inmediato al Director de Sistemas
 - Se informará a la alta dirección
- Cuando aplique:
 - Se notificará a entidades regulatorias conforme a la normativa vigente
 - Se informará a terceros afectados

3.16.6. Seguimiento y mejora continua

- Los incidentes deberán ser analizados periódicamente para identificar tendencias
- Se implementarán acciones correctivas y preventivas
- Se actualizarán los controles de seguridad cuando sea necesario

3.17. Plan de respuesta a emergencias en caso de pérdida de información

Ante cualquier evento que implique la pérdida parcial o total de información, ya sea por corrupción de datos, eliminación accidental, fallos de infraestructura, sabotaje o ataque malicioso, se activará inmediatamente el Plan de Respuesta a Emergencias bajo la coordinación del área de sistemas de información. La primera acción será contener el incidente, preservando evidencia y desconectando los sistemas afectados para evitar una mayor propagación o impacto. Paralelamente, se realizará una evaluación preliminar del alcance de la pérdida, identificando los activos comprometidos, su clasificación y la posible afectación a procesos críticos, cumplimiento legal o compromisos contractuales.

Una vez contenida la situación, se procederá a la restauración de los datos desde respaldos verificados y probados previamente, siguiendo los procedimientos definidos. Esta restauración deberá realizarse en el menor tiempo posible definido para cada activo. Finalizada la recuperación, se documentará el incidente en su totalidad, incluyendo análisis de causa raíz y planes de mejora para

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 27 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

prevenir recurrencias. Si la pérdida involucra datos personales, información confidencial o activos regulados, se deberá notificar a las autoridades competentes y a los afectados, conforme a los plazos legales aplicables.

3.18. Planificación de la continuidad del negocio.

El Fondo de Fomento Panelero (FFP), en cumplimiento de su responsabilidad de asegurar el desarrollo sostenible del sector panelero colombiano, establece este Plan de Continuidad del Negocio (PCN) con el fin de garantizar la operación resiliente de sus procesos misionales, incluso ante situaciones de interrupción severa. Se consideran escenarios de contingencia como desastres naturales, ciberataques, indisponibilidad de sedes físicas, pérdida de conectividad y fallas que puedan afectar la disponibilidad de la infraestructura tecnológica.

Este plan se basa en la identificación previa de procesos esenciales, activos de información prioritarios y dependencias tecnológicas y operativas, y responde a un análisis que identifica como procesos críticos: la gestión del recaudo, el soporte a proyectos de investigación y asistencia técnica a productores, la administración de información estratégica del sector y la coordinación con entidades gubernamentales y agremiaciones.

Ante una interrupción significativa, se activará el protocolo definido por el área de sistemas de información, que incluye en primer lugar coordinar la respuesta según el nivel de afectación. Se priorizará la recuperación de los sistemas financieros y de recaudo, el acceso a las bases de datos de productores y el restablecimiento de los canales de comunicación con aliados estratégicos e instituciones del gobierno.

Se implementarán estrategias de recuperación que incluyen: restauración prioritaria de plataformas tecnológicas (sistemas contables, bases de datos de productores, aplicativos sectoriales), uso de respaldos cifrados con retención mínima de 30 días, y despliegue de soluciones temporales en entornos alternos o en la nube. Para operaciones presenciales, se habilitarán puntos de contingencia previamente definidos y se activarán procedimientos manuales para asegurar la continuidad del recaudo, el pago de compromisos y la atención a usuarios.

Todos los procesos restaurados deberán cumplir con los RTO y RPO definidos según su criticidad, con especial énfasis en restablecer operaciones financieras y regulatorias en las primeras 24 horas.

El Fondo de Fomento panelero procurará realizar auditorías anuales y actualizaciones posteriores a cada evento disruptivo, garantizando así la mejora continua del plan. Asimismo, se prevé la capacitación periódica del personal clave y el fortalecimiento de alianzas estratégicas con proveedores tecnológicos, para asegurar la sostenibilidad operativa del sector ante cualquier eventualidad.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025



**MANUAL INTERNO DE SEGURIDAD DE LA
INFORMACIÓN
AREA SISTEMAS DE INFORMACIÓN
FONDO DE FOMENTO PANELERO**

VERSIÓN:03

Página 28 de 28

FECHA DE APROBACIÓN MANUAL:
DICIEMBRE 2024

CONTROL DE CAMBIOS

Versión No.	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
01	15/02/2020	Creación del documento
02	10/03/2020	Se adicionó el canal de un correo electrónico para la gestión de ciertas bases de datos, para la recolección de la información, vía formularios web, es el siguiente: ffpdatos@gmail.com
03	15/12/2024	Modificación en el formato del manual. Adición de introducción y objetivo general. Complemento de objetivos específicos. Adición de utilización, vigencia y modificaciones. Complemento de definiciones. Eliminación del apartado condiciones generales. Actualización del apartado de políticas y lineamientos.
04	30/12/2025	Complemento de definiciones de acuerdo con procedimientos adicionados. Actualización de los procedimientos de seguridad: adición del procedimiento de control de acceso y borrado seguro de la información, para la reutilización y/o baja de activos tecnológicos y el procedimiento de uso de dispositivos móviles, tanto institucionales como no institucionales Actualización de las políticas establecidas: adición de la política de conexión remota a los equipos, complemento de la política de incidentes de seguridad, renombrada a política de gestión de incidentes de seguridad de la información.

RESPONSABLE	ELABORÓ/MODIFICÓ	REVISÓ	APROBÓ
Nombre: Cargo: Fecha:	Catalina García Marroquín Profesional de apoyo en Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025	Mauricio Angel Riveros Director de Sistemas de Información Diciembre / 2025