ifc

INSTITUTO FINANCIERO DE CASANARE

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Elaborado por:	Revisado por:	Aprobado por:
Nombre: Erika Pilar Madero S. Profesional de apoyo área de sistemas	Nombre: Mirama López Zamudio Cargo: Subgerente Administrativa y Financiera	~~Nombre: BRAULIO CASTELBLANCO~~ VARGAS. Cargo: Gerente. Acta de comité institucional de Gestión y Desempeño 03 del 30-01-2023.

"ES EL TIEMPO DE CASANARE"

CONTENIDO

INTRODUCCION

Actualmente la información es reconocida como un activo valioso, siempre se busca desarrollar y adoptar mecanismos que garanticen salvaguardar estos activos de información para cualquier empresa pública o privada; los sistemas de información también son parte importante, ya que son ellos quienes apoyan cada vez más los procesos que se manejan en una empresa y/o entidad.

El siguiente documento presenta una descripción de las políticas y normas del PSPIL; determinadas por el IFC, con respecto a la protección de los activos de información de: funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluida el hardware y el software. Que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos

El MINTIC ha establecido que para proteger estos activos de información y garantizar su disponibilidad, integridad y confidencialidad debe adoptarse y aplicarse el Modelo de Seguridad y Privacidad de la información por tal razón, dentro de las nuevas Políticas de Gobierno Digital tiene como uno de sus habilitadores la Seguridad y Privacidad de la información aquí plasmada.

De acuerdo al **Decreto 1078 de 2015**, establece que las entidades públicas deben implementar la Política de Seguridad y Privacidad de la Información así como la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

MARCO NORMATIVO

El Estado colombiano cuenta con normatividad vigente que obliga el correcto tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- ✓ Norma Técnica Colombiana NTC - ISO/IEC 27001, Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.
- ✓ **Ley 527 de 1999,** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
- ✓ **Ley 1474 de 2011,** Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
- ✓ **Ley estatutaria 1581 de 2012,** Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- ✓ **Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, el artículo 3° manifiesta que, "Principio de transparencia.** Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley."

- ✓ **Ley 1712 de 2014**, **artículo 4°,** Establece como derecho fundamental la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública.

- ✓ ***Ley 1712 de 2014, artículo 7:*** "Disponibilidad de la información"
  "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos,

remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Así mismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- ✓ **Decreto 4632 de 2011,** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- ✓ **Decreto 2573 del 12 de Diciembre 2014** por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, en el artículo 5° numeral 4° se encuentra como componente la Seguridad y Privacidad de la Información.

  "4. **Seguridad y privacidad de la Información.** Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada."

- ✓ Decreto 103 de 2015, Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.

- ✓ **Decreto 1078 de 2015**, establece que las entidades públicas deben implementar la Política de Seguridad y Privacidad de la Información.

- ✓ **El Decreto 1413 de 2017, artículo 2.2.17.6.6, indica que "Seguridad de la información.** Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.

- ✓ **Decreto 1413 de 2017, artículo 2.2.17.6.1**, "Responsable y encargado del tratamiento": "Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."

- ✓ **Decreto 1413 de 2017, artículo 2.2.17.6.3, "Responsabilidad demostrada y programa integral de gestión de datos.** Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales."
- ✓ **Ley 1437 de 2011, Capítulo IV**: "Utilización de medios electrónicos en el procedimiento administrativo".

  "Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."
- ✓ **Ley 1581 de 2012**, en el artículo 4° frente a los Principios para el Tratamiento de datos personales indica que; "En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

- ✓ **Ley 1581 Artículo 17, ítem d,** ibídem, frente a los deberes de los responsables del Tratamiento de la información establece el legislador que debe "Conservar la

información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

DEFINICIONES

- ✓ **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- ✓ **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- ✓ **Integridad**: La propiedad de salvaguardar la exactitud y complejidad de la información.
- ✓ **Software:** Son las instrucciones que el ordenador necesita para funcionar, no existen físicamente, o lo que es igual, no se pueden ver ni tocar.
- ✓ **Hardware:** Componentes físicos del ordenador, es decir, todo lo que se puede ver y tocar. Clasificaremos el hardware en dos tipos: El que se encuentra alrededor de la torre o CPU, y que por lo tanto, sí que vemos a simple vista, y que denominamos periféricos.
- ✓ **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- ✓ **MinTic**: Ministerio de Tecnologías de la Información y las Comunicaciones es la entidad que se encarga de diseñar planes y políticas para que la tecnología llegue a todos los departamentos y ciudades de Colombia.
- ✓ **IFC:** Instituto Financiero de Casanare
- ✓ **Inventario de activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)
- ✓ **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 consecuencias. (ISO/IEC 27000).
- ✓ **Dato privado**: Es el dato que por su naturaleza íntima o reservada sólo es

relevante para el titular

- ✓ **Dato público**: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
- ✓ **PSPIL:** Plan de Seguridad y Privacidad de la Información.
- ✓ **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- ✓ **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- ✓ **Tecnología de la Información (TI)**: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- ✓ **Sistema de Información (SI):** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

OBJETIVOS

Objetivo General

Instrumentar el Modelo de Seguridad y Privacidad de la información para fortalecer y garantizar que el manejo, control y administración de los servicios de TI, la información y los procesos que se generan en el IFC, preserven la confidencialidad, integridad y disponibilidad de la información.

Objetivos Específicos

- ✓ Implementar Políticas de seguridad de la información para el IFC
- ✓ Establecer un plan de trabajo para la implementación de las Políticas y su adecuado seguimiento
- ✓ Capacitar y concientizar a todos los usuarios activos de información tanto digitales como físicos del IFC sobre el proceso de la seguridad y privacidad de la información.

POLITICAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición del Instituto Financiero de Casanare de la ciudad de Yopal (Cas), con respecto a la protección de los activos de información donde (Funcionarios de planta, contratistas, terceros, la información, los procesos, las TI, incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información de la entidad.

Para asegurar el direccionamiento estratégico, el Instituto Financiero de Casanare, establece políticas y objetivos de seguridad para la información, como los siguientes:

1. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
2. Cumplir con los principios de seguridad de la información.
3. Proteger los activos de información.
4. Apoyar la innovación tecnológica.
5. Cumplir con los principios de la función administrativa.
6. Implementar el sistema de gestión de seguridad de la información.
7. Minimizar los riesgos en la entidad.
8. Mantener la confianza de los funcionarios, contratistas y terceros.
9. Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas y clientes externos del IFC.
10. Garantizar la continuidad del servicio frente a incidentes.

ALCANCE

La seguridad de la información es un esfuerzo que se logra en equipo, se requiere la participación y el apoyo de todos los miembros de la organización que trabajan con sistemas de información o utilizan de la Infraestructura Tecnológica de la entidad (IFC).

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con el Instituto Financiero de Casanare, esto con el fin de alcanzar un nivel adecuado de protección de las características de seguridad y calidad de la información relacionada.

NIVEL DE CUMPLIMIENTO

A continuación se establecen las políticas que soportan el plan de seguridad y privacidad de la información del Instituto Financiero de Casanare. Políticas que deben ser cumplidas por todo el personal de la entidad.

1. Garantizar a la entidad la disponibilidad en sus procesos y la continuidad de su operación basada en el impacto que pueden generar ciertos eventos.
2. Controlar la operación de los procesos de la entidad garantizando la seguridad de los recursos tecnológicos y la red de datos.
3. Proteger la información generada, procesada o resguardada por los procesos realizados en la entidad, así como los activos de información que hacen parte de los mismos.
4. Implementa controles de acceso a la información, sistemas y recursos de red.
5. Garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
6. Proteger la información de amenazas originadas por parte del personal.

7. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

DESCRIPCION DE LAS POLITICAS

RIESGOS EN LA SEGURIDAD DE LA INFORMACION

Los riesgos de la seguridad de la información en el Instituto Financiero de Casanare se pueden clasificar en 3 grupos: Riesgos por sucesos físicos, riesgos por criminalidad común, y riesgos por sucesos derivados de la negligencia de los usuarios(as) y/o por decisiones de la misma entidad.

RIESGOS POR SUCESOS FÍSICOS

1. Sismo
2. Inundación
3. Incendio
4. Polvo
5. Sobre carga eléctrica
6. Falta de ventilación
7. Falla en el sistema (Daño en el disco duro)
8. Falla de corriente (Apagones)

RIESGOS POR CRIMINALIDAD COMUN

1. Virus
2. Fraude
3. Sabotaje (Ataque físico y electrónico)
4. Daños por vandalismo
5. Violación a derechos de autor

6. Robo / Hurto (Físico)
7. Robo / Hurto (Información)

RIESGOS POR NEGLIGENCIA DE USUARIOS / AS Y/O DECISIONES DE LA ENTIDAD

1. Perdida de datos
2. Entrega de contraseñas vía telefónica o chat
3. Falta de capacitación, inducción y sensibilización sobre los riesgos
4. Acceso electrónico no autorizado a sistemas externos
5. Mal manejo de sistemas y herramientas
6. Compartir contraseñas o permisos a terceros no autorizados
7. Manejo inadecuado de datos
8. Utilización de programas no autorizados (Ilegales)

DESCRIPCION DE POLITICAS, CONTROLES, RECOMENDACIONES Y OPERACIONES BASICAS

El Instituto Financiero de Casanare cuenta en todas sus dependencias con información y procesos reservados que deben tener un manejo adecuado ya que son el activo principal de la entidad, para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios de los sistemas de información, como son la integridad, disponibilidad y confidencialidad de la información.

CONTROLES PARA COMPUTADORES, PORTATILES Y SERVIDORES

- El funcionario o contratista será el único responsable del equipo de cómputo asignado.
- Los equipos de cómputo son asignados de acuerdo al puesto de trabajo o función

laboral en su área de trabajo

- En caso que el usuario considere no tener los conocimientos suficientes y/o experiencia, se notificara al área de sistemas o al jefe inmediato quien será el responsable de realizar la capacitación correspondiente.
- Cada equipo tiene instalado el software y los aplicativos de acuerdo a las necesidades del área de trabajo o dependencia a la que pertenezca.
- En ningún caso el usuario en su área de trabajo y/o escritorio deberá tener bebidas, alimentos u otros materiales que puedan derramarse sobre el equipo.
- En caso de presentarse una falla física o lógica se deberá notificar al área de sistemas, o si el equipo debe ser entregado para revisión técnica se hará mediante procedimiento establecido.
- En ningún caso el usuario deberá intentar reparar el equipo o diagnosticarlo, únicamente debe reportar al área de sistemas la falla.
- Toda recepción de equipos de cómputo por adquisición para la entidad se realiza a través de almacén y con el apoyo del área de sistemas, como parte técnica.
- Cualquier persona que ingrese al instituto financiero de Casanare a prestar sus servicios profesionales por CPS en cualquiera de sus dependencias y que le sea exigido equipo portátil como herramienta de trabajo, primero que todo deberá registrar su equipo en el área de sistemas, teniendo su antivirus totalmente licenciado.
- Es responsabilidad del área de sistemas crear un usuario y una contraseña en el directorio activo (Usuario NT), para que la persona pueda ingresar a su escritorio remoto asignado.
- El centro de cómputo, oficina de sistemas y servidores son áreas restringidas, donde solo el personal autorizado por el área de sistemas podrá acceder a ellos por medio de la huella.

- Los equipos de cómputo asignados deberán ser usados para uso exclusivo de las funciones de la institución.
- Los funcionarios no deben mover o reubicar los equipos de cómputo, telecomunicaciones, impresoras, instalar ni desinstalar dispositivos, sin autorización del área de sistemas, en caso de ser requerir el servicio, solicitarlo a sistemas con previo aviso.
- Es responsabilidad de los funcionarios almacenar toda su información únicamente en la partición del disco duro en el servidor o equipo asignado, o en su defecto en la carpeta compartida (Publica) en la red.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- Queda prohibido que el usuario abra o desarme los equipos de cómputo, esta función es netamente del personal autorizado por el área de sistemas
- El área de almacén es el encargado de generar el resguardo de todos los activos informáticos que se le asignen de conservarlos en un área específica (Si así se requiere) por el área de sistemas.
- Es deber de los usuarios configurar (Manualmente) el bloqueo de pantalla para que se active a los 5 minutos como mínimo de inactividad y que requiera contraseña al reasumir actividades en el equipo.
- No está permitido el uso de módems en los equipos que tengan también conexión a la red, todas las comunicaciones de datos deben efectuarse a través de la red local (LAN) de la entidad, esto con el fin de prevenir la intrusión de hackers.
- Está prohibido el uso de dispositivos USB, por tal razón se tienen inhabilitados los puertos en todos los equipos de los funcionarios (Planta y CPS), si requieren copiar, mirar o modificar archivos en medios extraíbles (CD, USB), deben hacerlo con previa autorización desde uno de los equipos del área de sistemas, para así verificar de donde viene y para donde iría la información.
- Todo equipo portátil debe tener instalado su antivirus licenciado y verificado

desde el área de sistemas.

- Es responsabilidad del área de sistemas realizar copias de seguridad de los equipos de la entidad; en el IFC se realizan diariamente.
- Todos los equipos portátiles, Video Beam, mouse y teclados propiedad del IFC no podrán desplazarse si no es con previa autorización del área de sistemas, además debe diligenciar una planilla de salida y regreso
- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable de la terminal Tecnológica.
- Los encargados del área de sistemas, son los responsables de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo de la entidad.
- Los servidores deberán ubicarse en un área física que cumpla las normas para un centro de telecomunicaciones: Acceso restringido, Temperatura adecuada a los equipos, protección contra descargas eléctricas, mobiliario adecuado que garantice la seguridad de los equipos.

MANEJO Y CONTROL PARA LAS IMPRESORAS

- Todo documento impreso en el Instituto Financiero de Casanare debe ser de carácter institucional.
- Es responsabilidad del usuario conocer el uso adecuado del manejo de los equipos de impresión (Escáner y fotocopiado), de lo contrario que pida la asesoría desde el principio, esto con el fin de no afectar su correcto funcionamiento.

- Ningún usuario debe realizar labores de reparación o mantenimiento, en caso de presentarse alguna falla, esta se debe reportar al área de sistemas.

MANEJO Y CONTROL DE SWITCHES Y ROUTERS

- El área de sistemas es absolutamente responsable del manejo de todos los dispositivos de red de los que disponga el IFC, velando siempre por su correcto funcionamiento y porque estén en lugares seguros y protegidos tanto a nivel físico como lógico.
- Definir procedimientos de recuperación ante alguna eventualidad física que se llegase a presentar.
- Se debe asignar personal encargado de efectuar actividades tales como: instalación, desinstalación, mantenimiento y conexión física de este tipo de dispositivos.

USO DE INTERNET

- Siendo conscientes de que el uso de internet es una herramienta fundamental para el desempeño de labores, el área de sistemas del IFC cuenta con un firewall que limita el acceso de internet en las máquinas virtuales de los usuarios.
- Se prohíbe el acceso a sitios web como los son: Messenger, Facebook, youtube, twitter, chats, etc.
- Se prohíbe la descarga de archivos p2p, música, videos, pornografía, etc.

CORREO ELECTRONICO INSTITUCIONAL (Outlook)

El correo electrónico institucional es personal e intransferible, por tal motivo es deber de cada uno de los usuarios:

- El área de sistemas es el encargado de crear las cuentas de correo para aquellos usuarios a quienes les sea requerido dentro sus actividades a desempeñar dentro de la entidad.
- Mantener su uso y manejo de contraseña con privacidad
- Al enviar información, el único responsable es el usuario asignado a esa cuenta.

- Los mensajes enviados y archivos adjuntos deben ser de carácter institucional y manejados como comunicación privada y directa entre emisor y receptor
- No completar información, como datos personales de correos sospechosos.
- Solo se enviara y recibirá información de interés laboral.

IMAGEN INSTITUCIONAL

- Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean netamente institucionales.
- Cada usuario es responsable del cuidado de su herramienta de trabajo, por lo que se recomienda limpiar externamente el equipo de manera continua.
- Todos los accesorios de apoyo podrán tener plasmadas imágenes institucionales.

CONTROL Y USO DE CONTRASEÑAS

- El área de sistemas es el encargado inicialmente de generar y entregar al usuario las respectivas contraseñas de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.
- Los usuarios deben mantener sus contraseñas personales en secreto, las contraseñas que les sean otorgadas a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgadas, ni transferidas a ninguna persona, a menos que exista un requerimiento legal o un procedimiento que implique hacerlo.
- Los usuarios deben cambiar su contraseña de dominio cada vez que el sistema lo solicite, dicha frecuencia es establecida por el área de sistemas.
- El usuario puede solicitar directamente al área de sistemas asignación de una nueva contraseña en caso que la haya olvidado por completo.
- Las contraseñas son diseñadas de acuerdo a la complejidad de la misma y a ciertos parámetros de seguridad ya establecidos.

POLITICAS GENERALES

- Es deber de todos los usuarios y funcionarios cumplir con las políticas antes mencionadas, de lo contrario podrá ser acreedor a una sanción por parte de su jefe inmediato o por algún directivo de la entidad.

- Los líderes de cada área del Instituto Financiero de Casanare deben apoyar al cumplimiento de los lineamientos antes mencionados.
- El área de sistemas del IFC se mantendrá en contacto con los funcionarios para hacerles saber las nuevas disposiciones tecnológicas y de procedimientos dadas.

CONTROL DE CAMBIOS

Versión	Fecha [dd/mm/yy]	Elaborado por:	Razón de la actualización
0.0	29/12/2015	G ERIKA PILAR MADERO S. Profesional de apoyo área de sistemas	Versión Inicial
1.0	10/02/2022	ALEXANDER DELGADO OCHICA Ingeniero de sistemas	Revisión y ajuste de contenido.
1.1	31/01/2023	ALEXANDER DELGADO OCHICA Ingeniero de sistemas	Revisión y ajuste de contenido.
1.1	23/01/2022	MIRAMA LÓPEZ ZAMUDIO Subgerente Administrativa y Financiera.	Revisión y ajuste de contenido.