ifc

INSTITUTO FINANCIERO DE CASANARE

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023

Elaborado por	Revisado por	Aprobado por:
Nombre: G&H INVESTMENTS S.A.S Consultoría	Nombre: MIRAMA LOPEZ ZAMUDIO Cargo: Subgerente Administrativa y Financiera	Nombre: BRAULIO CASTELBLANCO VARGAS. Cargo: Gerente. Acta de comité institucional de Gestión y desempeño No. 03 del 30-01-2023.

CONTENIDO

INTRODUCCION

La política de Gobierno Digital (antes gobierno en Línea) es uno de los pilares del Estado en el proceso de transformación y modernización de las entidades públicas. Dentro de los elementos que conforman dicha política se encuentra el de Seguridad y Privacidad, el cual busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.[1]

El Instituto Financiero de Casanare (IFC) pensando siempre en la continua mejora de sus procesos, implementa un método sistematizado que permite identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a el manejo de la información interna, y de esta manera lograr evitar que estos no afecten de una manera relevante a la misma.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al

[1]Plan de seguridad y privacidad de la información https://www.agencialogistica.gov.co/sites/default/files/attachments/page/Plan%20de%20seguridad%20y%20privacidad%20de%20la%20informacion.pdf

materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio.

Dentro de sus actividades diarias, el instituto financiero hace uso de las TIC´S en cuanto a recolección, procesamiento, tratamiento y reporte de información que tanto interna como externamente debe ser comunicada a los diferentes entes de control de orden departamental y nacional, por lo tanto no se debe descartar la posibilidad de que esta información sea vulnerada a ataques mal intencionados o a una mala manipulación de la misma, lo que acarrea problemas económicos, legales, y administrativos para la entidad.

Este documento busca establecer una línea de trabajo que permita a la entidad evadir los riesgos que lo rodean y lograr que la información sea segura para quienes requieren y hacen uso de ella.

OBJETIVO

OBJETIVO GENERAL

Brindar al *Instituto Financiero de Casanare (IFC)* herramientas como el Modelo de Seguridad y Privacidad de la información (MSPI) que proporcionen las pautas necesarias para controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, con el fin de tener un enfoque de mejora continua.

OBJETIVOS ESPECIFICOS

- ✓ Describir el entorno general de la seguridad y privacidad de la información del Instituto Financiero de Casanare, así como el marco normativo aplicable.

- ✓ Definir las etapas para establecer y validar los recursos con los que cuenta actualmente el IFC y así poder desarrollar un plan de tratamiento de riesgo de seguridad y privacidad de la información

- ✓ Implementar el Modelo de Seguridad y privacidad de la Información en la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno Vive Digital.

- ✓ Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.

- ✓ Optimizar la gestión de la información al interior de la entidad

ALCANCE

Con el desarrollo de este manual, se busca orientar las actividades a desarrollar en el instituto financiero de Casanare en cuanto a la identificación de los posibles riesgos en la privacidad de la información, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

ABREVIATURAS

TI: Tecnologías de la Información

SI: Sistemas de Información

MSPI: Modelo de Seguridad y Privacidad de la Información

RESPONSABLES

Personas encargadas del control tecnológico de la Subgerencia Administrativa y Financiera, técnico de sistemas y/o personal contratado con actividades especificas

GLOSARIO

Los principios de protección de la información se enmarcan en:

- **Confidencialidad**: Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad**: Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad**: propiedad que la información sea accesible y utilizable en el momento que se requiera.

- **Activos tecnológicos o informáticos:** Se consideran activos tecnológicos o informáticos todos los elementos de hardware, software, información y de comunicaciones entregados por la entidad al funcionario con el fin de facilitarle el desempeño de sus funciones. De esta manera, son activos tecnológicos, además de los programas (software aplicativo y de ofimática), los computadores o equipos de cómputo junto con sus periféricos (tarjeta de red, mouse, teclado, monitor, parlantes, unidades externas de almacenamiento, micrófono, entre otros), impresoras, escáneres, etc. También los equipos y elementos de comunicaciones (telefonía, switches, routers, cableado, etc) y la información almacenada en los diversos equipos y bases de datos.[2]

- **Gobierno Digital:** Es una política del Estado Colombiano encaminada a promover el uso y aprovechamiento de las tecnologías de la información y

[2] Plan de seguridad y privacidad de la información

las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.[3]

- **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)[4]

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.[5]

CUMPLIMIENTO – NORMATIVIDAD

El instituto financiero de Casanare da cumplimiento a lo estipulado por la ley como entidad pública del estado, preservando y dando seguridad y privacidad a la información que allí se maneja.

[3] https://www.agencialogistica.gov.co/

[4] Plan de seguridad de la información https://www.agencialogistica.gov.co/

Código único disciplinario

- Articulo 34
- Articulo 35

Código penal colombiano

- Ley 1273 de 2009

Protección de datos

- Ley 1266 de 2008
- Ley 1581 de 2012
- Ley 1712 de 2014
- Decreto 1377 de 2013

Políticas públicas

- Decreto 1377 de 2013
- Decreto 1078 del 2015
- Decreto 32 del 2013
- Decreto 1008 del 2018, artículo 2.2.9.1.1.3.
- Circular 052
- Circular 042
- Resolución 305[6]
- Resolución 0500 de Marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones.

PERCEPCIONES

Aquellos pensamientos que se pueden llegar a tener cuando se habla de la seguridad y privacidad de la información de una empresa, aspectos de los cuales no nos debemos confiar. Por fortuna, en el Instituto Financiero de Casanare ha

[6] Taller de seguridad y privacidad de la información.
http://estrategia.gobiernoenlinea.gov.co/623/articles-9337_recurso_1.pdf

logrado sacar avante de la mejor manera los ataques externos, tomando medidas y correctivos que permiten mejorar la seguridad minimizando las posibilidades de robo o secuestre de información que pueda poner en riesgo la información e integridad que la entidad maneja sobre sus funcionarios y clientes.

1. Nuestra entidad no es blanco de ataques
2. No existe nada en la empresa que valga la pena que se roben
3. Las amenazas son solo externas
4. Tenemos instalado un firewall ...entonces estamos protegidos
5. Estamos gastando más que suficiente en seguridad
6. Si pasa algo, podemos asumir la perdida
7. Después de una falla podemos siempre restaurar el sistema
8. Los problemas ocasionados por el virus siempre son menores
9. Todos los problemas se solucionan comprando equipos. [7]

ERRORES COMUNES DE LOS USUARIOS

Los siguientes errores son los que humanamente cometemos, tal vez no con mucha frecuencia pero si es de prestar atención a ellos y darles la importancia pertinente, ya que esto sirve como puente en algunas ocasiones para que la seguridad y privacidad de la información de una entidad esté en riesgo.

1. Compartir el usuario y la contraseña

[7] Taller de seguridad y privacidad de la información
http://estrategia.gobiernoenlinea.gov.co/623/articles-9337_recurso_1.pdf

2. Abrir archivos adjuntos de correos de origen desconocido
3. Utilizar el correo institucional para enviar "SPAM"
4. Instalar software no autorizado
5. Subir a la nube información de trabajo
6. Conectarse a una red vía telefónica o Wireless mientras se está conectado a la LAN
7. Navegar en sitios "peligrosos"[8]

MARCO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El modelo de operación, contempla un ciclo de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

[8] Taller de seguridad y privacidad de la información
http://estrategia.gobiernoenlinea.gov.co/623/articles-9337_recurso_1.pdf

Ciclo de operación

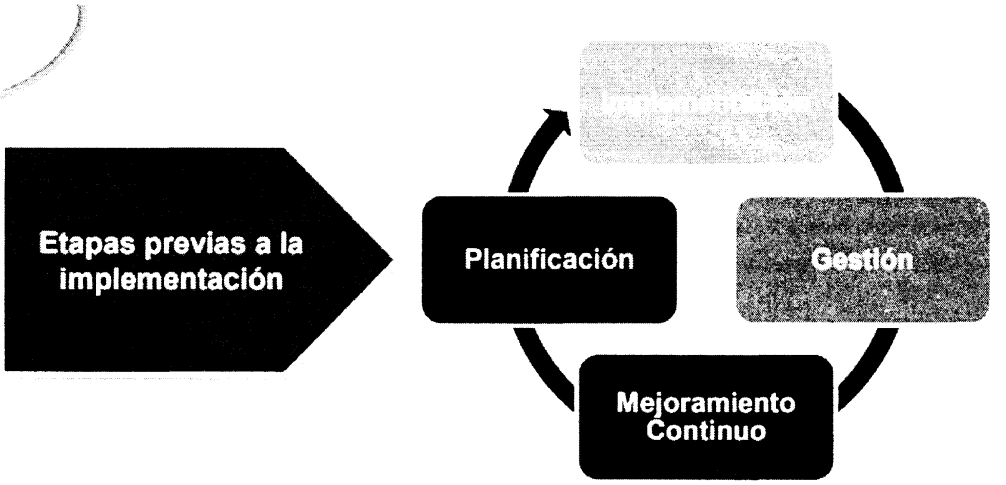


Figura 1. Marco del Modelo de Seguridad y Privacidad de Información
Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-9337_recurso_1.pdf

ETAPAS PREVIAS A LA IMPLEMENTACIÓN

Estado actual de la entidad

Como política de calidad el instituto financiero de Casanare contribuye al desarrollo productivo y social de la región y al mejoramiento de las competencias de sus habitantes, buscando la satisfacción de sus clientes a través de la prestación de servicios financieros, en el sector productivo y educativo y con la gestión de programas y proyectos mediante el uso eficiente de recursos, el compromiso del personal, la mejora continua, el cumplimiento normativo, manteniendo el sistema de gestión de calidad y propendiendo por el mejoramiento de la calidad de vida, el

crecimiento económico y organizacional que asegure la continuidad y reconocimiento institucional en el departamento.

Con base en esta política de calidad el instituto financiero se preocupa por brindar siempre un excelente y rápido servicio a sus clientes, haciendo uso de las tecnologías de la información (TI) a través de diferentes aplicaciones que permiten dar un manejo a la información suministrada tanto de usuarios como clientes de la entidad dentro de sus diferentes procesos administrativos y financieros.

Algunas de las aplicaciones utilizadas por los funcionarios del IFC son:

1. El ***Qfdocument*** que es la herramienta de consulta del sistema de digitalización de documentos, que permite masificar el uso del sistema aprovechando las ventajas de Internet, con una interface especialmente diseñada para facilitarle a los usuarios el desarrollo de las actividades que involucren todo tipo de documentos.

2. La empresa Solutions System vinculada al instituto financiero hace algunos años, proporciona una de las aplicaciones más importantes ***IAS*** para el manejo de información de cartera y créditos dentro de la entidad.

3. El ***spark*** el cual funciona como chat institucional, el cual permite no solo la comunicación escrita entre todas las dependencias y funcionarios de la entidad, sino la transferencia de archivos.

4. ***Outlook*** el cual funciona como correo institucional permitiendo ser otra línea de comunicación dentro de la entidad para uso exclusivo de directivos y funcionarios.

   Es de aclarar a quienes hacen uso del mismo, que no deben participar con correos electrónicos que inciten o incentiven el envío de cadenas o publicidad que no sean de interés o estén relacionados con el Instituto Financiero de Casanare (IFC).

IDENTIFICACIÓN DEL ESTADO DE MADUREZ DE LA INFORMACIÓN DE LA ENTIDAD

En el presente Modelo de Seguridad y Privacidad de la Información se contemplan diferentes niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

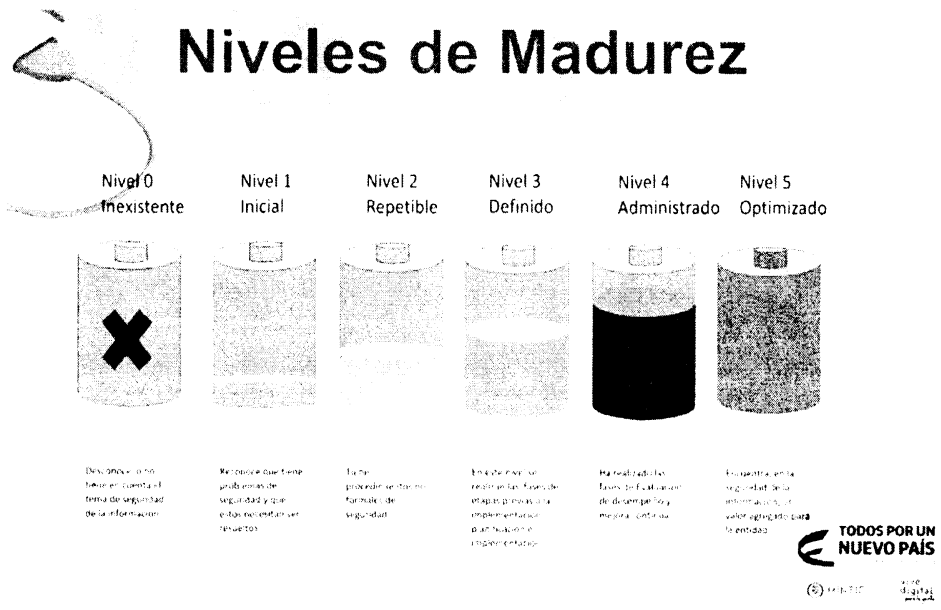


Figura 2 Niveles de Madurez
Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-9337_recurso_1.pdf

El esquema que muestra los niveles de madurez del MSPI, busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en una entidad del Estado.

En la tabla, se presentan los requerimientos de cada uno de los niveles de madurez con una descripción general.

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humano, entre otros. Sin embargo no están alineados a un modelo de seguridad. • No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información
Inicial	• Se han identificado las debilidades en la seguridad de la información • Los incidentes de la seguridad de la información se tratan de forma reactiva • Se tiene la necesidad de implementar el MSPI para definir políticas, procesos y procedimientos que den respuesta proactiva a la amenazas sobre seguridad de la información que se presente en la entidad.
Repetible	• Se identifican en forma general los activos de información • Se clasifican los activos de información • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
Definido	• La entidad ha realizado un diagnostico que le permite establecer el estado actual de la seguridad de la información • La entidad ha determinado los objetos, alcance y límites de la seguridad de la información • La entidad ha establecido formalmente políticas de seguridad de la información y estas han sido divulgadas • La entidad tiene procedimientos formales de seguridad de la información • La entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información • La entidad ha realizado un inventario de activos de información

Nivel	Descripción
	• La entidad trata riesgos de seguridad de la información a través de una metodología • Se implementa el plan de tratamiento de riesgos
Administrado	• Se revisa y monitorea periódicamente los activos de información de la entidad • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización • Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.

Tabla #1 Descripción de los niveles de madurez de una entidad
Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

Según la figura y analizando el estado actual de la entidad, el instituto financiero de Casanare se encuentra en un nivel de madurez #4 (Administrado) en cuanto al manejo de la seguridad y privacidad que le dan a la información.

Esto gracias a que el sistema de información (SI) que maneja la entidad cuenta tanto en su parte hardware como software con elementos que brindan soportes de seguridad, no solo en los cuidados de los activos tecnológicos, sino también las actualizaciones pertinentes que cada aplicación en uso va requiriendo

Se identifican los riesgos que puede llegar afectar los activos tecnológicos e informáticos que involucra manejo y privacidad de la información de la entidad y que en algún momento pudiesen llegarse a presentar, algo que hasta el momento no ha sucedido.

Levantamiento de información

El instituto financiero de Casanare actualmente dentro del área de sistemas con los siguientes activos tecnológicos para el manejo de la información.

Categorías de Activos	Código	Descripción
Datos	D1	Archivos digitales de respaldo de la contabilidad.
	D2	Archivo digital con información corporativa.
	D3	Archivos digitales con información corporativa.
	D4	Archivos digitales de clientes de la entidad
	D5	Archivos digitales con registro histórico de clientes de la entidad
	D6	Archivos digitales con registro histórico de clientes de la entidad
	D7	Archivos digitales con información de clientes de la empresa.
	D8	Archivos digitales con información de los correos corporativos.
Datos	D9	Archivo digital en red del Sistema de Gestión de Calidad
	D10	Archivo físico con información del Sistema de Gestión de Calidad
	D11	Archivos digitales de respaldo de la contabilidad.
	D12	Archivo digital con información presupuestal de la empresa.
	D13	Archivos físicos de respaldo de presupuesto
	D14	Extractos bancarios
	D15	Archivos físicos con información de los trabajadores
	D16	Archivos digitales con los procesos en tecnología
	D17	Archivos digitales con los procesos en tecnología

Servicios	S1	Página web
	S2	Correo corporativo.

	S3	Sistema financiero asociado al manejo de la información de la entidad (IAS Solutions)
	S4	Gestión Documental (QFDocument)
	S5	Conexión a base de datos asociada a la información financiera del instituto
	S6	Conexión a base de datos de entidades asociadas para el pago oportuno y otros cargos a favor de terceros.
	S7	Conexión a base de datos asociada a información de pólizas de clientes.
	S8	Scanner y Fotocopiado
	S9	Servicio de Conectividad a Internet (UTP-Wifi)

Software	SO1	Software de correo corporativo.
	SO2	Sistema operativo de los equipos de cómputo, Windows 7, Windows 8
	SO3	Office Profesional (2007, 2010 y 2013)
	SO4	Software antivirus ESET ENDPOINT
	SO5	Navegador (Explorer - Chrome - Mozilla)
	SO6	Servidor de archivos (ftp).
	SO7	Acrobat Reader X.
	SO8	Software integral de información financiera institucional (IAS Solutions)
	SO9	Software con información institución documental QFDocument
Software	SO10	VMWARE
	SO11	Software de Visitantes SV200
	SO12	Software de gestión del Control Biométrico
	SO13	ARCServer
	SO14	Windows Server 2012 R2
	SO15	Windows Server 2003
	SO16	Oracle Linux 6.0
	SO17	Gestor Unificado de Amenazas
	SO18	Software Winbox - WIFI
	SO19	CNT
	SO20	SHIP
	SO21	Circuito cerrado de TV
	SO2	Software calificador de servicio

Hardware	**Ha1**	Router.
	Ha2	Computadores.
	Ha3	Impresora/Scanner.
	Ha4	Impresora de red.
	Ha5	Fax.
	Ha6	Puntos de calificación
	Ha7	UPS
	Ha8	Servidores
	Ha9	Planta Telefónica
	Ha10	Planta eléctrica
	Ha11	Strip Telefónico
	Ha12	Televisores
	Ha13	Switch 3com
	Ha14	Patch Panel de Red y Comunicaciones
	Ha15	Cámaras de Seguridad

Redes de Comunicación	**RC1**	Celulares corporativos.
	RC2	Conexión a internet.
	RC3	Teléfono fijo.
	RC4	VPN.
	RC5	Conexión inalámbrica
	RC6	Red LAN
	RC7	Troncal SIP

FASE DE PLANIFICACION

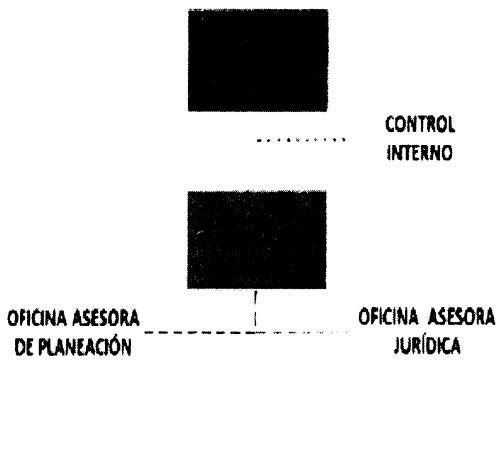
Contexto de la entidad

El Instituto Financiero De Casanare - IFC, es una empresa de Gestión Económica de carácter departamental, sometida al régimen jurídico de las empresas industriales y comerciales del Estado de acuerdo a la ley 489 de 1998. Es una entidad con personería jurídica, autonomía administrativa y patrimonio propio vinculada a la Secretaría de Agricultura Ganadería y Medio Ambiente de Casanare.

Se creó mediante el Decreto No. 107 de 27 de julio de 1992 inicialmente bajo el nombre de FONDESCA; nace de la necesidad de apoyar la ejecución de las políticas, planes y proyectos de índole Nacional, Departamental y Municipal diseñadas para fortalecer, articular y desarrollar el sector productivo de Casanare.

Con el propósito de ampliar su radio de acción y facultarlo para adquirir mayores compromisos, de acuerdo a las exigencias de la modernización Departamental, se reorganiza mediante el Decreto No. 0073 del 30 de mayo de 2.002 emanado de la Gobernación de Casanare y recibe el nombre de Instituto Financiero de Casanare. Como institución financiera líder que dota de las herramientas necesarias a la comunidad para el desarrollo de sus proyectos a través de financiación y asesoría crediticia con criterios de equidad, productividad, competitividad, sostenibilidad y participación de los sectores productivos.[9]

ORGANIGRAMA



[9] Página web Instituto Financiero de Casanare. http://www.ifc.gov.co/?idcategoria=92

POLÍTICAS DE SEGURIDAD

Las Políticas definidas en este documento incluyen las acciones que los funcionarios sin importar su tipo de vinculación y sin excepción alguna, deben adoptar y realizar para el manejo de los servicios y recursos informáticos que provee el IFC y de la información que allí se opera.

- ✓Los archivos descargados de Internet, deben ser verificados mediante antivirus antes de ser transmitidos a otro computador. En caso de detectarse virus que no puede ser removido, el archivo debe eliminarse por completo.
- ✓La información confidencial o de manejo especial de la organización no debe quedar residente en los servidores de intranet y/o Internet.
- ✓El área de Sistemas utilizará herramientas de monitoreo del uso de los recursos de internet, intranet y correo electrónico, por lo cual podrá establecer controles de acceso a páginas Web que considere degradan el desempeño de las conexiones a Internet o no son útiles para las labores del IFC.
- ✓Personal ajeno a el área de Sistemas no podrá registrar, publicar o poner en marcha sitios de Internet desde el Interior del IFC, al igual que el uso, registro, o puesta en marcha de nombres de dominios no autorizados o con alusiones directas o indirectas a el IFC.
- ✓Queda prohibido el uso de cuentas de correo electrónico personales y ajenas a las proporcionadas por el IFC, para cualquier trámite, trasmisión y/o recepción de información que utilicen datos o información del IFC.
- ✓La única dependencia autorizada para hacer uso de escáneres de redes, snifers, software de monitoreo de red y tráfico de red, sobre las redes de datos de la Entidad es el área de Sistemas.
- ✓Cada funcionario beneficiario del servicio de correo electrónico, tiene la obligación de notificar inmediatamente al área de Sistemas, de cualquier uso no autorizado de su contraseña o cuenta o de cualquier otro fallo de seguridad. De igual forma, debe asegurarse de que su cuenta sea cerrada al final de cada sesión. Cada usuario es único responsable de la pérdida o daño que resulte como consecuencia de su incumplimiento por el manejo seguro y adecuado de su casilla de correo asignada.

El área de Sistemas desactivará las cuentas de correo electrónico:

- ✓ Al funcionario que sea desvinculado, se le desactivará y borrará su cuenta previo backup de ésta realizado por la aplicación de correo.
- ✓ A los funcionarios que hayan infringido alguna de las condiciones aquí descritas, se les desactivará y borrará su cuenta previo backup de ésta realizado por la aplicación de correo.
- ✓ A los funcionarios que en un plazo mayor a un (1) mes, se detecte que no ha utilizado el servicio, se le desactivará y borrará su cuenta de correo.

Aspectos técnicos

- ✓ El acceso a Internet en cada una de las dependencias, deberá tener la configuración "Internet – dispositivo de conexión – firewall (software, hardware) – dispositivo de red - ...".
- ✓ Está prohibido la conexión a través de módems (dial-up) a estaciones de trabajo que estén simultáneamente conectadas a una red de área local o a otra red de comunicación interna. Las conexiones de computadores a contactos externos mediante módems o la instalación de software remoto para emular módems, deben ser debidamente aprobadas por el área de Sistemas, quien estipulará los mecanismos de seguridad apropiados.
- ✓ El IFC capacitará con frecuencia a sus funcionarios en el uso de las herramientas informáticas de las que se dispone.

Lineamientos generales

- ✓ Concierne al área de Sistemas gestionar que todo el software instalado en el IFC esté de acuerdo a la ley de propiedad intelectual a que dé lugar.
- ✓ El área de Sistemas administrará los diferentes tipos de licencias de software, número de usuarios y vigilará su vigencia.
- ✓ Los usuarios deben respetar las condiciones de licencia y copyright del software instalado en sus equipos. Así, ningún tipo de software no pueden ser copiados para fines personales o comerciales, con o sin ánimo de lucro.
- ✓ Cualquier software que requiera ser instalado para trabajar en los equipos de la Entidad deberá ser evaluado y autorizado por el área de Sistemas.

Adquisición de sistemas de información

Para la adquisición de Sistemas de Información, por parte del IFC se puede recurrir a la adquisición de aplicativos comerciales y/o adquirir aplicativos desarrollados a la medida.

En todo caso, la adquisición de cualquier tipo de sistema de información debe cumplir con las siguientes consideraciones básicas:

- ✓ Toda compra de software llevará la autorización y visto bueno del área de Sistemas.
- ✓ El área de Sistemas realizará la evaluación técnica de las necesidades presentadas, con el fin de obtener una definición clara de las mismas, dimensionamiento adecuado de la posible solución y requerimientos técnicos de hardware y software para su instalación.
- ✓ La relación contractual debe incluir como mínimo los siguientes compromisos por parte del proveedor:
- ✓ Declara compromiso de confidencialidad del sistema y la información.
- ✓ Constituir a favor del IFC un documento que exprese la licencia de uso o autorización del mismo, incluyendo como mínimo: Nombre del software, versión del producto, número de licencias y tiempo de licenciamiento.
- ✓ Brindar actualización y soporte técnico, por el término de un (1) año como mínimo.
- ✓ Capacitar y entrenar al personal involucrado en la instalación, operación, administración y desinstalación del sistema.
- ✓ Informar al IFC, a través del área de Sistemas, cuando el fabricante genere alguna nueva versión del sistema de información, y hacer entrega de medios magnéticos sin costo alguno para su respectiva instalación, durante la vigencia del licenciamiento.
- ✓ Entregar en idioma castellano, el manual técnico, de operación y del usuario.
- ✓ Instalar las licencias adquiridas y entregar los instaladores de las mismas al área de Sistemas del IFC.

Adquisición de software de ofimática

El IFC requiere para el normal funcionamiento de sus actividades, el uso de diversos software de propósito específico que demanda licenciamiento continuo, para lo cual se seguirán las siguientes directrices:

- ✓ Procurar comprar la última versión del software disponible en el mercado.
- ✓ Todo aplicativo orientado a garantizar la seguridad de la información deberá mantenerse actualizado.
- ✓ El IFC propenderá por el uso de software libre. Para dar cumplimiento a esta directriz, el área de Sistemas deberá incluir dentro de sus proyectos o planes de sistemas, la migración de herramientas de software a herramientas de libre licenciamiento

Software producido en el IFC

- ✓ Todo aplicativo, base de datos o herramienta de software, producido al interior de la Entidad por cualquier funcionario sin importar su tipo de vinculación, es propiedad del IFC y mantendrá los derechos que la ley de propiedad intelectual le confiera. Sólo se excluye esta directriz en caso que se hayan pactado otras condiciones en la obligación contractual firmada.
- ✓ La Oficina Jurídica en coordinación con el área de Sistemas deberá realizar el registro de los paquetes de programación de propiedad del IFC que así lo ameriten
- ✓ Los aplicativos que se desarrollen en el IFC, sólo se realizarán con la utilización de las herramientas de desarrollo disponibles para tal fin.

Derechos de autor

Concierne al área de Sistemas gestionar que todo el software instalado en el IFC esté de acuerdo a la ley de propiedad intelectual a que dé lugar. Cuando el IFC adquiera software desarrollado a la medida la documentación y el "Software" de propiedad del IFC incluirán avisos sobre derechos de autor y propiedad intelectual.

PLANEACIÓN Y SOPORTE

El proceso de gestión tecnológica es de vital importancia para el IFC, pues de él se deriva la seguridad y confianza a los clientes y público en general acerca de los servicios ofrecidos (transparencia), imagen favorable, generando credibilidad tanto

en los funcionarios, como en todas las personas que hagan parte de la entidad; a su vez es el área responsable de mantener una gestión de los procesos financieros eficaz y confiable, soportados con tecnología (continuidad del negocio y recuperación), como el manejo y control de posibles riesgos informáticos.

PROGRAMACIÓN MANTENIMIENTO PREVENTIVO

El Técnico de Sistemas elaborará un Programa Anual de Mantenimiento Preventivo con cubrimiento a toda la entidad, para ser desarrollado por personal del área o por contratación baja su supervisión, según disponibilidad de talento humano.

MANTENIMIENTO CORRECTIVO

CONCEPTO Acción de carácter puntual a raíz del uso, agotamiento de la vida útil u otros factores externos, de componentes, partes, piezas, y en general, de elementos que constituyen la infraestructura tecnológica, permitiendo su recuperación, restauración o renovación.
Requiere hacerse en el momento en que suceda cada evento por tanto para ello se llenará un formato Solicitud Soporte de Sistemas donde el responsable del equipo describa lo sucedido.

RESPONSABLE: Técnico de Sistemas

IMPLEMENTACION

EVALUACION Y CLASIFICACION DE LOS RIESGOS

CLASIFICACIÓN DE LOS RIESGOS

Para los efectos del presente manual los riesgos operacionales se clasifican de la siguiente manera:

Fraude interno: Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de IFC o incumplir normas o leyes, en los que está implicado al menos un empleado de la entidad.

Este evento se puede subdividir en los siguientes:

- ✓ Hurto.
- ✓ Desfalco.

- ✓ Sabotaje a la reputación de IFC
- ✓ Uso indebido a la propiedad intelectual.
- ✓ Fraude de programación de software.
- ✓ Mal uso de información privilegiada.
- ✓ Uso indebido de los bienes del Instituto.
- ✓ Manipular información dirigida a organismos de Vigilancia y control.

Fraude Externo: Actos realizados por una persona externa a IFC, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

Este evento se puede subdividir en los siguientes:

- ✓ Coerción.
- ✓ Hurto.
- ✓ Lavado de Activos.
- ✓ Terrorismo.
- ✓ Daño a la propiedad.
- ✓ Incendio premeditado.
- ✓ Falsificación de títulos valores.
- ✓ Mal uso de información confidencial.

GESTION

EVALUACION DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Dentro de las ***fortalezas*** con las que cuenta el IFC para prevenir estos riesgos y que aseguran que el tratamiento y seguridad de la información sea el adecuado están:

- ✓ El líder del proceso tiene la preparación adecuada y suficiente para las labores a ejecutar en el instituto, donde se destaca su conocimiento en redes y montaje de infraestructura tecnológica. Esto permite identificar, consolidar y validar propuestas de mejora dentro del área tecnológica de la entidad, al igual que implementar los proyectos para mejorarla.

- ✓ La solicitud y el préstamo de equipos a los funcionarios, además de la gestión del portal web del instituto, se realizan adecuadamente, garantizando los servicios requeridos por las demás áreas del instituto.
- ✓ Los procesos de apoyo se ejecutan y se llevan a cabo adecuadamente, dado al apoyo del Subgerente Administrativo y Financiero al área de sistemas y a sus propuestas de mejora y crecimiento en tecnología.
- ✓ El IFC cuenta actualmente con una infraestructura tecnológica y física adecuada, robusta y que ofrece confiabilidad a los demás procesos del instituto, destacando que ya está obsoleta afectando la eficiencia, eficacia, y aumentando gradualmente las posibilidades en riesgos informáticos e información.

MEJORAMIENTO CONTINUO

Se trabaja porque día a día el tratamiento y manejo que se la da a la información dentro del Instituto Financiero de Casanare sea transparente y el más óptimo para el éxito en sus procesos financieros, para que esto sea posible existen algunas fortalezas desde la parte de Mantenimiento y de protocolos de seguridad de la información que nos permiten dar un paso más, en cuanto a la seguridad y privacidad de la información

Mantenimiento Soporte Técnico y Gestión de la Infraestructura Física y Tecnológica

- ✓ El área de sistemas cuenta con procedimientos establecidos para cada una de las solicitudes especiales requeridas por la entidad. Dichos procedimientos tienen las actividades y eventos adecuados, según los requerimientos de mantenimiento y soporte técnico respectivo.

- ✓ El área de sistemas tiene la capacidad técnica y/o profesional para soporte técnico y mantenimiento. Además, cuenta con la información y el apoyo suficiente de los proveedores de servicios, al momento en que se requiera realizar un procedimiento de mayor tamaño y/o que necesite herramientas complementarias a las disponibles en el instituto.

Protocolos en seguridad de la información

- ✓ El área de sistemas cuenta con procedimientos y políticas en seguridad informática, como base a los lineamientos que debe llevar el instituto.

- ✓ Se está haciendo la transferencia de servicios tecnológicos a red Cisco y manejo de bases de datos de SQL Server a Oracle, lo cual permite aumentar la seguridad de los datos, mitigando riesgos referentes a copia o pérdida de información importante de la entidad.

- ✓ El área de sistemas cuenta con formatos para el registro de entrada y salida de equipos de la entidad. Igualmente, utilizan el registro biométrico para los funcionarios y el registro de visitantes y sus elementos al ingresar a las instalaciones. Esto permite mantener un control permanente sobre el ingreso por parte de visitantes a áreas restringidas de la entidad y sobre los elementos que ingresan y salen de las instalaciones.

- ✓ El instituto tiene servicio de seguridad privada, y cámaras de vigilancia, lo que permite un mayor control y vigilancia sobre los espacios generales de las instalaciones.

USO Y RECOMENDACIONES

1. ***Uso y protección de los equipos de cómputo***

   - En los equipos de cómputo propiedad del IFC únicamente se podrán instalar y utilizar software o programas, sistemas de información, herramientas de software que sean licenciados y autorizados por la entidad.

   - No podrán ser utilizados para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.

2. ***Uso de las Impresoras y servicio de impresión***

- Todo documento impreso en las impresoras del instituto financiero deberán ser de carácter institucional.

- Las labores de reparación y/o mantenimiento de las impresoras es de manejo exclusivo del equipo de sistemas y ningún funcionario o persona diferente al área de sistemas o contratado para tal fin podrá realizar dicha actividad.

3. ***Escritorios y Pantallas limpias***

- Los escritorios (puestos de trabajo) deberán estar en la medida de lo posible organizados y libres de la exposición de información documental que sea clasificada como confidencial.

- Las pantallas de los equipos de los usuarios deberán ser bloqueadas para aquellos momentos en que no esté utilizando el equipo o ante la ausencia del funcionario de su puesto de trabajo.

4. **Uso de Internet**

- IFC se reserva el derecho de realizar monitoreo o seguimiento de los accesos a sitios en internet realizados por parte de los funcionarios públicos.
- El acceso y uso del servicio de internet se concederá solo para propósitos laborales o fines particulares definidos y aprobados por IFC
- Se permitirá el acceso a servicios de internet, con lineamientos que garanticen la navegación y uso controlados de componentes del servicio.
- Se restringe toda posibilidad de descarga de software no autorizado o código malicioso en los equipos de cómputo del IFC.
- Crear un ambiente laboral hostil y/o exponer al IFC con acusaciones y actos de irresponsabilidad corporativa, por el acceso a material inadecuado, colocar información en la red que infrinja los derechos de los demás y/o la participación en foros a nombre de la entidad sin la debida autorización.

- Provocar deliberadamente el mal funcionamiento de computadores, estaciones o servidores de redes y sistemas.
- Dar a conocer información confidencial de la entidad.
- No se permite el acceso a sitios web con contenidos que están en contra de la ley, principios de ética moral del IFC tales como, pornografía, terrorismo, contenidos obscenos, discriminación racial o similar.

CONTROL DE CAMBIOS

Versión	Fecha [dd/mm/yy]	Elaborado por:	Razón de la actualización
0.0	15/11/2018	ERIKA PILAR MADERO SANABRIA Profesional de apoyo área 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	23/01/2023	MIRAMA LÓPEZ ZAMUDIO Subgerente Administrativo y Financiero	Revisión y ajuste de contenido