CÓDIGO: MOI-GSI-GSE001

VERSIÓN: 01

FECHA DE APROBACIÓN: 13 de septiembre de 2017

FONCEP

Fondo de Prestaciones Económicas, Cesantías y Pensiones.

BOGOTÁ MEJOR PARA TODOS

	MANUAL	**MANUAL DE MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Gestión de servicios internos Gestión de servicio de información	**MACROPROCESO** **PROCESO**	

	OBJETIVO	Establecer la política general de seguridad de la Información, alcance, condiciones generales y políticas adicionales, las cuales son de obligatorio cumplimiento para las personas que laboran en el FONCEP independiente de su tipo de vinculación, alineada con la estrategia de Gobierno en Línea (GEL), adoptadas para salvaguardar la Información como activo fundamental de la Entidad.

Inicia con la definición del alcance de la política, pasando por los principios, responsabilidades e implementación y finaliza con la definición de otras políticas asociadas al marco de Modelos de Seguridad y Privacidad de la Información (MSPI).	**ALCANCE**	

	NORMATIVIDAD	• Decreto 2573 de 12 diciembre de 2012 • Resolución 305 del 20 de octubre de 2008 • NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001 • GUÍA TÉCNICA GTC-ISO/IEC COLOMBIANA 27002

Activo, Administración Remota, Amenaza, Archivo Log, Ataque, Confidencialidad, Cuenta, Desastre, Contingencia, Disponibilidad, Cifrado, Información, Integridad, Impacto, Normativa de Seguridad ISO/IEC 17799, Responsabilidad, Servicio, Soporte Técnico, Riesgo, Usuario, Usuario de información, Vulnerabilidad, Medios removibles.	**DEFINICIONES**	

Introducción

La información es el activo más importante de una organización y adopta diferentes formas como: impresa, escrita, papel, digital, correo electrónico, páginas web, archivos magnéticos, sistemas de información, videos, o conversaciones como medio fundamental de la comunicación del ser humano.

Por su naturaleza, importancia y disponibilidad de la información, cada día está más expuesta a amenazas y vulnerabilidades, por lo tanto, la seguridad de la información es la protección de la información contra una amplia gama de amenazas; para minimizar los daños y garantizar la continuidad del negocio.

El propósito de un Sistema de Gestión de la Seguridad de la Información (SGSI), no es garantizar que no se presenten vulnerabilidades, sino garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización en forma sistemática, estructurada, continua, repetible, eficiente, adaptada a los cambios que se produzcan en la organización y con los soportes documentales apropiados. El SGSI protege los activos de información de una organización, independientemente del medio en que se encuentre.

La seguridad de la información se establece mediante la implementación de un conjunto adecuado de políticas, procesos, procedimientos de la organización, controles, hardware y software; pero lo más importante, mediante comportamientos éticos de las personas.

La seguridad de la información es la preservación de los principios básicos de la confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento. Estos tres pilares se definen como:

- Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.
- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

La dirección como máxima autoridad dentro de la organización, debe establecer de forma clara las líneas de actuación y manifestar su apoyo y compromiso incondicional a la seguridad de la información, con el fin de garantizar su implementación en toda la organización y sus procesos.

El tal sentido, la Entidad en cumplimiento de las revisiones permanentes que se debe realizar a la política y al compromiso que tiene para el proceso de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), ha expedido la RESOLUCIÓN No. DG—0231 - 11 JUL 2016.

Contenido

Desarrollo del Manual

1. **Alcance de la política de seguridad de la información**

   Teniendo como marco la norma técnica NTC-ISO/IEC 27001 en su versión 2013, las políticas de seguridad de la información del FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP, están dirigidas a:

   - Todas las personas vinculadas al FONCEP como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista y pasante; así como al personal vinculado con firmas que prestan servicios al FONCEP.
   - Todos los recursos y activos de información de la Entidad.
   - Todos los procesos y procedimientos de la Entidad.
   - Toda la infraestructura tecnológica y los Sistemas de Información que soportan la funcionalidad de la Entidad y
   - Todas las sedes físicas de la Entidad

2. **Política general de Seguridad de la Información**

   El FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP, como entidad responsable del pago de cesantías y reconocimiento y pago de pensiones a las servidoras y servidores públicos del Distrito Capital, con régimen de retroactividad, afiliados al FONCEP; es consiente que la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad al interior de la Entidad.

   Por lo tanto, todas las personas naturales y jurídicas que laboran en el FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES – FONCEP, serán responsables por el cumplimiento de las políticas, controles, normas, procedimientos y estándares vigentes respecto a la seguridad de la información, permitiendo a la Entidad, identificar y minimizar los riesgos a los cuales se expone su información y establecer una cultura de seguridad que garantice el cumplimiento de los requerimientos legales, contractuales y técnicos mediante la adopción de las mejores prácticas.

   La Política general de seguridad de la información de FONCEP se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiaran la gestión adecuada de la información.

3. Objetivos específicos de seguridad de la información

Para cada uno de los 114 controles contenidos en los 14 objetivos de control definidos en el Anexo A de la norma ISO-IEC-27001-2013, se deben establecer la declaración de aplicabilidad que permitan a la Entidad proteger su información; los cuales deben ser implementados de acuerdo con las metas y objetivos relacionados en el Plan Estratégico 2016-2019.

Consciente de sus necesidades actuales el FONCEP implementar un Modelo de Seguridad y Privacidad de la Información (MSPI), como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información de la Entidad.

4. Implementación del MSPI

Para la implementación del MSPI, se ha incluido en el plan estratégico el proyecto denominado "Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI)", y su control se realizará mediante la metodología establecida por la Entidad.

5. Otras políticas asociadas

Adicionalmente se definen las siguientes políticas, que determinan el comportamiento y los lineamientos que se deben cumplir en materia de seguridad de la información.

5.1 Organización de la seguridad de la información

5.1.1 Objetivo

Garantizar un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la entidad y establecer los lineamientos de seguridad de la información en el uso de opciones de teletrabajo y el uso de dispositivos móviles.

5.1.2 Política

Se debe establecer la organización interna y los roles para el manejo de la seguridad de la información, estableciendo contactos con las autoridades y grupos de interés en la materia, a fin de poder contar con las directrices y apoyo requerido en el proceso de implementación del Modelo de Seguridad y Privacidad de la Información.

Se debe implementar esquemas de seguridad de la información, en el manejo de los proyectos de la Entidad y definir políticas y gestión de seguridad para el manejo de dispositivos móviles que se conecten a la red interna de la Entidad y para los esquemas de teletrabajo que se implementen.

5.2 Seguridad de los Recursos Humanos.

5.2.1 Objetivo

Establecer las responsabilidades del personal en materia de Seguridad de la Información, las necesidades de capacitación y los procedimientos de manejo de incidentes, con el objeto de reducir el riesgo de error humano, fraude o mal uso de los bienes de información.

5.2.2 Política

Desde la vinculación del personal al FONCEP, se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Los términos y condiciones de empleo o trabajo deben establecer la responsabilidad de los funcionarios, temporales, supernumerario y contratistas, por la seguridad de los activos de información, que van más allá de la finalización de la relación laboral o contractual, por lo que se debe firmar un acuerdo de confidencialidad por todas las personas vinculadas a la Entidad, independiente de su forma de vinculación.

El personal vinculado al FONCEP, deben cooperar con los esfuerzos por proteger la información y ser responsables de actualizarse en cada materia, así como consultar, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deba llevarse a cabo cuando se incurra en violaciones a las políticas, controles o normas de seguridad.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

5.2.3 Funciones y responsabilidades

Todas las personas vinculadas al FONCEP como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista y pasante; deben tener claramente definidas sus funciones y su rol y responsabilidades en cuanto a la Seguridad de la Información dentro de la Entidad. Adicionalmente, se deben establecer las responsabilidades y derechos legales del empleado o contratista en cuanto a aspectos de propiedad intelectual, protección de la información y leyes aplicables.

5.2.4 Selección

Todas las personas vinculadas al FONCEP como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista y pasante; deben ser adecuadamente seleccionados, de acuerdo con el Manual del Funciones del cargo y deben aceptar las políticas de Seguridad de la Información establecidas y

definidas, las cuales deben ser conocidas por el empleado o contratista en el momento de su vinculación. Cuando la vinculación se realice por intermedio de terceros, se debe especificar la responsabilidad de ellos en el proceso de selección y la forma en que se debe manejar cualquier incumplimiento de los requisitos establecidos.

5.2.5 Términos y condiciones laborales

Existirá una Cláusula de confidencialidad y buen manejo de la información, para todos los usuarios del Sistema de Información o funcionarios del FONCEP, la cual se hará conocer al momento de hacer entrega del usuario creado para cada uno, y se incluirá de manera expresa esta cláusula en los contratos de servicio firmados con otras empresas o con contratistas directos del FONCEP o con terceros. Este requerimiento también se debe aplicar al caso de contratación de personal temporal o cuando se permita el acceso a los recursos informáticos del FONCEP a usuarios externos y se definirá y asignará claramente las responsabilidades para llevar a cabo la terminación o el cambio a nivel laboral.

5.2.6 Responsabilidades de la Dirección

La dirección exigirá que los empleados, contratistas y usuarios externos apliquen la seguridad según las políticas y los procedimientos establecidos por el FONCEP.

5.2.7 Educación, formación y concientización sobre la seguridad de la información.

Los funcionarios del FONCEP serán entrenados y capacitados para las funciones y cargos a desempeñar con el fin de proteger adecuadamente los recursos y la información de la entidad. En los casos en que así se establezca, este entrenamiento debe cubrir a personal contratista, o terceros, cuando sus responsabilidades lo exijan. Existirá un programa continuo de concientización en seguridad de la Información, de forma que les permita recibir la capacitación adecuada y periódica, de forma tal que se encuentre en condiciones de comprender el alcance y contenido de las políticas de Seguridad Informática detalladas en este documento y la necesidad de respaldarlas y aplicarlas de manera permanente.

5.2.8 Proceso disciplinario

Todos los incidentes de seguridad ocurridos en el FONCEP deben ser investigados con el fin de determinar sus causas y responsables. Los procesos derivados de los reportes y análisis de los Incidentes de Seguridad deben ser manejados por el área encargada en el FONCEP, de acuerdo con el resultado de la incidencia.

5.2.9 Devolución de activos

En el retiro de cualquier funcionario de la Entidad, independiente de su modalidad de vinculación, se debe contar con un procedimiento para garantizar que todos los activos de información manejados y asignados al funcionario se transfieran al FONCEP y se elimine con seguridad la información del equipo del usuario.

Se documentará y transferirá a la entidad el conocimiento que sea importante para la continuidad de las operaciones que tenga un empleado, contratista o usuario de terceras partes.

5.2.10 Retiro de los derechos de acceso

Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se retirarán al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después de un cambio o traslado del funcionario.

5.3 Gestión de Activos de Información.

Ver detalle de las políticas en el documento **POL-GSI-GSE001 POLÍTICA DE USO APROPIADO DE LOS ACTIVOS DE INFORMACIÓN.**

5.3.1 Objetivo

Mantener un inventario de activos o bienes de información, así como los propietarios y responsables de su gestión para establecer un nivel de protección adecuado para los mismos.

5.3.2 Política

Toda la información sensible del FONCEP, así como los Activos de Información donde ésta se almacena o procesa, son inventariados, asignándoles un responsable y clasificarlos de acuerdo con los requerimientos de seguridad de la información y los criterios que dicte el Comité de Seguridad de la Información del FONCEP. A partir de esta clasificación se establecerán los niveles de protección orientados a determinar a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación. La clasificación debe revisarse periódicamente y atender a los cambios que se presenten en la información o la estructura que puedan afectarla.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

5.3.3 Inventario de activos

El FONCEP mantendrá un inventario de los activos o bienes de Información,

estableciendo Claramente el propietario del activo y el valor cualitativo para cada una de sus características de Confidencialidad, Integridad y Disponibilidad de forma tal que permita a la organización identificar sus activos y el valor e importancia de cada uno de ellos.

5.3.4 Propiedad de los activos

Cada activo informático estará claramente identificado y además debe tener un propietario asociado, quien es el responsable de su utilización y administración.

5.3.5 Uso aceptable de los activos

Se identifica, documenta e implementan las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

5.3.6 Clasificación de la información

La información en el FONCEP está clasificada de forma tal que permita a los usuarios dar buen uso de la misma, por lo tanto, todos los usuarios deben respetar la protección de dicha información.

Se debe contar con una política de clasificación de la información, que permita identificarla, catalogarla y documentarla de acuerdo con la criticidad de la misma dentro de la organización, a las normas vigentes y la ley de transparencia.

Los propietarios de la información son responsables por la clasificación de la misma. Cada uno de ellos, es responsable de asegurar el apropiado nivel de seguridad y protección de la información. La clasificación se revisa de manera periódica por el propietario, y la definición debe ser aprobada por el Responsable de Área y/o Líder Funcional y los usuarios que tengan permisos para accederla deben utilizarla estrictamente para el propósito de la organización.

Está expresamente prohibido utilizar información perteneciente al FONCEP para uso y beneficio personal.

5.3.7 Etiquetado y manejo de la información

Toda información en formato electrónico e impreso perteneciente al FONCEP estará debidamente identificada mediante un rótulo o etiqueta (label), el cual permita establecer por parte del usuario la categoría de Clasificación del bien dentro del FONCEP. Esta identificación corresponde a lo expresado en el punto anterior.

5.4 Control de acceso

Ver detalle de las políticas en el documento **POL-GSI-GSE002 POLÍTICA DE CONTROL DE ACCESO A SERVICIOS DE TI.**

5.4.1 Objetivo.

Definir las pautas generales para asegurar un acceso controlado a la información y a las aplicaciones de la Entidad

5.4.2 Política

El acceso a la información y a los recursos informáticos de la Entidad debe ser solicitado y aprobado por el jefe del área de la dependencia y asignados por la Oficina de Informática y Sistemas, quien entregará las claves respectivas para el adecuado uso de la información y los recursos.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

Los jefes de las áreas de la Entidad son los responsables de definir los roles que se le deben asignar a cada uno de los usuarios de su dependencia, realizar el seguimiento adecuado, solicitar las modificaciones cuando sea necesario y el retiro cuando el usuario deje de pertenecer a la Entidad.

Los funcionarios deben dar uso adecuado de los recursos asignados (equipos de cómputo, impresoras, puesto de trabajo, software, entre otros) y/o servicios informáticos (cuentas de usuario, carpetas compartidas, correo electrónico institucional, intranet, internet, datos e información, sistemas de información, entre otros) de acuerdo con las normas y procedimientos establecidos por la Entidad.

Los funcionarios deben proteger y no transferir el usuario y la palabra clave asignado por la Entidad a otra persona o funcionario, ni utilizar otra cuenta de usuario para el ingreso a los recursos de la Entidad y responder por todas las operaciones efectuadas y la información registrada con esta cuenta de usuario.

No se permite conectar a la red o instalar dispositivos (móviles o fijos tales como portátiles, celulares, tabletas, teléfonos inteligentes, enrutadores, agendas electrónicas, puntos de acceso inalámbrico) que no sean autorizados por la Oficina de Informática y Sistemas.

La conexión remota a la red de área local de la Entidad debe ser hecha a través de una conexión segura y será solicitada por el jefe del área que la

requiera y validada y asignada por la Oficina de Informática y Sistemas. Las condiciones de infraestructura y de seguridad, las proporcionará la Oficina de Informática y Sistemas. En lo posible se debe contar con auditorías de las actuaciones realizadas con estas conexiones.

Se deben establecer los procedimientos requeridos para la implementación de esta política.

5.5 Criptografía

Ver detalle de las políticas en los documentos **POL-GSI-GSE005 POLÍTICA DE SEGURIDAD DE INTERCAMBIO DE INFORMACIÓN y POL-GSI-GSE007 POLÍTICA DE CRIPTOGRAFÍA.**

5.5.1 Objetivo

Definir la utilización de medios criptográficos adecuados para proteger la confidencialidad, autenticidad o integridad de la información en los eventos que lo establezca la entidad.

5.5.2 Política

Para la información que se considere susceptible de proteger criptográficamente, ya sea de los sistemas de información o que se requiera intercambiar con otras entidades; se debe garantizar la utilización de esquemas seguros de cifrado para su conservación o intercambio.

En caso de requerirse Se deben definir procedimientos y protocolos de cifrado y descripción de la información, en forma segura.

5.6 Seguridad Física.

Ver detalle de las políticas en el documento **POL-GSI-GSE003 POLÍTICA DE SEGURIDAD FÍSICA.**

5.6.1 Objetivo.

Prevenir el acceso no autorizado, el daño y la interferencia de la información y de las instalaciones en donde se encuentren sistemas de procesamiento de información del FONCEP.

5.6.2 Política.

Se deben establecerse áreas seguras para la gestión, almacenamiento y procesamiento de información en el FONCEP; que en lo posible deben contar con protecciones físicas y ambientales acordes a los activos que protegen, incluyendo perímetros de seguridad, controles de acceso físicos,

controles especiales en áreas de mayor sensibilidad, seguridad de los

equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios adecuados que preserven el medio ambiente.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

5.6.3 Perímetro de seguridad física

El FONCEP debe definir claramente las áreas seguras con el fin de proteger instalaciones de procesamiento de información. Para el efecto, deben ser protegidas con controles de ingreso físico, que permitan el acceso solamente al personal autorizado, y permitan la implementación de mecanismos de registro de todo ingreso y egreso de funcionarios y visitantes que deban acceder a diferentes áreas seguras establecidas en la entidad.

5.6.4 Controles de acceso físico

El control de acceso para los funcionarios en las áreas seguras se debe hacer mediante el uso de tarjetas magnéticas de aproximación, preferiblemente utilizando mecanismos de doble autenticación, acompañadas de mecanismos que permitan implementar registros de auditoría de los accesos.

Todo el personal del FONCEP debe usar de forma permanente y en un lugar visible su identificación como funcionario o contratista.

Los visitantes deben portar en todo momento la identificación suministrada en el control de ingreso al edificio. Queda prohibida la permanencia de visitantes sin supervisión en las áreas seguras. En cualquier caso, las visitas deben ser autorizadas directamente por un responsable.

Las áreas Seguras deben ser definidas en un documento de carácter confidencial de uso restringido al interior del Grupo de Seguridad, con base en los resultados del Análisis de Riesgos y Valoración e Identificación de Activos.

Los medios de respaldo deben ser almacenados en zonas aisladas, separadas de las áreas de procesamiento, con control de acceso físico restringido y protegidas contra amenazas físicas similares a los centros de procesamiento de información.

El grupo de apoyo de la Seguridad de la Información debe realizar revisiones periódicas de los niveles de acceso y privilegios establecidos, y debe actualizar los niveles definidos, de forma periódica.

Queda prohibido el almacenamiento de material o sustancias inflamables en las áreas seguras, en las áreas definidas para Centros de Cómputo, y en áreas consideradas de alto riesgo.

No se permite el ingreso de funcionarios, contratistas o visitantes, sin las autorizaciones correspondientes o que no sigan el procedimiento adecuado. Se deben establecer los procedimientos de ingreso al edificio por el área encargada de la protección de las instalaciones, y debe ser tomado como procedimiento de apoyo a esta política.

Los funcionarios del FONCEP no deben permitir que personas desconocidas o no autorizadas atraviesen las puertas u otras entradas con control físico de acceso, al mismo tiempo en que lo hacen ellos, y que se pueda evitar de esa forma su control.

Los equipos como fotocopiadoras y faxes deben estar ubicados en zonas con control de acceso restringido, y se debe controlar su uso por parte de personal autorizado solamente, para lo cual debe existir un registro de su utilización. Se debe tener especial cuidado en su uso (incluyendo las impresoras), para garantizar que no permanezca en ellas, sin atención, material con información sensible, y que no se use papel reciclado que contenga información crítica o confidencial.

5.6.5 Protección contra amenazas externas y ambientes

Deben existir protecciones físicas contra daño por incendio inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

Los materiales combustibles o peligrosos se deben almacenar a una distancia prudente de las áreas de seguridad. Los suministros a granel tales como los materiales de oficina, no se deben almacenar en un área segura.

Se deben suministrar equipos apropiados contra incendios y deben ser ubicados adecuadamente.

5.6.6 Trabajo en áreas seguras

Las actividades de limpieza en las áreas seguras deben ser controladas estrictamente por el responsable de la infraestructura.

5.6.7 Áreas de carga, despacho y acceso público

Los puntos de acceso tales como las áreas seguras de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones de deben controlar, si es posible, aislar de los servicios de

procesamiento de información para evitar el acceso no autorizado.

5.6.8 Escritorios y pantalla limpia

El personal del FONCEP, debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

El personal de la Entidad debe bloquear la pantalla de su computador con el protector de pantalla designado por la entidad, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Al imprimir documentos de carácter público o reservado, estos deben ser retirados de la impresora inmediatamente.

5.6.9 Ubicación y protección de los equipos

La infraestructura de procesamiento de datos (equipos de hardware y software, y elementos de red y comunicaciones que se utilicen para el tratamiento de información) debe estar protegida de manera física o con controles lógicos, contra amenazas de carácter ambiental, y de los peligros generados por accesos no autorizados. Los dispositivos y mecanismos de protección deben estar alienados con base en el análisis de *riesgos.*
La red de datos debe ser protegida de accesos y conexiones físicas no autorizadas, así como de daños o interferencias que puedan afectar la integridad y disponibilidad de la información, mediante mecanismos *físicos o lógicos.*

5.6.10 Servicios de suministro

Toda la red eléctrica debe ser regulada. Para el centro de Cómputo y para algunas áreas de procesamiento debidamente identificadas, se debe instalar equipos de Suministro de Energía de Forma Ininterrumpible (UPS).

5.6.11 Seguridad del cableado

El acceso a los módulos de cableado y a los cuartos de cableado debe ser controlado y solo podrá acceder personal autorizado.

5.6.12 Mantenimiento de los equipos

Todos los equipos de procesamiento de información, de transmisión de datos y de soporte de la infraestructura, elementos de red; deben contar con los contratos de mantenimiento apropiados de acuerdo con su nivel de criticidad y a los requerimientos de disponibilidad identificados, y con una Hoja de Vida donde esté establecida la frecuencia de revisión y

mantenimiento.

5.6.13 Seguridad de los equipos fuera de las instalaciones

Los equipos portátiles deben estar protegidos por mecanismos antirrobo o con elementos como guayas de seguridad, en adición a los controles lógicos establecidos.

Cuando un equipo de cómputo deba repararse, éste no saldrá del edificio sin tener una autorización firmada por parte del director del área a la cual pertenece o está asignado el equipo, y por el Director de Recursos Físicos, donde se detalle su número de serie, marca y modelo. Se debe llevar un registro estricto con los datos de la empresa y la persona que se lleva dicho equipo. Para cualquier traslado de equipos o dispositivos que contengan información y archivos, los mismos deben ser borrados para evitar la fuga de información.

5.6.14 Seguridad en la reutilización o eliminación de los equipos

Toda la información que se encuentre en equipos de usuarios y que van a ser reutilizados debe ser borrada y se debe realizar un formateo completo de los discos y la reinstalación del Sistema y de las aplicaciones.

La información que se encuentre en otros medios y que sea desechada, debe ser destruida de acuerdo con los niveles identificados en el proceso de análisis de riesgos, o en procesos de revisión realizados por parte del Grupo de Seguridad.

5.6.15 Retiro de propiedad

El comité de seguridad o el responsable de Seguridad Informática debe precisar el tipo de información que se puede mantener en equipos portátiles o dispositivos removibles, aún si estos no son propiedad del FONCEP (caso computadores personales).

No se debe retirar información, en ningún formato, de las instalaciones del FONCEP, sin la debida autorización previa por parte del Director de Área.

5.7 Seguridad de las Operaciones.

5.7.1 Objetivo.

Garantizar la existencia de procedimientos, registros y guías de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura informática del FONCEP.

5.7.2 Política.

Deben documentarse los procedimientos y responsabilidades de

administración y seguridad que sean necesarios en cada ambiente tecnológico y físico, garantizando un adecuado control de cambios y el seguimiento a estándares de seguridad que deben definirse, así como el seguimiento a los incidentes de seguridad que puedan presentarse. Debe buscarse una adecuada segregación de funciones.

Deben garantizarse una adecuada planificación y aprobación de los sistemas de información que consideren o provean las necesidades de capacidad futura.

Deben considerarse protecciones contra software malicioso y un adecuado mantenimiento y administración de la infraestructura, así como un adecuado cuidado de los medios de almacenamiento y seguridad en el intercambio de información.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios

5.7.3 Procedimientos de operación documentados

Deben existir procedimientos, registros y guías de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura informática y de Sistemas en el FONCEP. A cada procedimiento debe tener responsable para su definición y mantenimiento.

5.7.4 Gestión del cambio

Todo cambio a la infraestructura informática debe estar controlado y ser realizado de acuerdo con los procedimientos definidos por el FONCEP, con el fin de asegurar que los cambios efectuados no afecten la disponibilidad e integridad de la información y los servicios.

5.7.5 Separación de las instalaciones de desarrollo, ensayo y operación

Para la gestión de las operaciones de los sistemas de información en el FONCEP, deben existir mecanismos que permitan contar con ambientes de desarrollo, pruebas y operación, para todos los aplicativos con los que se cuente los archivos fuente y pruebas y operación, para los que no se cuente con los archivos fuente.

5.7.6 Controles contra códigos maliciosos

La Infraestructura de red debe estar protegida para asegurar que no se ejecuten virus o códigos maliciosos, mediante la utilización de un sistema de “Antivirus” para todos los equipos que formen parte de la infraestructura del FONCEP.

El sistema de control de virus debe contar con los procesos y contratos de soporte necesarios para mantenerlo actualizado y es responsabilidad del usuario y del Administrador de Red asegurar que el software Antivirus no sea deshabilitado por ningún motivo

5.7.7 Respaldo de la información

Deben existir procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y períodos de retención de la misma. Estos procedimientos deben establecer el uso de sistemas de inventario e identificación de los medios magnéticos, la identificación de la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a la información resguardada.

El procedimiento de gestión de copias de respaldo debe incluir los aspectos relacionados con las pruebas periódicas de verificación de las copias de respaldo.

Toda información resguardada en medios magnéticos debe almacenarse en lugares que cumplan con máximas medidas de protección, en cajas o gabinetes de seguridad y el sitio debe contar con mecanismos de detección de humo, calor y humedad, incendio y control de acceso físico.

5.7.8 Registros del administrador y del operador

Todas las actividades de operación realizadas por los administradores de sistemas de la infraestructura deben estar debidamente registradas y se deben revisar periódicamente por el personal encargado para este propósito dentro del Grupo de Seguridad de la Información.

5.7.9 Instalaciones de software en sistemas operativos y Restricción sobre la instalación de software

Solo personal designado por el Oficina de Informática y Sistemas está autorizada para instalar software o hardware en los Pc, portátiles, servidores e infraestructura de telecomunicaciones la Entidad.

5.8 Seguridad de las comunicaciones

5.8.1 Objetivo.

Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

5.8.2 Política.

Deben documentarse los procedimientos y responsabilidades de administración y seguridad que sean necesarios en el manejo de las redes

de la Entidad, garantizando un adecuado control, mantenimiento, así como el seguimiento a los incidentes de seguridad que puedan presentarse.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios

5.8.3 Controles de las redes

Debe existir un conjunto de controles físicos y lógicos para el acceso a los diferentes recursos informático, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad.

5.8.4 Seguridad de los servicios de red

Se debe garantizar el monitoreo de los elementos físicos de la red y el tráfico de información que se transporta, a fin de establecer las necesidades de los recursos, su buen desempeño y uso inadecuado de los recursos.

Los servicios de correo e internet deben ser usados por los funcionarios estrictamente para realizar actividades de la entidad, con el cuidado de no realizar procesos masivos que afecten el desempeño de los servicios.

5.8.5 Políticas y procedimientos para transferencia de información

Los intercambios de información y de software se deben basar en una política de intercambio, ejecutar según los acuerdos de intercambio y cumplir la legislación correspondiente.

5.8.6 Acuerdos sobre transferencia de información

Para el intercambio de Información con organizaciones o con usuarios externos, se debe establecer un Acuerdo de Confidencialidad, donde queden especificadas las responsabilidades para cada una de las partes.

5.8.7 Mensajería electrónica

Cada usuario es responsable por el contenido de todas las comunicaciones que almacene o envíe utilizando su cuenta de correo electrónico. Los usuarios no deben enviar mensajes que puedan afectar la imagen de la entidad o generar daño en entes externos.

Está prohibido el uso de la cuenta de correo electrónico del FONCEP, asignada al funcionario, para efectos personales ajenos a las funciones y actividades propias de su cargo.

Queda prohibido la descarga e instalación de software o programas no autorizados desde Internet, así como archivos del tipo música, video, y ejecutables en cualquier formato, sin la respectiva autorización del jefe de

área.

5.9 Adquisición, desarrollo y mantenimiento de sistemas

5.9.1 Objetivo

Garantizar que la Política de Seguridad esté incorporada a los sistemas de información.

5.9.2 Política

Se debe asegurar un adecuado análisis e implementación de los requerimientos de seguridad en el software desde su diseño, ya sea interno o adquirido y debe incluir garantías de validación de usuarios, datos de entrada y salida, así como de los procesos mismos, de acuerdo con la clasificación de los activos a gestionar en la herramienta. Además, se establecerán controles para cifrar la información confidencial y se buscará evitar la posibilidad de una acción indebida por parte de un usuario del sistema. Igualmente, se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.

Para todos los sistemas automáticos que operen y administren información para el FONCEP, se deben buscar que se pueda realizar registro de los eventos de seguridad y permitir el monitoreo de accesos indebidos e intrusiones y la activación de archivos de registro de auditoría (Logs), que permitan determinar y demostrar las distintas acciones modificaciones que sufre esa información crítica y que pueda ser evaluada y auditada por el dueño del activo de la información.

Toda la información utilizada y almacenada en los distintos sistemas informáticos, debe tener un responsable o dueño directo quien es el encargado de establecer los niveles de clasificación aplicable. Estos controles deben estar soportados por procedimientos específicos de manejo y control de información.

Para la implementación de esta política se debe tener en cuenta entre otros los siguientes principios.

5.9.3 Análisis y especificación de los requisitos de seguridad

La inclusión de un nuevo producto de software en el FONCEP o control de cambio a los aplicativos existentes, debe estar precedida de la definición de los requerimientos funcionales, controles, registros de auditoría y características o especificaciones de seguridad asociados a él y a su implantación, además del análisis de riesgo y de impacto derivado en una posible falla.

5.9.4 Procedimientos de control de cambios de los sistemas

Se debe implementar un procedimiento de control de cambio para los sistemas, que permita realizar toda la trazabilidad de las solicitudes, los cuales deben asegurar que sólo los cambios autorizados sean implantados. Se debe dar una aprobación formal por parte de las áreas propietarias de la información (funcionalidad), para que los programas sean implantados en los entornos de producción. Se debe mantener un registro de todas las implantaciones realizadas en el ambiente de producción para identificar quién, cuándo y dónde se realizó la instalación. Este procedimiento debe ser funcional para los desarrollos realizados directamente por FONCEP, como los contratados.

El procedimiento, debe contemplar todos los pasos requeridos en el control de cambios como son: Definición detallada de la necesidad, solicitud, viabilidad, análisis, diseño, desarrollo, pruebas, aprobación, documentación e implementación en el ambiente de producción; incorporando en los pasos requeridos los lineamientos y necesidades en cuanto a la seguridad de la información.

5.10 Relaciones con los proveedores

Ver detalle de las políticas en el documento **POL-GSI-GSE004 POLÍTICA DE PROVEEDORES**

5.10.1 Objetivo

Garantizar que la relación con los proveedores este claramente definida y ajustada a las necesidades de Seguridad de la de información.

5.10.2 Política

Se debe asegurar que riesgos asociados con la tercerización de servicios y bienes, deben tener un adecuado manejo de las condiciones de seguridad de la información, en las fases de selección del tercero, contratación, ejecución, finalización y retiro.

Se debe contar con acuerdo de confidencialidad y niveles de servicio que permitan cumplir con las políticas de seguridad de la información y realizar seguimiento permanente de su cumplimiento.

5.11 Gestión de incidentes de seguridad de la información

5.11.1 Objetivo.

Gestionar las incidencias que afectan a la seguridad de la Información.

5.11.2 Política.

Se debe asegurar que se haga una adecuada evaluación del impacto en

el FONCEP frente a los eventos de seguridad relevantes, en los cuales las políticas de seguridad hayan sido desatendidas o traspasadas y realizar planes de atención de incidentes y mejora de procesos, para aquellos eventos que resulten críticos para la supervivencia del mismo. Estos planes deben considerar medidas técnicas, administrativas y de vínculo con entidades externas; deben probarse y revisarse periódicamente; y deben estar articulados en todo el organismo con los diferentes tipos de recursos tecnológicos y no tecnológicos. La Entidad debe contar con los procedimientos que se consideren necesarios para el reporte, control, seguimiento, recolección de evidencias, solución, mejoramiento y aprendizaje

5.12 Aspectos de seguridad de la información de la gestión de continuidad de negocio

5.12.1 Objetivo.

Considerar la continuidad de seguridad de la información en los procesos de gestión de la continuidad de negocio de la Entidad.

5.12.2 Política.

El FONCEP debe incluir los requisitos de seguridad de la información en los procesos de gestión de continuidad de negocio en toda la organización.

Se debe desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información con las condiciones de calidad requeridos por la Entidad, después de la interrupción o la falla de los procesos críticos para la entidad. Dichos planes deben cumplir con los requisitos de seguridad de la información definidos por las políticas de seguridad de la información establecidas en este documento.

Se debe procurar que las instalaciones de procesamiento la Entidad, cuente redundancia suficiente para cumplir los requisitos de disponibilidad requeridos y realizar pruebas de simulación de varios escenarios posibles de emergencias y lograr buscando la recuperación de información en los tiempos y condiciones definidos.

5.13 Cumplimiento

5.13.1 Objetivo.

Prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y de las exigencias de

seguridad.

5.13.2 Política.

Garantizar que la gestión de la seguridad dé cumplimiento adecuado a la legislación vigente para lo cual analizará los requisitos legales aplicables a la información que se gestiona incluyendo los derechos de propiedad intelectual, los tiempos de retención de registros, privacidad de la información, uso adecuado de recursos de procesamiento de información y uso de criptografía.

Para la implementación de esta política se debe tener en cuenta los siguientes principios.

5.13.3 Identificación de la legislación aplicable.

El FONCEP establece que, ante cualquier requerimiento o implementación relacionada con los sistemas de información, se deben observar las leyes y regulaciones vigentes para asegurar los requisitos regulatorios que apliquen.

5.13.4 Derechos de propiedad intelectual (DPI).

Deben existir controles y se deben ejecutar revisiones de su aplicación para asegurar que se están respetando los derechos de propiedad intelectual del material contenido en los sistemas de información utilizados por la entidad.

Deben existir mecanismos que permitan un control estricto de las licencias de software utilizadas en la Entidad, garantizando que se tenga el permiso o adquisición necesario para su uso.

El Administrador de cada plataforma debe mantener el control de todas las licencias de software adquiridas e instaladas.

Se deben realizar revisiones periódicas a los sistemas de información, servidores y estaciones de trabajo, a fin de verificar que no se tenga instalado software no licenciado y autorizado previamente, de acuerdo con el procedimiento de autorización de software. El usuario es responsable por la instalación y utilización de programas no autorizados en su computador.

5.13.5 Protección de los registros de la organización.

Todos los registros que el líder funcional y los jefes de área definan como importantes para el FONCEP, deben guardarse en sitios seguros con el fin de evitar pérdidas, destrucción y falsificaciones. La solicitud debe

realizarse en forma explícita por parte del propietario de la información.

5.13.6 Protección de los datos y privacidad de la información personal.

Los registros de personal y sus datos privados establecidos por la normatividad deben almacenarse en lugar seguro para evitar robo de información privada que pueda afectar la integridad de los usuarios del FONCEP.

Se debe establecer el tiempo de retención apropiado, determinado por la legislación colombiana vigente, para el almacenamiento de los registros identificados.

5.13.7 Reglamentación de los controles criptográficos.

Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes

5.13.8 Cumplimiento con las políticas y las normas de seguridad.

Los Directivos y el Comité de Seguridad de la Información, debe asegurar que todas las políticas, normas, procedimientos y estándares definidos para el FONCEP son cumplidas en su totalidad.

5.13.9 Verificación del cumplimiento técnico.

Los sistemas de información del FONCEP, deben ser revisados periódicamente para verificar que cumplan con los estándares de seguridad definidos.

Toda actividad de Auditoría debe estar planificada y acordada con el cotte de seguridad de la información, previo a su ejecución de modo que no afecte a la operatoria diaria del Sistema y evitar interrupciones graves en toda la plataforma tecnológica.

5.14 Conexión Segura del Teletrabajo

Ver detalle de las políticas en el documento **POL-GSI-GSE006 POLÍTICA DE CONEXIÓN SEGURA DEL TELETRABAJO.**

5.14.1 Objetivo.

Definirá lineamientos para controlar la modalidad de Teletrabajo en sus oficinas como instrumento para promover la modernización de la organización, la inserción laboral, reducir el gasto en las Instituciones

Públicas, incrementar la productividad del funcionario, el ahorro de combustibles, la protección del medio ambiente, y favorecer la conciliación de la vida personal, familiar y laboral, mediante la utilización de las Tecnologías de la Información y las Comunicaciones Tics

5.14.2 Política.

La presente política tiene por objeto establecer los lineamientos técnicos en seguridad de la información necesarios para aplicar el Teletrabajo de conformidad con las nuevas tecnologías de la Información y Comunicación desarrolladas o que lleguen a serlo dentro del FONCEP, con la finalidad de cuidar la confidencialidad, integridad y disponibilidad de la información de FONCEP. Este documento formara parte de la política general de Teletrabajo de FONCEP.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	Fecha de emisión del documento 13 de septiembre de 2017	Creación y Adopción del Documento El documento pertenecía al proceso de Gestión de Administración de activos.

Elaborado por:	Revisado por:		Aprobado por:
	Contenido	Metodológica OAP	
DAVID DELGADO Contratista	**MARIANA MARIN**	**ALEJANDRA SUÁREZ**	**SILVIA FERNANDA ALZATE PÉREZ** Jefe de la Oficina de Informática y Sistemas
	Contratista	Contratista OAP	