ESTADO PLURINACIONAL DE BOLIVIA

FONABOSQUE
Fondo Nacional de Desarrollo Forestal

RESOLUCIÓN ADMINISTRATIVA Nº 053

La Paz, 19 SEP 2018

VISTOS Y CONSIDERANDO:

Que el Artículo 103 parágrafo II que señala: *"El Estado asumirá como política de implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación".*

CONSIDERANDO:

Que la Ley N°164 de 28 de julio de 2011 establece en el artículo 72 parágrafo I: *"El Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales".*

Que el Decreto Supremo N°1793 de 13 de noviembre de 2013, señala en su artículo 4 parágrafo II inciso d) lo siguiente: *"Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento".* Asimismo el artículo 8 *del decreto referido señala: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".*

Que el Decreto Supremo N°3525 de 04 de abril de 2018, señala en su artículo 1: "*El presente Decreto Supremo tiene por objeto:* a) *Establecer la Política de Atención a la Ciudadanía: Bolivia a tu Servicio y el Portal de Trámites del Estado;* b) *Normar el archivo digital, la interoperabilidad y la tramitación digital. Asimismo el* artículo 3 del decreto referido señala: **"***El presente Decreto Supremo, tiene la finalidad de brindar mayor transparencia y fluidez en la interacción entre los administrados y el sector público, la transferencia de información entre entidades del Estado y entre éstas con la población, de acuerdo al ordenamiento jurídico de manera accesible e inmediata; y promover la celeridad de los trámites administrativos".*

Que el Decreto Supremo N°2514 de 09 de Septiembre de 2015, señala en su artículo 7 inciso i) las funciones de la AGETIC, *"Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática".*

CONSIDERANDO:

Que los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) señala como responsabilidades de la Máxima Autoridad Ejecutiva, en el numeral 6.1.1. Inciso g) *Aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución.* Asimismo el inciso h) refiere: *Cumplir y hacer cumplir el Plan Institucional de Seguridad de la Información de su entidad o institución.*

CONSIDERANDO:

Que la Ley Nº 1700, de 12 de Julio de 1996, Ley Forestal en su Artículo 23, parágrafo I, crea el Fondo Nacional de Desarrollo Forestal – FONABOSQUE, como entidad pública bajo la tuición

del Ministerio de Desarrollo Sostenible y Medio Ambiente, con personalidad jurídica de derecho público con autonomía técnica, administrativa, económica y financiera, con la finalidad de promover el financiamiento para la utilización sostenible y la conservación de los bosques y las tierras forestales. Su organización estará determinada en sus estatutos, aprobados mediante Decreto Supremo.

Que mediante Decreto Supremo N°2916 se aprueban los Estatutos del Fondo Nacional de Desarrollo Forestal – FONABOSQUE, que tienen por objeto establecer la estructura organizacional, técnica y operativa para el funcionamiento del Fondo Nacional de Desarrollo Forestal – FONABOSQUE y entre las funciones al Director General Ejecutivo establecidas en el artículo 7 señala: *"a) Ejercer la representación legal de la institución; g) Realizar y autorizar los actos administrativos necesarios para el funcionamiento de la institución; i) Aprobar el plan estratégico institucional, plan operativo anual, manuales internos, presupuesto y sus modificaciones".*

CONSIDERANDO:

Que mediante Informe DGE-JNCT-134-INF/18 de 18 de septiembre de 2018 el Responsable de Seguridad de la información, adjunta el Plan Institucional de Seguridad de la Información y solicita al Comité de Seguridad de la Información conformado mediante Resolución Administrativa Nº 52/2018 de 17 de septiembre de 2018, su revisión para posterior aprobación por la Máxima Autoridad Ejecutiva.

Que el Comité de Seguridad de la Información se reunió a efectos de la revisión del Plan Institucional de Seguridad de la Información (PISI) del FONABOSQUE, estableciendo que corresponde su aprobación previa remisión al área legal para la elaboración de la Resolución Administrativa correspondiente.

Que mediante Informe Legal DGE-AL- KGM-0360-INF/18 de 19 de septiembre de 2018, se concluye y recomienda que se suscriba la correspondiente Resolución Administrativa para la aprobación del Plan Institucional de Seguridad de la Información (PISI) del Fondo Nacional de Desarrollo Forestal FONABOSQUE.

POR TANTO:

El Director General Ejecutivo del FONABOSQUE, en ejercicio y uso pleno de sus facultades, atribuciones y funciones conferidas y la designación efectuada mediante Resolución Suprema Nº23807 de 11 de junio de 2018.

RESUELVE:

PRIMERO.- Aprobar el Plan Institucional de Seguridad de la Información (PISI) del Fondo Nacional de Desarrollo Forestal FONABOSQUE.

SEGUNDO.- Designar al Responsable de Seguridad de la Información (RSI), como el encargado de la Implementación del Plan Institucional de Seguridad de la Información (PISI) en el Fondo Nacional de Desarrollo Forestal – FONABOSQUE.

Regístrese, comuníquese, cúmplase y archívese.

ASESORA LEGAL
FONABOSQUE

Lic. Mike Alejandro Gemio Pérez
DIRECTOR GENERAL EJECUTIVO
FONABOSQUE

FONABOSQUE

Políticas de Seguridad

Introducción

El Parágrafo I del Artículo 72 de la Ley N° 164 de 28 de julio de 2011, Ley General de Telecomunicaciones, que establece que: "El Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales".
El inciso d) del Artículo 4 (Principios), parágrafo II, del Decreto Supremo N° 1793 de 13 de noviembre de 2013, que señala que: "Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento".
El Artículo 8 (Plan de contingencia) del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que menciona que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".
El Fondo Nacional de Desarrollo Forestal- FONABOSQUE, como entidad descentrlizada del Ministerio de Medio Ambiente y Agua encargada de promover, administrar y otorgar recursos financieros para el manejo sustentable de bosques, con enfoque de gestión integral de cuencas, conservación de los bosques y suelos forestales, recuperación de suelos degradados en áreas forestales y manejo integral del fuego , considera que la información es vital para el desarrollo de sus actividades, en razón a que es una herramienta de gran importancia para la toma de decisiones, motivo por el cual, el FONABOSQUE está comprometido a proteger los activos de información de la entidad, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad de la información.
En este sentido la institución ha generado transitoriamente este documento de politicas de seguridad de la información como una politica basica por el cual se enmarca las actividades de manejo de información.

Términos y Definiciones

Información: la información es la interpretación que se da a un conjunto de datos, pudiendo residir esta en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos del FONABOSQUE generados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.
Seguridad de la Información: es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad de la institución, minimizar el daño y, cumplir su misión y objetivos estratégicos.
Confidencialidad: es asegurar que la información es accesible sólo para las personas autorizadas para ello.
Integridad: es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.
Disponibilidad: es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos.
Personal interno o funcionario: es toda persona a la cual se le concede autorización para acceder a la información y a los sistemas del FONABOSQUE. El personal puede ser interno o externo a la institución.
Responsable de la Información: es el usuario a cargo de la información y de los procesos que la manipulan sean estos manuales, mecánicos o electrónicos.
Encargado de Seguridad: es la persona que la autoridad máxima de la institución designa para la definición, diseño, implementación y supervisión de las medidas de seguridad de la información.
Comité de Seguridad: es el equipo conformado por la MAE, coordinadores que representan a las áreas de la institución, responsable de la toma de decisiones en temas de la seguridad de la información.
Activo de Información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
Podemos distinguir 3 tipos de activos:
a) La Información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, etc.).
b) Los Equipos/Sistemas que la soportan.
c) Las Personas que la utilizan.

Los activos poseen valor para la institución, y necesitan por tanto ser protegidos adecuadamente, para que el FONABOSQUE no se vea perjudicado (implica detectar vulnerabilidades y establecer controles).

Objetivo general

Determinar los lineamientos que permitan proteger la Información del FONABOSQUE a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad.

Objetivos específicos

-Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios respecto al correcto manejo y protección de la información que es gestionada y resguardada en el FONABOSQUE.
-Idententificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.
-Proteger la información y los activos tecnológicos de la Institución.
-Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad.

Alcance

La Política de Seguridad de la Información aplica a todo el FONABOSQUE y sus funcionarios, contratistas y pasantes, que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Institución.

Roles y Responsabilidades

RESPONSABILIDADES OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
Establecer, mantener y divulgar las políticas de seguridad de información, el uso de los servicios tecnológicos en toda la institución.
-Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la DGE y diferentes Coordinaciones del FONABOSQUE.
-Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital del FONABOSQUE.
-Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información del FONABOSQE.
-Brindar el soporte necesario para garantizar el funcioanmiento de los equipos de computación como de los sistemas de información implementados en la institución.

RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN
Son propietarios de la información cada uno de las coordinaciones así como los jefes de las areas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.
-Valorar y clasificar la información que está bajo su administración y/o generación
RESPONSABILIDADES DE LOS FUNCIONARIOS
-Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas.
-Manejar la Información de la Institución y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
-Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido
-Evitar la divulgación no autorizada o el uso indebido de la información.
-Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
-Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico científicos designados para el desarrollo de sus funciones.
-Usar software autorizado por el area de Tecnologias. No está permitido la instalación ni uso de software sin el consentimiento de sus superiores y visto bueno de la Oficina de Tecnologías.

Desarrollo

Ámbito de Seguridad / Descripción	Postura Institucional	Estado
1. Seguridad en recursos humanos	El FONABOSQUE implementa acciones para asegurar que los	No Utiliza

Ámbito de Seguridad / Descripción	Postura Institucional	Estado
Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.	funcionarios de la Entidad, entiendan sus responsabilidades, como usuarios y responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones. Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información. Se debe asegurar que los funcionarios adopten sus responsabilidades en relación con las políticas de seguridad de la información En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá aplicar las normas que reglamenten los procesos disciplinarios para los funcionarios del estado. El funcionario debe entregar los activos de información de acuerdo procedimiento de terminación o cambio de empleo de acuerdo al formato Informe de Entrega por desvinculación.	
2. Gestión de activos de información Con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y asignar responsabilidades en el uso y protección de los mismos.	El FONABOSQUE es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas. El FONABOSQUE es propietario de los activos de información y los administradores de estos activos son los funcionarios que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).	Utiliza
3. Control de accesos Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.	El FONABOSQUE define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataformas informáticas considerándolas como importantes para la seguridad de la información. La conexión remota a la red de área local del FONABOSQUE debe realizarse a través de una conexión VPN segura y suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por el Área de Tecnologías y Sistemas de información. Todo aplicativo informático o software debe ser comprado o aprobado por el Área de Tecnologías y Sistemas de información en concordancia con la política de adquisición de bienes de la entidad. Ningún usuario deberá acceder a la red o a los servicios TIC del FONABOSQUE, utilizando una cuenta de usuario o clave de otro usuario. El area de Tecnologias suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Las claves o contraseñas deben: Tener mínimo ocho (8) caracteres alfanuméricos. Cada vez que se cambien estas deben ser distintas por lo menos de las últimas cinco anteriores	No Utiliza
4. Criptografía El uso de técnicas criptográficas aporta mayores niveles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación.	EL area de Tecnologías de Información y Comunicación debe realizar un analisis de la pertinencia de utilizar criptografia en los datos enviados y recibidos por los canales de comunicacion electrónica.	No Utiliza
5. Seguridad física y ambiental Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.	El area Administrativa debe implementar un sistema de seguridad física para las instalaciones del FONABOSQUE. El Área de Tecnologías y Sistemas de Información debe implementadas alarmas de detección de intrusos a los centros de datos y centros de cableado del FONABOSQUE. En las instalaciones del centro de datos o de los centros de cableado, No está permitido: • Fumar dentro del Data Center. • Introducir alimentos o bebidas al Data Center • Mover, desconectar y/o conectar equipo de cómputo sin autorización. • Modificar la configuración del equipo o intentarlo sin	Utiliza

Ámbito de Seguridad / Descripción	Postura Institucional	Estado
	autorización. • Alterar software instalado en los equipos sin autorización. • Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas. Extraer información de los equipos en dispositivos externos. • Abuso y/o mal uso de los sistemas de información. • Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.	
6. Seguridad de las operaciones Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.	El area de Tecnologías debe definir las reglas para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento y uso de equipamiento informatico del FONABOSQUE.	No Utiliza
7. Seguridad de las comunicaciones Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.	-Los procedimientos y responsabilidades de operación y administración de la plataforma tecnológica y de seguridad deben estar documentados, garantizando un adecuado control de cambios. -A efectos de proteger la integridad y confidencialidad de los activos de información es imprescindible que se cuente con protecciones contra software de seguridad mantenimiento de los equipos, administración de la red y bloqueo de puertos en la red de telecomunicaciones. -El Proceso de TICs debe ser la encargado de bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. -Toda adquisición, mantenimiento y eliminación de medios de almacenamiento deberá ser realizada por el proceso de Gestión de TICs, de manera que se garantice seguridad en estos activos de información.	No Utiliza
8. Desarrollo, mantenimiento y adquisición de sistemas Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos.	El FONABOSQUE debe asegurar que se haga el diseño e implementación de los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación y autorización de perfiles de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro. -El FONABOSQUE, debe establecer controles para cifrar la información que sea considerada sensible y evitar la posibilidad de alteración de una acción por parte de un usuario del sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse. -La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como el desarrollo de soluciones. -La información tratada por las aplicaciones aceptadas por el FONABOSQUE, debe preservar su confiabilidad desde su ingreso, transformación y entrega a las aplicaciones de la Entidad.	No Utiliza
9. Gestión de incidentes de seguridad de la información Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la institución o entidad pública para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.	El FONABOSQUE debe asegurar que se establecen y ejecutan procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información. -Todos los usuarios de la información del FONABOSQUE deben reportar los incidentes de seguridad que se presenten.	No Utiliza
10. Plan de contingencias tecnológicas Implementar un Plan de Contingencias Tecnológicas que permita controlar un incidente de seguridad de la información o una situación de emergencia, minimizando sus consecuencias negativas. Asimismo deberá determinar	El Plan de Contingencias de Tecnologías de Información y Comunicación del FONABOSQUE incluye al menos una prueba al año. La prueba dependerá de lo que se quiera ensayar y consiste en llevar a cabo simulacros de:	No Utiliza

Ámbito de Seguridad / Descripción	Postura Institucional	Estado
sus requisitos para la seguridad de la información ante situaciones adversas.	1. Recuperación de la información de las copias de seguridad para verificar su correcto proceso de restauración. 2. Puesta en producción de los equipos de respaldo de los sistemas de información críticos del FONABOSQUE. 3. Pruebas de suministro de energía eléctrica con UPS. 4. Conectar los equipos en un switch administrable.	
11. Cumplimiento Asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma.	El FONABOSQUE, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo entre otros los derechos de propiedad intelectual, protección de datos linstitucionale, el uso inadecuado de recursos de procesamiento y el uso de criptografía. -Cumplimiento de la normatividad y los controles relacionados con la seguridad de la información y los que son técnicamente compatibles con los diferentes ambientes o tecnologías de la entidad. -Realización de auditorías, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información. -Estas políticas junto a todo el PLAN INSTITUCIONAL DE SEGURIDAD DE INFORMACION DEL FONABOSQU, debe ser auditado anualmente para verificar su cumplimiento y determinar su actualización y aplicación. -La información de auditoría generada por el uso de los controles de seguridad de los Recursos de Tecnología, debe ser evaluada por el Responsable para: * Detectar Violaciones a la Política. * Reportar incidentes de seguridad. Los contratos de trabajo de consultores de linea y por producto deben contar con cláusulas respecto a la propiedad intelectual que le pertenece al FONABOSQUE.	No Utiliza

Difusión

La MAE sera la encargada de realizar la difusión del presente documento inicial de politicas de seguridad de la información.

Cumplimiento

La presente Política General de Seguridad de la Información entra en vigencia una vez aprobado por la MAE y el Comite de Seguridad de la Información.

Sanciones

Las sanciones al incumpimiento de la presente politica sera completada previa consulta ante la MAE y Coordinadores y jefes del FONABOSQUE bajo el asesoramiento de la Undad Legal, en un plazo no mayor a un año posterior a la aprobación.

Histórico de Cambios

Fecha	Formulario	Estado	Encargado
2018-09-19	Políticas de Seguridad	EN_REVISION	Justo Nicanor Colquehuanca Ticona
2018-09-19	Políticas de Seguridad	APROBADO	Patricia Santader

Metodología de Gestión de Riesgo

El PISI contempla la gestión de riesgos en el ámbito de la seguridad de la información. Para esto, se adopta la metodología de gestión de riesgos propuesta dentro de los Lineamentos para la Elaboración e Implementeación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, con el objetivo de implementar controles de seguridad o mejorar la eficacia de los controles ya existentes.

La evaluación del riesgo permitirá identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces, además de determinar y categorizar las amenazas potenciales y vulnerabilidades asociadas a activos de información.

El resultado de este proceso permitirá determinar la identificación de controles que reducirán los riesgos.

Identificación, Clasificación y Valoración de Activos de Información

El RSI, de forma conjunta con los responsables de los procesos identificados dentro del alcance del Plan Institucional de Seguridad de la Información, coordinó el proceso de identificación, clasificación y valoración de activos de información, haciendo uso de la guía incluida en el Anexo B de los Lineamentos para la Elaboración e Implementeación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.

La identificación determina qué activos de información formarán parte del PISI haciendo uso de una clasificación.

La valoración de activos de información tiene como objetivo asegurar que la información asociada a los mismos reciba niveles de protección adecuados.

Se valorara los activos de la información en las dimensiones que requiere la institución (Disponibilidad, Integridad y Confidencialidad).

La valoración presenta una escala para la valoración cuantitativa de las características del activo de información.

#	Activo	Descripción	Tipo	Ubicación	Unidad Responzable	Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad	Valoración Final	Fecha inicial	Fecha final
1	Archivos documentales del FONABOSQUE	Es el conjunto de todos los documentos fisicos que se tiene en el area ARCHIVO CENTRAL	Información	Se encuentra en el piso 2 de las oficinas de FONABOSQUE y carece de medidas de seguridad tanto de acceso fisico como de acceso a la información propiamente dicha	Area de Archivos	Luis Vera, Encargado de Archivos	Encargado de Archivos	ALTO	ALTO	MEDIO	3.67	2018-11-01	2019-02-28

Evaluación del Riesgo

El responsable del activo de información determina; en base a sucesos, y la importancia que tiene el activo sobre las posibles amenazas y vulnerabilidades a las que está expuesto y realiza una descripción del escenario en el cual se puede dar la materialización de la amenaza, asumiendo que el responsable conoce y entiende los riesgos sobre el activo.La entidad o institución pública

Una vulnerabilidad es toda aquella debilidad que presenta el activo de información, dada comúnmente por la inexistencia o ineficacia de un control.

Una amenaza es todo elemento que haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, independientemente de que se comprometa o no la seguridad de un sistema.

Evaluación del Riesgo la metodología seleccionada realiza la identificación, análisis y valoración de los riesgos asociados a los activos de información previamente identificados, clasificados y valorados y permite identificar amenazas y vulnerabilidades.

La Identificación del Riesgo se toma en cuenta las vulnerabilidades y amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información.

Análisis y Valoración del Riesgo evalúa las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades presentes en los activos de información.

La priorización esta claramente establecida a partir del nivel de riesgo máximo definido previamente por la entidad o institución pública a través del CSI.

Prioritarios

#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de riesgo
1	Archivos documentales del FONABOSQUE	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion	Muy Probable	Severo	ALTO
2	Archivos documentales del FONABOSQUE	Deterioro fisico por algun incidente natural	Como no esta protegido fisicamente los estantes del archvo central hay riesgo de que la documentacion fisica	perdida de la consistencia fisica de documentacion	Probable	Moderado	MEDIO
3	Archivos documentales del FONABOSQUE	por falta de digitalización existe deterioro fisico de los documentos	Como los documentos no estan digitalizados y cuando algun funcionario o persona externa a la institución desea prestarse alguna documentacion, el encargado de archivos presta los originales y con uso se deterioran	Deterioro fisico lo que conduce a una perdida parcial o total de la informacion	Cierta/ Inminente	Crítico	CRÍTICO
4	Archivos documentales del FONABOSQUE	Indisponibilidad de informacion digital de la memoria institucional fisica que se encuentra en el archivo central	Como toda la documentacion no esta digitalizada no se cuenta con una plataforma de repositorio virtual para almacenar los documentos y el contenido de los mismos	Indisponibilidad de la informacion para su facil acceso	Cierta/ Inminente	Crítico	CRÍTICO

No prioritarios

#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de riesgo

Matriz de Valoración del Riesgo

Cierta/Inminente	BAJO	MEDIO	ALTO	CRÍTICO	CRÍTICO 3, 4
Muy Probable	BAJO	MEDIO	ALTO	ALTO 1	CRÍTICO
Probable	IRRELEVANTE	BAJO	MEDIO 2	ALTO	ALTO
Poco Probable	IRRELEVANTE	BAJO	BAJO	MEDIO	MEDIO
Improbable	IRRELEVANTE	IRRELEVANTE	IRRELEVANTE	BAJO	BAJO
	Irrelevante	Menor	Moderado	Severo	Crítico

Tratamiento de Riesgo

Se tomarón decisiones acerca de las medidas más apropiadas para el tratamiento del riesgo identificado.

El tratamiento del riesgo implica tomar decisiones para aceptar, reducir, retener, evitar o transferir los riesgos.

Nro	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo	Control
1	Archivos documentales del FONABOSQUE	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion	Muy Probable	Severo	ALTO	5.1.1.iii. Identificar las áreas e instalaciones consideradas seguras o críticas. 5.1.1.iv. Elaborar procesos/ procedimientos de acceso a las diferentes áreas e instalaciones según las características de seguridad de la información. 5.1.1.viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente. 5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente. 5.1.1.xi. Los ingresos y salidas de visitas deberán ser registradas, autorizadas y controladas. Asimismo deberán portar la identificación de visitante en lugar visible. 5.1.1.xii. Los servidores públicos deberán portar la identificación correspondiente en un lugar visible. 5.1.1.xiii. La seguridad fisica perimetral de la entidad o institución pública deberá inspeccionar y verificar el ingreso de elementos que comprometa la seguridad. 5.1.1.xvii. Contar con señalética visible, para evacuaciones o contingencias de la institución.
2	Archivos documentales del FONABOSQUE	Deterioro fisico por algun incidente natural	Como no esta protegido fisicamente los estantes del archvo central hay riesgo de que la documentacion fisica	perdida de la consistencia fisica de documentacion	Probable	Moderado	MEDIO	5.1.1.viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente. 5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente. 5.1.1.xvii. Contar con señalética visible, para evacuaciones o contingencias de la institución.
3	Archivos documentales del FONABOSQUE	por falta de digitalización existe deterioro fisico de los documentos	Como los documentos no estan digitalizados y cuando algun funcionario o persona externa a la	Deterioro fisico lo que conduce a una perdida parcial o total de la informacion	Cierta/ Inminente	Crítico	CRÍTICO	2.3.1.i. Elaborar procedimientos de uso de medios removibles donde mínimamente se establezcan quién, cómo, cuándo y para qué se accede a esos medios.

Nro	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo	Control
			institución desea prestarse alguna documentacion, el encargado de archivos presta los originales y con uso se deterioran					
4	Archivos documentales del FONABOSQUE	Indisponibilidad de informacion digital de la memoria institucional fisica que se encuentra en el archivo central	Como toda la documentacion no esta digitalizada no se cuenta con una plataforma de repositorio virtual para almacenar los documentos y el contenido de los mismos	Indisponibilidad de la informacion para su facil acceso	Cierta/ Inminente	Crítico	CRÍTICO	2.2.1.i. Elaborar un procedimiento de clasificación de la información institucional, que contenga los requisitos, nivel de clasificación, los responsables, las restricciones y la gestión de la información en general. 2.2.1.ii. Establecer requisitos de protección para cada nivel de clasificación definido que deberán considerar las necesidades de la entidad o institución pública respecto a la apertura o restricción de la información. 2.2.1.iii. Reclasificación de la información de acuerdo a requerimiento y/o normativa vigente.

Listado de Controles Implementados y por Implementar

Control	SI/NO	Justificación
5.1.1.iii. Identificar las áreas e instalaciones consideradas seguras o críticas.	si	
5.1.1.iv. Elaborar procesos/procedimientos de acceso a las diferentes áreas e instalaciones según las características de seguridad de la información.	si	
5.1.1.viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente.	si	
5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.	si	
5.1.1.xi. Los ingresos y salidas de visitas deberán ser registradas, autorizadas y controladas. Asimismo deberán portar la identificación de visitante en lugar visible.	si	
5.1.1.xii. Los servidores públicos deberán portar la identificación correspondiente en un lugar visible.	si	
5.1.1.xiii. La seguridad fisica perimetral de la entidad o institución pública deberá inspeccionar y verificar el ingreso de elementos que comprometa la seguridad.	si	
5.1.1.xvii. Contar con señalética visible, para evacuaciones o contingencias de la institución.	si	
5.1.1.viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente.	si	
5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.	si	
5.1.1.xvii. Contar con señalética visible, para evacuaciones o contingencias de la institución.	si	
2.3.1.i. Elaborar procedimientos de uso de medios removibles donde mínimamente se establezcan quién, cómo, cuándo y para qué se accede a esos medios.	si	
2.2.1.i. Elaborar un procedimiento de clasificación de la información institucional, que contenga los requisitos, nivel de clasificación, los responsables, las restricciones y la gestión de la información en general.	si	
2.2.1.ii. Establecer requisitos de protección para cada nivel de clasificación definido que deberán considerar las necesidades de la entidad o institución pública respecto a la apertura o restricción de la información.	si	
2.2.1.iii. Reclasificación de la información de acuerdo a requerimiento y/o normativa vigente.	si	

Controles Implementados y por Implementar

Directriz				
2.2.1.i. Elaborar un procedimiento de clasificación de la información institucional, que contenga los requisitos, nivel de clasificación, los responsables, las restricciones y la gestión de la información en general.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	CRÍTICO	Indisponibilidad de informacion digital de la memoria institucional fisica que se encuentra en el archivo central	Como toda la documentacion no esta digitalizada no se cuenta con una plataforma de repositorio virtual para almacenar los documentos y el contenido de los mismos	Indisponibilidad de la informacion para su facil acceso
Desarrollo				
1.- Organización de los archivos fisicos de acuerdo a la tematica o areas técnicas y administrativas del FONABOSQUE 2.- Adquisicion de un escanner de alto trafico que sirva para la digitalización de los archivos fisicos, segun la organizacón realizada. 3.- Digitalizar o escanear toda la documentación contenida en los archivos fisicos. 4.- Implementar una plataforma para la gestión documental 5.- Configurar la plataforma para la clasificación de la documentacion digitalizada 6.- Registro en la plataforma de toda la documentacion digitalizada y ordenada segun configuración				

Directriz				
2.2.1.ii. Establecer requisitos de protección para cada nivel de clasificación definido que deberán considerar las necesidades de la entidad o institución pública respecto a la apertura o restricción de la información.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	CRÍTICO	Indisponibilidad de informacion digital de la memoria institucional fisica que se encuentra en el archivo central	Como toda la documentacion no esta digitalizada no se cuenta con una plataforma de repositorio virtual para almacenar los documentos y el contenido de los mismos	Indisponibilidad de la informacion para su facil acceso
Desarrollo				
1.- Una vez que se tenga el archivo central digitalizado y automatizado, se debera establecer el ingreso a la plataforma con acceso restringido a usuarios que van a alimentar al sistema, usuarios que van a administrar el sistema y usuarios que solamente van a tener acceso de solo lectura de la documentación. 2.- Ingreso fisico a las oficinas o area de archivos estara restringido a traves de una chapa con llave que solamente tendran las copias el encargado de archivos y el Coordinador Administrativo Financiero.				

Directriz				
2.2.1.iii. Reclasificación de la información de acuerdo a requerimiento y/o normativa vigente.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	CRÍTICO	Indisponibilidad de informacion digital de la memoria institucional fisica que se encuentra en el archivo central	Como toda la documentacion no esta digitalizada no se cuenta con una plataforma de repositorio virtual para almacenar los documentos y el contenido de los mismos	Indisponibilidad de la informacion para su facil acceso
Desarrollo				
1.- Implementar la plataforma de gestion documental y disponibilizar en el servidor interno par su acceso a la información. 2.- El acceso a la información de la plataforma sera a tres niveles, un administrador que pueda confgurar el sistema, un nivel de alimentadores de información que vana subir documentos al sistema y un nivel de lectores que solamente podran leer y bajar informacion del sistema.				

Directriz				
2.3.1.i. Elaborar procedimientos de uso de medios removibles donde mínimamente se establezcan quién, cómo, cuándo y para qué se accede a esos medios.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	CRÍTICO	por falta de digitalización existe deterioro fisico de los documentos	Como los documentos no estan digitalizados y cuando algun funcionario o persona externa a la institución desea prestarse alguna documentacion, el encargado de archivos presta los originales y con uso se deterioran	Deterioro fisico lo que conduce a una perdida parcial o total de la informacion
Desarrollo				
1.- Digitalizar todos los documentos de la memoria institucional y tener en formato digital la copias de los documentos para posteriormente se pueda entregar algun funcionario que requiera tener una copia del documento.				

Directriz				
5.1.1.iii. Identificar las áreas e instalaciones consideradas seguras o críticas.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- Instalación de mamparas en las oficina del archivo central para asegurar fisicamente el area donde se encuentran los archivos fisicos. 2.- Instalar una puerta de acceso a las oficinas del archivo central con chapa y dos llaves (una que lo tenga el encargado del archivo central y otra copia que lo tenga el Coordinador Administrativo Financiero). 3.- Instalación de camaras de seguridad que grabe en video quienes ingresan y salen de las oficinas del archivo central de la institución. 4.- Instalación de alarma con sensores de movimiento para la restricción de acceso a personal no autorizado en horas fuera de oficina.				

Directriz				
5.1.1.iv. Elaborar procesos/procedimientos de acceso a las diferentes áreas e instalaciones según las características de seguridad de la información.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- Elaborar procesos y procedimientos para el ingreso y gestión documental del area de archivos a ser realizado por el encargado de archivos en coordinacion con el area de Gestión Institucional y Desarrollo Organizacional				

Directriz				
5.1.1.viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	MEDIO	Deterioro fisico por algun incidente natural	Como no esta protegido fisicamente los estantes del archvo central hay riesgo de que la documentacion fisica	perdida de la consistencia fisica de documentacion
Desarrollo				
1.- Instalación de camaras de seguridad que grabe en video quienes ingresan y salen de las oficinas del archivo central de la institución.				

Directriz
2.- Instalación de alarma con sensores de movimiento para la restricción de acceso a personal no autorizado en horas fuera de oficina.

Directriz				
5.1.1.viii. Instalar sistemas de monitoreo y vigilancia enmarcados a la normativa legal vigente.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- Instalación de camaras de seguridad que grabe en video quienes ingresan y salen de las oficinas del archivo central de la institución. 2.- Instalación de alarma con sensores de movimiento para la restricción de acceso a personal no autorizado en horas fuera de oficina.				

Directriz				
5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	MEDIO	Deterioro fisico por algun incidente natural	Como no esta protegido fisicamente los estantes del archvo central hay riesgo de que la documentacion fisica	perdida de la consistencia fisica de documentacion
Desarrollo				
1.- Instalar extintores para incendios en las oficinas de archivos. 2.- Instalar sistema de alarma con detectores de humo en las oficinas de archivos				

Directriz				
5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- Instalar extintores para incendios en las oficinas de archivos. 2.- Instalar sistema de alarma con detectores de humo en las oficinas de archivos				

Directriz				
5.1.1.xi. Los ingresos y salidas de visitas deberán ser registradas, autorizadas y controladas. Asimismo deberán portar la identificación de visitante en lugar visible.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- El ingreso y salidas a las oficinas de archivos debe ser registrado por las camaras de vigilancia. 2.- El personal de la institución debe portar necesariamente su credencial. 3.- El personal externo la institución debe registrarse en una planilla.				

Directriz

Directriz				
5.1.1.xii. Los servidores públicos deberán portar la identificación correspondiente en un lugar visible.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- El personal de la institución debe portar necesariamente su credencial.				

Directriz				
5.1.1.xiii. La seguridad fisica perimetral de la entidad o institución pública deberá inspeccionar y verificar el ingreso de elementos que comprometa la seguridad.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- El ingreso y salidas a las oficinas de archivos debe ser registrado por las camaras de vigilancia.				

Directriz				
5.1.1.xvii. Contar con señalética visible, para evacuaciones o contingencias de la institución.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	MEDIO	Deterioro fisico por algun incidente natural	Como no esta protegido fisicamente los estantes del archvo central hay riesgo de que la documentacion fisica	perdida de la consistencia fisica de documentacion
Desarrollo				
1.- La oficina de archivos debe contar con la señaletica correspondiente tanto de ingreso como de salida.				

Directriz				
5.1.1.xvii. Contar con señalética visible, para evacuaciones o contingencias de la institución.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivos documentales del FONABOSQUE	ALTO	Perdida de informacion por acceso no deseado	Como no se tiene mamparas que protegan de una accesibilidad a los archivos entonces queda vulnerable la seguridad	Perdida de informacion
Desarrollo				
1.- La oficina de archivos debe contar con la señaletica correspondiente tanto de ingreso como de salida.				

Controles Mínimos de Seguridad de la Información

Los controles de Seguridad de la información que seran implementados se encuentran referenciados en "Controles Implementados y por Implementar" y en el punto de "Desarrollo" de la politica de la Seguridad de la Información y sus respectivos archivos adjuntos

Indicadores y Métricas

El RSI establece los indicadores y métricas de cumplimiento al momento de elaborar y desarrollar un determinado control de seguridad, con la finalidad de evaluar la eficacia de dichos controles una vez que se implementen.

En general, un indicador y métrica deberá ser:

a) Específico.

b) Medible cualitativa o cuantitativamente y/o con indicadores y atributos.

c) Alcanzable.

d) Relevante.

e) Repetible en periodos de tiempo.

2019

#	Control de Seguridad	Indicador y métrica	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	5. Seguridad física y ambiental													
		Ingreso fisico a las oficinas o area de archivos estara restringido a traves de una chapa con llave que solamente tendran las copias el encargado de archivos y el Coordinador Administrativo Financiero.	Ini: 14 Fin: 28											
		Instalación de mamparas en las oficina del archivo central para asegurar fisicamente el area donde se encuentran los archivos fisicos.	Ini: 14 Fin: 28											
		Instalar una puerta de acceso a las oficinas del archivo central con chapa y dos llaves (una que lo tenga el encargado del archivo central y otra copia que lo tenga el Coordinador Administrativo Financiero).	Ini: 14 Fin: 28											
		Instalación de camaras de seguridad que grabe en video quienes ingresan y salen de las oficinas del archivo central de la institución.		Ini: 11 Fin: 25										
		Instalación de alarma con sensores de movimiento para la restricción de acceso a personal no autorizado en horas fuera de oficina.		Ini: 11 Fin: 25										
		Instalar extintores para incendios en las oficinas de archivos.		Ini: 11 Fin: 25										

#	Control de Seguridad	Indicador y métrica	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
		Instalar sistema de alarma con detectores de humo en las oficinas de archivos		Ini: 18	Fin: 4									
		La oficina de archivos debe contar con la señaletica correspondiente tanto de ingreso como de salida.			Ini: 4 Fin: 18									
2	2. Gestión de activos de información													
		Digitalizar o escanear toda la documentación contenida en los archivos fisicos.		Ini: 11 Fin: 25										
		Implementar una plataforma para la gestión documental		Ini: 4 Fin: 18										
		Configurar la plataforma para la clasificación de la documentacion digitalizada		Ini: 4 Fin: 25										
		Registro en la plataforma de toda la documentacion digitalizada y ordenada segun configuración			Ini: 11 Fin: 25									
		Una vez que se tenga el archivo central digitalizado y automatizado, se debera establecer el ingreso a la plataforma con acceso restringido a usuarios que van a alimentar al sistema, usuarios que van a administrar el sistema y usuarios que solamente van a tener acceso de solo lectura de la documentación.			Ini: 4 Fin: 25									
		El acceso a la información de la plataforma sera a tres niveles, un administrador que pueda confgurar el sistema, un nivel de alimentadores de información que vana subir documentos al sistema y un nivel de lectores que solamente podran leer y bajar informacion del sistema.			Ini: 11 Fin: 25									
		Elaborar procesos y procedimientos para el ingreso y gestión documental del area de archivos a ser realizado por el encargado de archivos en coordinacion con el area de Gestión Institucional y	Fin: 1											

#	Control de Seguridad	Indicador y métrica	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
		Desarrollo Organizacional												
		El personal de la institución debe portar necesariamente su credencial. El personal externo la institución debe registrarse en una planilla.			Ini: 11 Fin: 25									

2018

#	Control de Seguridad	Indicador y métrica	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	2. Gestión de activos de información													
		Organización de los archivos fisicos de acuerdo a la tematica o areas técnicas y administrativas del FONABOSQUE										Ini: 15 Fin: 31		
		Adquisicion de un escanner de alto trafico que sirva para la digitalización de los archivos fisicos, segun la organizacón realizada.											Ini: 12 Fin: 26	
		Ingreso fisico a las oficinas o area de archivos estara restringido a traves de una chapa con llave que solamente tendran las copias el encargado de archivos y el Coordinador Administrativo Financiero.												Ini: 10 Fin: 24
		Elaborar procesos y procedimientos para el ingreso y gestión documental del area de archivos a ser realizado por el encargado de archivos en coordinacion con el area de Gestión Institucional y Desarrollo Organizacional												Ini: 10

Cronograma de Implementación

En el marco del Plan Institucional de Seguridad de la Información, la entidad o institución pública elabora un cronograma de implementación de los controles definidos. Para esto, todos los procesos y/o procedimientos que se desprenden de la Política de Seguridad de la Información ya se encuentran elaborados para su aplicación. El cronograma de implementación contempla mínimamente:

a) Fechas.

b) Controles a implementarse.

c) Roles y responsabilidades.

d) Actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles.

2018

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	5. Seguridad física y ambiental														
		Ingreso fisico a las oficinas o area de archivos estara restringido a traves de una chapa con llave que solamente tendran las copias el encargado de archivos y el Coordinador Administrativo Financiero.	Area administrativa y encargado de archivos									Ini: 8		Fin: 31	
		Instalación de mamparas en las oficina del archivo central para asegurar fisicamente el area donde se encuentran los archivos fisicos.	Area administrativa y encargado de archivos									Ini: 8		Fin: 17	
		Instalar una puerta de acceso a las oficinas del archivo central con chapa y dos llaves (una que lo tenga el encargado del archivo central y otra copia que lo tenga el Coordinador Administrativo Financiero).	Area administrativa y encargado de archivos									Ini: 8		Fin: 17	
		Instalación de camaras de seguridad que grabe en video quienes ingresan y salen de las oficinas del archivo central de la institución.	Area administrativa y encargado de archivos										Ini: 12	Fin: 24	
		Instalación de alarma con sensores de movimiento para la restricción de acceso a personal no autorizado en horas fuera de oficina.	Area administrativa y encargado de archivos										Ini: 12	Fin: 24	
		Instalar extintores para	Area administrativa											Ini: 3	

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
		incendios en las oficinas de archivos.	y encargado de archivos												
		Instalar sistema de alarma con detectores de humo en las oficinas de archivos	Area administrativa y encargado de archivos											Ini: 10	
2	2. Gestión de activos de información														
		Organización de los archivos fisicos de acuerdo a la tematica o areas técnicas y administrativas del FONABOSQUE	Responsable de archivos								Ini: 17	Fin: 29			
		Adquisicion de un escanner de alto trafico que sirva para la digitalización de los archivos fisicos, segun la organizacón realizada.	Area de Tecnologias de Informacion									Ini: 1 Fin: 31			
		Digitalizar o escanear toda la documentación contenida en los archivos fisicos.	Responsable de archivos										Ini: 5		
		Implementar una plataforma para la gestión documental	Area de Tecnologias de Informacion											Ini: 3	
		Configurar la plataforma para la clasificación de la documentacion digitalizada	Area de Tecnologias de Informacion											Ini: 17	
		Ingreso fisico a las oficinas o area de archivos estara restringido a traves de una chapa con llave que solamente tendran las copias el encargado de archivos y el Coordinador Administrativo Financiero.	Area administrativa y encargado de archivos											Ini: 3 Fin: 24	
		Elaborar procesos y	Responsable de archivos										Ini: 5 Fin: 26		

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
		procedimientos para el ingreso y gestión documental del area de archivos a ser realizado por el encargado de archivos en coordinacion con el area de Gestión Institucional y Desarrollo Organizacional													

2019

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	5. Seguridad física y ambiental														
		Instalar extintores para incendios en las oficinas de archivos.	Area administrativa y encargado de archivos												
		Instalar sistema de alarma con detectores de humo en las oficinas de archivos	Area administrativa y encargado de archivos												
		La oficina de archivos debe contar con la señaletica correspondiente tanto de ingreso como de salida.	Area administrativa y encargado de archivos												
2	2. Gestión de activos de información														
		Digitalizar o escanear toda la documentación contenida en los archivos fisicos.	Responsable de archivos												
		Implementar una plataforma para la gestión documental	Area de Tecnologias de Informacion												
		Configurar la plataforma para la clasificación de la documentacion digitalizada	Area de Tecnologias de Informacion												
		Registro en la plataforma de toda la documentacion digitalizada y ordenada segun	Responsable de archivos	Fin: 18											

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
		configuración													
		Una vez que se tenga el archivo central digitalizado y automatizado, se debera establecer el ingreso a la plataforma con acceso restringido a usuarios que van a alimentar al sistema, usuarios que van a administrar el sistema y usuarios que solamente van a tener acceso de solo lectura de la documentación.	Responsable de archivos		Ini: 4 Fin: 25										
		El acceso a la información de la plataforma sera a tres niveles, un administrador que pueda confgurar el sistema, un nivel de alimentadores de información que vana subir documentos al sistema y un nivel de lectores que solamente podran leer y bajar informacion del sistema.	Responsable de archivos	Ini: 4 Fin: 25											
		El personal de la institución debe portar necesariamente su credencial. El personal externo la institución debe registrarse en una planilla.	Responsable de archivos												

Historial de Cambios

Fecha	Formulario	Estado	Encargado
2018-09-19	Etapa Inicial	EN_REVISION	Justo Nicanor Colquehuanca Ticona
2018-09-19	Etapa Inicial	APROBADO	Patricia Santader
2018-09-17	Gestión de Riesgos	EN_REVISION	Justo Nicanor Colquehuanca Ticona
2018-09-17	Gestión de Riesgos	APROBADO	Patricia Santader
2018-09-19	Políticas de Seguridad	EN_REVISION	Justo Nicanor Colquehuanca Ticona
2018-09-19	Políticas de Seguridad	APROBADO	Patricia Santader
2018-09-19	Indicadores y Metricas	EN_REVISION	Justo Nicanor Colquehuanca Ticona
2018-09-19	Indicadores y Metricas	APROBADO	Patricia Santader
2018-09-19	Controles implementados y por implementar	EN_REVISION	Justo Nicanor Colquehuanca Ticona
2018-09-19	Controles implementados y por implementar	APROBADO	Patricia Santader
2018-09-17	Tratamiento de Riesgo	EN_REVISION	Justo Nicanor Colquehuanca Ticona
2018-09-17	Tratamiento de Riesgo	APROBADO	Patricia Santader

ANEXO

Documentación de la Entidad

En esta etapa, el Responsable de Seguridad de la Información identifico las siguientes fuentes principales de insumo para elaborar el PISI, que son listadas a continuación:

Plan Estrategico Institucional
Plan Operativo Anual
Manual Operativo de Funciones

Responsabilidades de la Máxima Autoridad Ejecutiva

La Máxima Autoridad Ejecutiva deberá:

a) Estar informada sobre el estado de seguridad de la información de la entidad o institución pública bajo su tutela.

b) Tomar conocimiento de la normativa vigente respecto a seguridad de la información (Decreto Supremo N° 2514 de 9 de septiembre de 2015 y Decreto Supremo N° 1793, de 13 de noviembre de 2013, de reglamentación a la Ley 164).

c) Designar al Responsable de Seguridad de la Información (RSI).

d) Conformar el Comité de Seguridad de la Información (CSI).

e) Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Institucional.

f) En lo posible, destinar los recursos administrativos, económicos y humanos para la elaboración e implementación del Plan Institucional de Seguridad de la Información.

g) Aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución.

h) Cumplir y hacer cumplir el Plan Institucional de Seguridad de la Información de su entidad o institución.

i) Asumir otras acciones a favor de la seguridad de la información.

Lo cual se puede evidenciar en el documento adjunto:

doc1.pdf,

Documento de Designación y Funciones del Responsable de Seguridad de la Información

El RSI tendrá las siguientes funciones:

a) Gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información (PISI).

b) Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de información.

c) Proponer la Política de Seguridad de la Información (PSI), que estará incorporada dentro del PISI.

d) Gestionar el cumplimiento del PISI.

e) Elaborar manuales de procesos y/o procedimientos de seguridad específicos que se desprendan de los lineamientos del Plan Institucional de Seguridad de la Información y promover su difusión en la entidad o institución pública.

f) Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la entidad o institución.

g) Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI.

h) Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en su entidad o institución.

i) Coadyuvar en la gestión de contingencias tecnológicas.

j) Proponer estrategias y acciones en mejora de la seguridad de la información.

k) Promover la realización de auditorías al Plan Institucional de Seguridad de la Información.

l) Gestionar la mejora continua de la seguridad de la información.

m) Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normales de la Institución.

n) Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar datos que puedan ser relevantes.

o) Monitorear la implementación y uso de mecanismos de seguridad, que coadyuven a la reducción de los riesgos identificados.

p) Otras funciones que resulten necesarias para preservar la seguridad de la información.

Lo cual se puede evidenciar en el documento adjunto, donde ademas se cuenta con la designación del RSI en una nota firmada por MAE:

doc2.pdf,

Documento de Conformación y Funciones del Comité de Seguridad de la Información

Mediante resolución expresa, la Máxima Autoridad Ejecutiva designa al personal que conformará el Comité de Seguridad de la Información (CSI).

El CSI esta conformado por:

a) La Máxima Autoridad Ejecutiva en calidad de presidente del CSI, con la posibilidad de delegar sus funciones.

b) Personal de nivel jerárquico, de acuerdo a la estructura organizativa de la entidad o institución pública. (detalle de quienes forman parte del Comité)

c) El Responsable de Seguridad de la Información (RSI).

El CSI establece su organización interna y asume como mínimo las siguientes funciones:

a) Revisar el Plan Institucional de Seguridad de la Información (PISI).

b) Promover la aprobación del PISI a través de la MAE.

c) Revisar los manuales de procesos y/o procedimientos de seguridad que se desprendan de la Política de Seguridad de la Información incorporada en el PISI.

d) Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.

e) Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.

f) Promover la concientización y capacitación en seguridad de la información al interior de la entidad o institución pública.

g) Proponer y promover las acciones necesarias en función a la gravedad de los incidentes de seguridad de la información, con el fin de prevenir incidentes futuros.

h) Otras funciones que resulten necesarias para la seguridad de la información.

Lo cual se puede evidenciar con la Resolución Administrativa y los documentos que se encuentran adjuntos a continuación

doc3.pdf,

Definición del Alcance del PISI

En Reunión del Comite de Seguridad de la Información define el alcance del PISI como:

Este documento establece un plan institucional de seguridad de la información que define lineamientos para la aplicación de las políticas de seguridad definidas en el documento Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público del CTIC-EPB.
Para la implementación de planes de seguridad de información en la institución será de forma gradual iniciando paulatinamente desde la presente gestión.
La planeación en esta etapa incluye controles preventivos y correctivos para incidencias de seguridad de la información en el area de archivos por considerarse un area en riesgo de perder la memoria institucional, posteriormente en la siguiente gestión se abordara otras areas criticas de la institución.