# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

# 2020

**CONTENIDO**

## 1. OBJETIVO

Definir las acciones que debe asumir el FONCEP para continuar con la implementación del Modelo de Seguridad y Privacidad de la Información-MSPI, preservando la integridad, confidencialidad y disponibilidad de la información.

## 2. ALCANCE

Inicia con la presentación del plan, las actividades que se han desarrollado para la implementación de la política de seguridad y privacidad de la información y finaliza con la proyección de las actividades a realizar en la siguiente vigencia

## 3. NORMATIVIDAD

- NTC ISO 27001
- Modelo Integrado de Planeación y Gestión - MIPG
- Modelo de Seguridad y Privacidad de la Información - MSPI

## 4. TERMINOLOGÍA

**Modelo de Seguridad y Privacidad de la Información - MSPI:** herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades.

**Activos de información:** son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

**PHVA:** es una herramienta de planificación y mejora continua.

**Seguridad de la Información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

**Plan de Continuidad de TI:** este documento se establecen las actividades que se requieren para el desarrollo del manual de continuidad de los servicios de TI y cubrirá los siguientes aspectos:

- Línea base, evaluación y mitigación del riesgo
- Plan del manejo de la emergencia
- Plan de recuperación

**SGSI:** Sistema de Gestión de Seguridad de la Información.

**MSPI**: Modelo de seguridad y privacidad de la información

# 5. PLAN DE IMPLEMENTACIÓN DEL MSPI

## 5.1. Introducción

El Plan de implementación para el Modelo de Seguridad y Privacidad de la Información (MSPI), es la respuesta activa a la fase de planeación en la que se define el alcance, las políticas, las acciones y el apoyo de la dirección; la publicación, difusión y apropiación por parte de los responsables de los activos de información.

Con las acciones de implementación no solo se identifican y clasifican los activos (inventario de activos de información) sobre los cuales se aplican diferentes controles para preservar la confidencialidad, integridad y disponibilidad de la información, sino que se evalúan los riesgos, amenazas, vulnerabilidades, se establecen responsables de la seguridad y se hacen las primeras mediciones. Vienen luego los indicadores, la valoración de los resultados y la mejora continua.

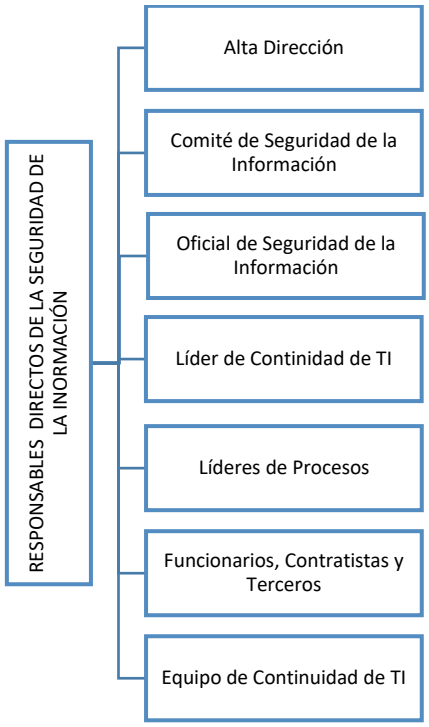
Si bien FONCEP presenta avances en la fase de implementación, el ciclo PHVA exige desarrollar estrategias concretas para su sostenibilidad, teniendo en cuenta factores como: cambios en la normatividad, dinámicas de la organización, infraestructura tecnológica, implementación de servicios, cambios en los sistemas de información y disponibilidad de los recursos.

También se debe tener en cuenta acciones de mejora propuestas en las auditorías internas del Modelo de Seguridad y Privacidad de la Información de FONCEP, lo que indica que la construcción de los principios de seguridad de la información tiene ya una trayectoria importante que se debe considerar y valorar.

## 5.2. Roles y responsabilidades de la seguridad de la información

La asignación y delimitación de responsabilidades para asegurar que se implanta y satisfacen los objetivos propuestos en la presente Política de Seguridad de la información para FONCEP; requieren del establecimiento de unas determinadas funciones encargadas de los aspectos generales de gestión de la seguridad de la información.

A continuación, se describe el gobierno de la seguridad de la información para FONCEP:




Los siguientes roles y responsabilidades establecidos en la Entidad, frente a la seguridad de la información:

| Roles | Responsabilidades y Funciones |
|---|---|
| **Alta Dirección** | • El equipo de la alta dirección y el Comité de Seguridad de la Información son responsables de garantizar que la seguridad de la información se aborde adecuadamente en toda la Entidad.<br>• Cada uno de los funcionarios de la alta dirección son los responsables de velar por la protección de la información que se gestiona en su área de acuerdo con las políticas y normas de seguridad de la información del FONCEP, al igual que realizar el levantamiento de los activos de información de cada una de sus áreas.<br>• La Dirección General es el dueño de la política de seguridad de la información y delega las responsabilidades de documentación sobre seguridad de la información a la persona responsable de la SGSI quien se apoyará en la Oficina de Informática y Sistemas para las definiciones y modificaciones que pueda requerir esta política con el trascurso del tiempo.<br>• Cualquier cambio a la política deberá ser aprobado por el Director General, Dueño de Proceso TI y Jefe de Infraestructura y/u Oficial de Seguridad Informática. |

| | |
|---|---|
| | • Velar por la aplicación del Plan de Continuidad de TI, así como formular, y gestionar las modificaciones en el mismo, y someterlas a aprobación por parte de la Junta Directiva.<br>• Validar los procesos críticos empresariales que se deban considerar en el Plan de Continuidad de TI, así como la estimación del tiempo máximo que puede soportar la Entidad con la interrupción del servicio, producto del incidente que se presente.<br>• Asegurar la formulación, evaluación y actualización de los Planes de Continuidad de TI, por parte de los responsables de los procesos críticos, y que se divulguen a todos los funcionarios, contratistas y proveedores de servicios. Se entiende como plan de continuidad de TI, un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto en la operación del negocio.<br>• Garantizar que se documenten y mantengan actualizados y disponibles los procedimientos para hacer frente a un incidente, desde que éste se presenta, hasta la restauración o vuelta a la normalidad, tanto en lo que se refiere al accionar interno como externo a la Empresa.<br>• Asegurar que las funciones y responsabilidades detalladas en los planes de continuidad de negocio, se asignen al personal idóneo para la atención de los incidentes. El mismo criterio se aplicará al plan de sucesión en caso de incidentes.<br>• Velar porque se cumpla con los planes de capacitación al personal, tanto titular como sucesor en los roles que debe desempeñar en caso de incidentes.<br>• Asegurar que, como parte de los planes de continuidad, se elaboren y actualicen los planes de comunicación interna y externa, para aplicar cuando se presente un incidente.<br>• Establecer el mecanismo para asegurar que se considere la opinión de los sujetos interesados en la elaboración de los planes.<br>• Asegurar que se mantenga actualizada la evaluación de proveedores de insumos para los procesos críticos y que se evalúen periódicamente los requerimientos de repuestos en stock para esos procesos críticos.<br>• Asegurar que los planes de continuidad incluyan en forma detallada los roles ante la presencia de un incidente y que se realicen las pruebas de validación y efectividad de estos planes, así como de control del tiempo requerido para la restauración de las operaciones.<br>• Asegurar que, ante cambios significativos en los procesos empresariales, se actualice el plan de continuidad de TI. |
| **Comité de Seguridad de la Información** | • Está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad de la información. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones, el Comité efectuará la evaluación y revisión de la situación de FONCEP en cuanto a seguridad de la información, |

| | |
|---|---|
| | incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.<br>• El Comité de Seguridad de Información de la Entidad, será el responsable de velar por el cumplimiento del plan de implementación del MSPI.<br>• El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.<br>**Funciones del comité.**<br>• Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.<br>• Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad.<br>• Acompañar e impulsar el desarrollo de proyectos de seguridad.<br>• Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de FONCEP.<br>• Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.<br>• Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.<br>• Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar, riesgos.<br>• Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.<br>• Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.<br>• Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.<br>• Las demás funciones inherentes a la naturaleza del Comité. |
| **Oficial de Seguridad de la Información** | El Oficial de seguridad de la información de FONCEP o quien haga sus veces, debe definir los procedimientos para aplicar la Política de seguridad informática y seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro del FONCEP<br>• Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades que permitan la implementación del MSPI<br>• Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.<br>• Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información. |

| | |
|---|---|
| | • Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.<br>• Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos de seguridad digital y reportar al Comité de seguridad en caso de ser necesario.<br>• Trabajar de manera integrada con el grupo o áreas asignadas |
| **Líder de Continuidad de TI** | Es el encargado de dirigir y liderar todas las actividades del plan de continuidad de TI. Es responsable de declarar la contingencia ante el escenario de interrupción del centro de cómputo principal, con base en las decisiones tomadas por el Equipo de Continuidad del Negocio o en situaciones donde amerite realizar su activación inmediata.<br>Responsabilidades<br>• Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad.<br>• Mantener comunicación constante entre Coordinadores de Recuperación del Negocio durante el estado de contingencia.<br>• Entregar los reportes correspondientes al Comité Directivo sobre el estado de la recuperación.<br>• Salvaguardar la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de la Entidad.<br>• Coordinar con el Comité Directivo, la actualización, mantenimiento y probar el plan de continuidad de TI.<br>• Evaluar y solicitar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia de la entidad.<br>• Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia.<br>• Velar por la ejecución del debido análisis causa – raíz del evento que ocasionó la contingencia. |
| **Líderes de Procesos** | Son los responsables de la aprobación de cambios o desarrollos adicionales sobre un sistema, así como la definición de usuarios que podrán acceder al sistema y los niveles de accesos otorgados a cada usuario para el cumplimiento de sus funciones con respecto a esta aplicación.<br>Son los responsables de la identificación y actualización de los activos de información de cada uno de los procesos de la Entidad. |
| **Funcionarios, Contratistas, Terceros y Proveedores** | Son todos aquellos que prestan algún servicio profesional a la Entidad y que en algunos casos tendrán acceso a la información y a los activos tecnológicos de la entidad, para la ejecución de sus labores profesionales según los compromisos adquiridos con la Entidad.<br>Estos deben firmar un acuerdo de confidencialidad con la Entidad cuando requieran conocer, acceder o manejar información confidencial o alguno de sus clientes.<br>Es responsabilidad de toda persona vinculada como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista o pasante; reportar los |

| | |
|---|---|
| | incidentes de seguridad, eventos sospechosos y/o el mal uso de los recursos institucionales de los cuales tenga conocimiento. |
| **Equipo de Continuidad de TI** | Conformado por los líderes designados o delegados de los procesos críticos quienes son los responsables de liderar y evaluar la funcionalidad de la operación del Plan de Continuidad de TI e informar al Líder de Continuidad de TI cualquier cambio que afecte las estrategias definidas en el mismo. |

### 5.3. Comunicación del plan

El plan se publica en el portal de la Entidad y se realizará la entrega al área de comunicaciones, para su respectiva difusión y socialización.

### 5.4. Actualización y monitoreo

El plan se validará y actualizará anualmente, estableciendo su avance y nuevas metas para el siguiente año.

### 5.5. Actividades para desarrollar para el seguimiento del Plan de implementación del PLAN

- **Política general de seguridad de la información**

  **Responsable:** Alta Dirección.

  **Actividades:**
  - Revisión semestral del cumplimiento de la política general de seguridad de la información.
  - Revisar y/o ajustar la política de seguridad de la información al menos cada año.
  - Hacer seguimiento a las evidencias de actualización y revisión del cumplimiento de la política de seguridad.

- **Procedimientos de seguridad de la información**

  **Responsable:** Encargado de la Seguridad - Líderes de los procesos de FONCEP.

  **Actividades:**
  - Realizar seguimiento de la implementación de los procedimientos del SGSI.
  - Revisar y/o actualizar los procedimientos del SGSI.
  - Hacer seguimiento a las evidencias de actualización y revisión y de la implementación de los procedimientos del SGSI.

- **Gestión de activos de TI**

  **Responsable:** Encargado de la seguridad - Líder proceso Gestión de Servicios de TI

**Actividades:**
- Realizar evaluación de vulnerabilidades y Ethical hacking a la infraestructura de TI y seguimiento a su remediación, de acuerdo con su nivel de criticidad. Esta labor se debe realizar al menos cada 12 meses.
- Verificar la ejecución del re-test de pruebas de seguridad.

- **Gestión de activos de información**

  **Responsable:** Líderes de los procesos del FONCEP
  **Actividades:**
  - Validar y actualizar el inventario de activos de información de cada proceso del FONCEP. Esta actividad se debe realizar cada 12 meses o cuando ocurra un cambio importante en los procesos y que generen cambios en los activos.

- **Indicadores de seguridad de la información**

  **Responsable:** Encargado de la seguridad
  **Actividades:**
  - Realizar seguimiento al cumplimiento de las metas de los indicadores del SGSI.
  - Realizar seguimientos a las acciones correctivas planteadas para los indicadores que no cumplen las metas.
  - Hacer seguimiento a las evidencias de ejecución de acciones correcticas.

- **Gestión de riesgos seguridad digital**

  **Responsable:** Encargado de la Seguridad – Planeación Estratégica y Líderes de los procesos de FONCEP.

  **Actividades:**
  - Revisar y realizar seguimiento trimestral de los Planes de Tratamiento de Riesgos.
  - Realizar valoración trimestral del riesgo residual.
  - Realizar seguimiento a la Documentación del Plan de Tratamiento de Riesgos.

- **Continuidad de TI**

  **Responsable:** Encargado de la Seguridad, jefe OIS y Líderes de los procesos de FONCEP.

  **Actividades:**
  - Realizar seguimiento y revisión de la ejecución de las pruebas del Plan de Continuidad de TI.
  - Realizar seguimiento a la documentación y lecciones aprendidas de los resultados de las pruebas del Plan de Continuidad de TI.
  - Revisión de las acciones de mejora planteadas para corregir las acciones de mejora identificadas en las pruebas del Plan de Continuidad de TI.

- **Plan de comunicación, socialización y sensibilización**

  **Responsable:** Encargado de la Seguridad – Planeación Integral, talento humano.

  **Actividades:**
  - Realizar mínimo 2 jornadas de sensibilización en seguridad de la información en el año y al menos una jornada de reinducción en el año.
  - Realizar evaluación de conocimientos de seguridad posterior a las capacitaciones (Encuestas).
  - Hacer seguimiento a las evidencias de socialización del SGSI.

- **Auditoría**

  **Responsable:** Planeación Estratégica.

  **Actividades:**
  - Realizar seguimiento al cierre de las no conformidades producto de las auditorías.
  - Programar una revisión de verificación de cierre de no conformidades del SGSI.
  - Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso.

- **Gestión de incidentes de seguridad de la información**

  **Responsable:** Encargado de la Seguridad

  **Actividades:**
  - Realizar el seguimiento a la gestión de incidentes de seguridad de la información incluyendo cierre.
  - Realizar seguimiento a las lecciones aprendidas producto de la gestión del incidente.
  - Realizar revisión y seguimiento de los reportes de eventos de seguridad de la información reportados por los funcionarios de FONCEP.

- **Resultados de pruebas de los servicios del centro de cómputo alterno y Plan de Continuidad de TI**

  **Responsable:** Encargado de la Seguridad – Encargado y/o administrador de recurso tecnológico.

  **Actividades:**
  - Revisar los informes de pruebas ejecutadas al centro de cómputo alterno y Plan de Continuidad de TI.
  - Realizar seguimiento a las lecciones aprendidas y acciones de mejora producto de las pruebas realizadas al centro de cómputo alterno y Plan de Continuidad de TI.
  - Realizar seguimiento a los riesgos identificados en las pruebas ejecutadas**.**

- **Resultados de revisión periódica del SGSI.**

**Responsable:** Planeación estratégica**.**

**Actividades:**

- Programar y realizar auditoría de del sistema de seguridad de la información
- Realizar seguimiento sobre los resultados de las revisiones periódicas.
- Hacer seguimientos al cierre de los hallazgos de incumplimiento a las políticas y controles del SGSI.
- Realizar seguimiento al cierre de hallazgos que quedan pendientes de la primera revisión.

- **Plan de mejoramiento de las No conformidades.**

**Responsable:** Planeación Integral y Gestión de Servicios de TI

**Actividades:**

- Realizar plan de mejoramiento, en concordancia con los recursos de la OIS
- Realizar seguimiento al cierre de las no conformidades producto de las auditorías externas al SGSI en el año.
- Programar una revisión de verificación de cierre de no conformidades del SGSI del año.
- Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso.

### 5.6. Seguimiento a la ejecución del plan 2019

#### 5.6.1. Aspectos generales

El plan del Modelo de Seguridad y Privacidad de la Información (MSPI) se implementa de acuerdo con las brechas encontradas y evaluadas en la matriz de aplicabilidad establecida por el MinTIC (articles-5482_Instrumento_Evaluacion_MSPI). Dicha matriz mide el avance del MSPI en el FONCEP y evidencia las acciones realizadas, en el marco de la NTC ISO 27001:2013.

#### 5.6.2. Avance sobre las actividades definidas en la matriz de aplicabilidad

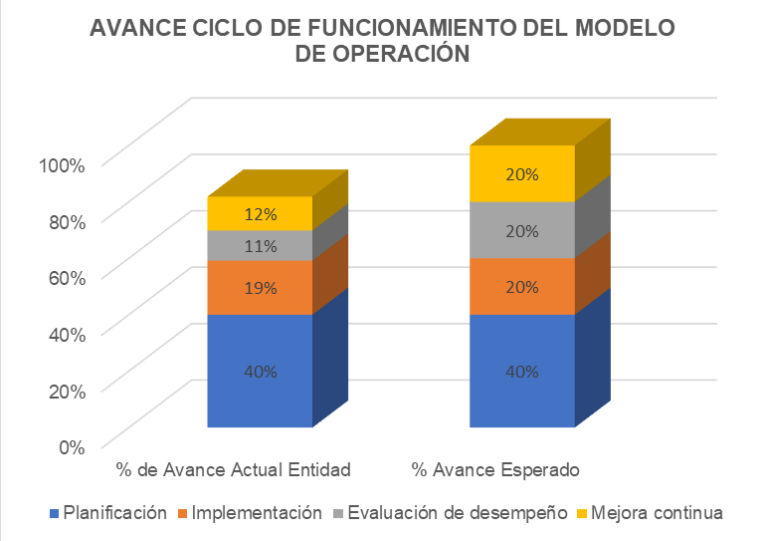
Para el 2019 el nivel de implementación del MSPI en FONCEP asciende al 84%, de acuerdo con lo siguiente:

En cuanto a la Evaluación de Efectividad de controles aplicados de la ISO 27001, el FONCEP se encuentra en la aplicación de 84%:

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual | Calificación Objetivo | EVALUACIÓN DE EFECTIVIDAD DE CONTROL |
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 100 | 100 | **OPTIMIZADO** |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 83 | 100 | **OPTIMIZADO** |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 90 | 100 | **OPTIMIZADO** |
| A.8 | GESTIÓN DE ACTIVOS | 98 | 100 | **OPTIMIZADO** |
| A.9 | CONTROL DE ACCESO | 100 | 100 | **OPTIMIZADO** |
| A.10 | CRIPTOGRAFÍA | 50 | 100 | **EFECTIVO** |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 95 | 100 | **OPTIMIZADO** |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 82 | 100 | **OPTIMIZADO** |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 68 | 100 | **GESTIONADO** |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 83 | 100 | **OPTIMIZADO** |
| A.15 | RELACIONES CON LOS PROVEEDORES | 80 | 100 | **GESTIONADO** |
| A.16 | ESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓ | 86 | 100 | **OPTIMIZADO** |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 80 | 100 | **GESTIONADO** |
| A.18 | CUMPLIMIENTO | 76 | 100 | **GESTIONADO** |
| **PROMEDIO EVALUACIÓN DE CONTROLES** | | **84** | **100** | **OPTIMIZADO** |


En cuanto al avance ciclo de funcionamiento del modelo de operación (PHVA), se encuentra en un 82%.

| Año | AVANCE PHVA | | |
|---|---|---|---|
| | COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
| 2015 | Planificación | 40% | 40% |
| 2016 | Implementación | 19% | 20% |
| 2017 | Evaluación de desempeño | 11% | 20% |
| 2018 | Mejora continua | 12% | 20% |
| **TOTAL** | | **82%** | **100%** |




Haber logrado estos avances de implementación del MSPI ha sido gracias al esfuerzo liderados por la OIS con la participación de toda la Entidad y con el respaldo incondicional de las directivas del FONCEP a la seguridad de la información, porque es claro que es un trabajo que toda la Entidad. Los resultados de todo este trabajo se resumen en las siguientes acciones.

### 5.6.2.1. Política general de seguridad de la información.

Creación inicial de la política de seguridad se adopta desde el 2016 y se ha venido revisando y actualizando. Mediante la modificación del Manual Modelo se Seguridad y Privacidad de la Información el 13 de septiembre de 2017, se modifica la 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."* Este manual fue adoptado en el acuerdo 10 de 2018.

En vigencia del 2019 se actualizó el manual, incluyendo un capítulo relacionado con los roles y responsabilidades en seguridad de la información y la política de tratamiento de datos personales, siendo adoptado por el comité de Dirección. Se encuentra publicada en la herramienta Visión.

#### 5.6.2.2. Procedimientos de seguridad de la información

Los procedimientos que en conjuntos con el Oficial de Seguridad de la Información y la OIS ha construido, se enlistan a continuación y se evidencia las actualizaciones que se han hecho para cada uno con el fin de mejorar el rendimiento de las operaciones en cuanto a seguridad de la información y plantear las actualizaciones para aquellos que así lo requieran.

| Código | Nombre | Versión | Fecha versión |
|---|---|---|---|
| PDT-APO-GST-015 | Procedimiento de Manejo de Incidentes de Seguridad de la Información. | 5 | 5/07/2019 |
| PDT-APO-GST-018 | Procedimiento Gestión de Logs | 1 | 10/06/2019 |
| PDT-APO-GST-014 | Procedimiento para Desarrollo y Soporte de Software | 5 | 14/08/2019 |
| PDT-APO-GST-012 | Procedimiento Pruebas del Plan de Continuidad de TI | 1 | 1/02/2019 |
| PDT-APO-GST-010 | Procedimiento Retorno a la Operación | 1 | 6/12/2018 |
| PDT-APO-GST-011 | Procedimiento Valoración de Daños y Activación de la Contingencia | 2 | 17/07/2019 |
| PDT-APO-GST-009 | Procedimiento para la Realización del Mantenimiento del PCSTI | 1 | 6/12/2018 |
| PDT-APO-GST-001 | Procedimiento Gestión de Redes y Comunicaciones | 1 | 10/07/2018 |
| PDT-APO-GST-016 | Procedimiento de Gestión de Mesa de Ayuda | 4 | 15/05/2019 |
| PDT-APO-GST-008 | Procedimiento Gestión de Monitoreo de Servicios de TI | 1 | 13/08/2018 |
| PDT-APO-GST-002 | Procedimiento Gestión de Vulnerabilidades Técnicas | 1 | 10/07/2018 |
| PDT-APO-GST-004 | Procedimiento Alistamiento de Equipos de Cómputo para Entrega | 2 | 8/11/2018 |

| | | | |
|---|---|---|---|
| PDT-APO-GST-005 | Procedimiento Gestión Bases de Datos | 1 | 10/07/2018 |
| PDT-APO-GST-017 | Procedimiento Gestión de Backup | 1 | 10/06/2019 |
| PDT-APO-GST-013 | Procedimiento Gestión de Activos | 1 | 20/02/2019 |
| PDT-APO-GST-003 | Procedimiento Gestión de los Cambios de TI | 3 | 1/08/2019 |

Toda la documentación relacionada se encuentra publicada en el sistema de gestión de calidad Suite Visión Empresarial.

#### 5.6.2.3. Gestión de activos de TI

Se realizó la contratación del análisis de vulnerabilidades y Ethical hacking, el cual arrojo las vulnerabilidades de la infraestructura, el plan de remediación para ser resueltas y su posterior verificación. Actualmente se está ejecutando el contrato.

#### 5.6.2.4. Gestión de activos de información del Foncep

En el 2018, se realizó las actividades definidas en la guía de Mintic para realizar el levantamiento de los activos de información de cada uno de los procesos de la Entidad. Como resultado, se genero la actualización de los activos y su publicación de la herramienta Visión y en el portal de la Entidad.

#### 5.6.2.5. Indicadores de seguridad de la información

La mejor forma de medir el nivel de implementación para el FONCEP en seguridad de la información es el porcentaje que arroja la matriz de MinTIC que abarca en su totalidad todos los controles de la ISO 27001, en esta matriz se evidencia que acciones se han realizado para cada control y que aquellas que aún no se han realizado. Adicionalmente permite definir un plan de acción para el mantenimiento y mejoramiento continuo basado en el ciclo PHVA.

#### 5.6.2.6. Gestión de riesgos de seguridad digital

Desde diciembre de 2018 se ha trabajado en la implementación de los riesgos de seguridad de la información. El proceso inicio con la identificación y aprobación de los activos de información por cada uno de los procesos del FONCEP, lo anterior se realizó en conjunto con el área de planeación, la Oficina de Informática y Sistemas y los líderes de cada proceso.

La aprobación de los activos de información se logró en el mes de febrero de 2019 y fueron publicados en la página del FONCEP. Posteriormente se realizaron dos talleres

en donde se expuso el cómo realizar la identificación de los riesgos de seguridad digital para cada uno de los procesos, los riesgos están publicados en la Suite Visión Empresarial.

Los riesgos fueron medidos para el segundo trimestre de 2019 y el seguimiento a dicha medición está a cargo de Control Interno, quien se encarga de revisar que se cumplan los monitoreos planteados y de igual forma se carguen todas las evidencias que se relacionan.

### 5.6.2.7. Continuidad de TI.

El plan de continuidad de TI se desarrolló en el mes de diciembre de 2018 y fue aprobado por el cómitre de Dirección y se encuentra publicados todos los procedimientos en la Suite Visión Empresarial.

La documentación a la que se hace relación se describe a continuación.

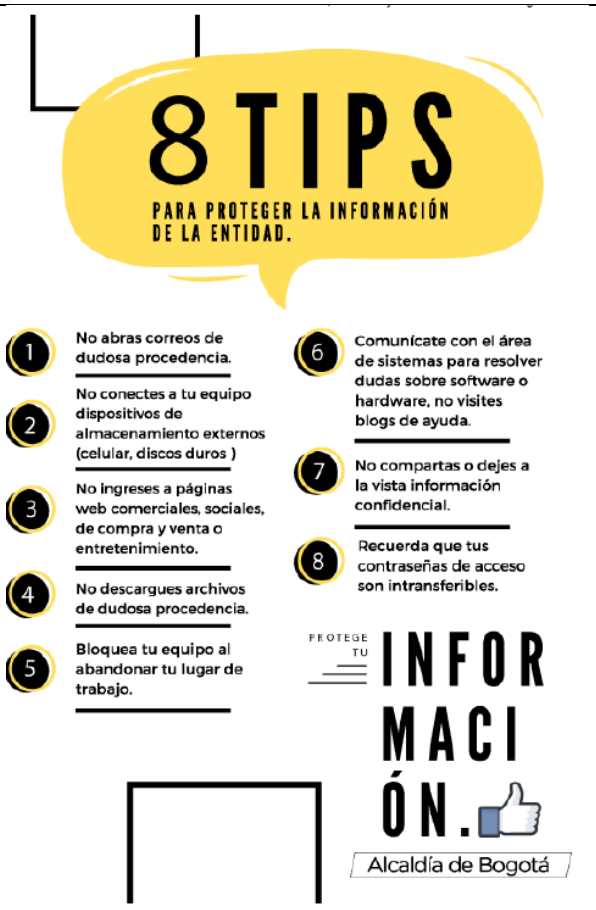
| Documento | Código | Versión | Fecha última actualización |
|---|---|---|---|
| Procedimiento Pruebas del Plan de Continuidad de TI | PDT-APO-GST-012 | 1 | 01/feb/2019 |
| Procedimiento para la Realización del Mantenimiento del PCSTI | PDT-APO-GST-009 | 1 | 06/dic/2018 |
| Procedimiento de Manejo de Incidentes de Seguridad de la Información. | PDT-APO-GST-015 | 5 | 05/jul/2019 |
| Procedimiento Retorno a la Operación | PDT-APO-GST-010 | 1 | 06/dic/2018 |
| Procedimiento Valoración de Daños y Activación de la Contingencia | PDT-APO-GST-011 | 1 | 06/dic/2018 |
| Formato Incidentes de Seguridad. | FOR-APO-GST-009 | 3 | 14/may/2019 |
| Formato de Reporte de Daños | FOR-APO-GST-001 | 1 | 06/dic/2018 |
| Formato Pruebas Plan de Continuidad de TI | FOR-APO-GST-003 | 1 | 01/feb/2019 |
| Formato de Retorno a la Operación | FOR-APO-GST-002 | 1 | 06/dic/2018 |

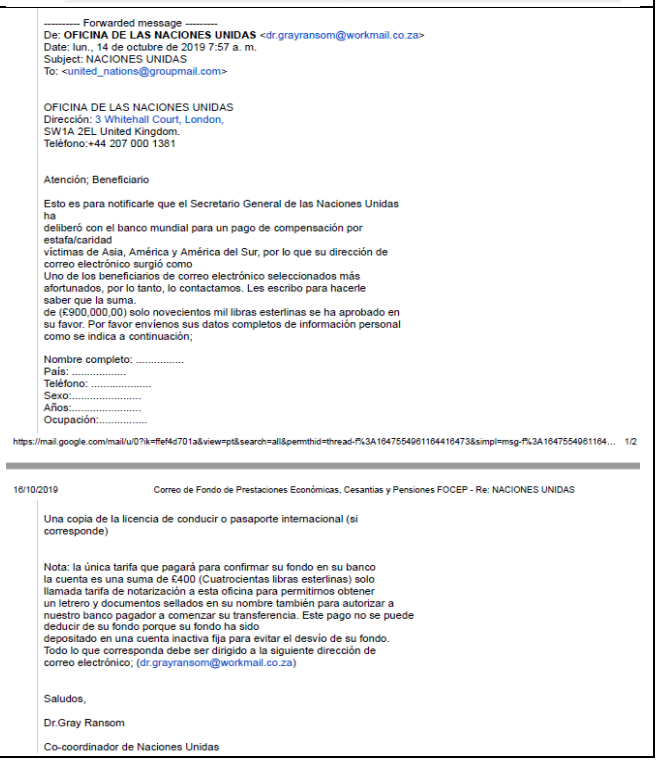
### 5.6.2.8. Plan de comunicación, socialización y sensibilización.

Se realizaron dos campañas de sensibilización y socialización en temas de seguridad de la información del FONCEP, estas incluyeron, charlas y piezas gráficas, una se realizó en el mes de febrero y otra en junio.

| Tema | Fecha de socialización | Resultado |
|---|---|---|
| **Recomendaciones de seguridad** | 11-06-2019 |  |
| **Por tu seguridad...** | 12-06-2019 |  |

| | | |
|---|---|---|
| **¡Atención! Tu correo pudo ser filtrado** | 13-02-2019 |  |
| **El dato de hoy** | 13-06-2019 |  |

| | | |
|---|---|---|
| **Hoy conferencia sobre seguridad en redes sociales**<br><br>**Para esta conferencia se contó con la participación de 57 personas de la Entidad.** | 14-06-2019 |  |
| **Protege la información** | 19-06-2019 |  |

| | | |
|---|---|---|
| **Foncepiando "Últimas noticias" Correo malicioso** | 14-08-2019 |  |
| **Foncepiando "Últimas noticias" Correo malicioso** | 16-10-2019 |  |

Se tiene prevista otra campaña una vez realizada las actividades de evaluación de vulnerabilidades y remediación.

### 5.6.2.9. Auditoría.

Hasta el momento, no se han realizado auditorias al MSPI y de acuerdo con lo planteado por Control Interno, es planeación quien debe realizar o contratar una auditoría externa y tener como plan a mediano plazo de certificar al FONCEP en seguridad de la información.

#### 5.6.2.10. Gestión de incidentes.

La gestión de los incidentes de seguridad de la información se ha registrado conforme a lo descrito en el Procedimiento de Manejo de Incidentes de Seguridad de la Información (PDT-APO-GST-015), los registros y acciones tomadas, se registran por medio de GLPI y los formatos se conservan de manera digital en el servidor atlas de la OIS.

El último incidente de seguridad registrado fue en noviembre de 2018 y hasta el momento no se han vuelto a presentar.

#### 5.6.2.11. Resultados de revisión periódica del SGSI.

Planeación realizó una revisión general este año y se actualizaron los nombres, códigos y formatos de toda la documentación que está registrada en el SGSI. En relación con los hallazgos encontrados relacionados con el incumplimiento del sistema de seguridad de la información, no se tienen debido a que no se han hecho auditorias relacionadas como se expuso en el numeral 8 de este documento.

Cada trimestre se realiza un seguimiento de las acciones definidas en el documento establecido por Mintic y se establece su avance con las acciones realizadas en el periodo.

#### 5.6.2.12. Plan de mejoramiento de las No conformidades.

Dado que hasta el momento no se han realizado auditorias al modelo, no se tiene un informe del estado y por lo tanto no se puede tomar medidas relacionadas con no conformidades.

Una vez programada la auditoria se hará el proceso correspondiente para atender las observaciones que se encuentren en el informe.

## 6. PLAN DE NUEVOS COMPROMISOS

Para el 2020 se plantea realizar las siguientes actividades las cuales darán continuidad a la implementación del modelo. Sin embargo, es necesario continuar con el seguimiento a todos los controles de la norma, para garantizar su cumplimiento y realizar ajustes en caso de establecer su necesidad.

| Control | Descripción | Actividad para desarrollar | Fecha implementación |
|---|---|---|---|

| | | | |
|---|---|---|---|
| A.6.1.5 | La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte. | Se debe solicitar a la Oficina de planeación, incluir en los proyectos la evaluación de riesgos de seguridad de la información. | 2020 |
| A.6.2.1 | Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | Definir y fortalecer la política de dispositivos móviles (celulares y portátiles) y establecer los controles | 2020 |
| A.6.2.1 | Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | Esto es de bajo impacto ya que no se tiene dispositivos móviles institucionales. | 2020 |
| A.6.2.1 | Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | Validar la política de uso de móviles en la red WIFI por perfiles. | 2020 |
| A.6.2.2 | Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. | Establecer un procedimiento que, de los lineamientos de teletrabajo, teniendo en cuenta la política interna del FONCEP. | 2020 |

| | | | |
|---|---|---|---|
| A.7.2.3 | Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | Incluir en el procedimiento de Control Interno Disciplinario, las investigaciones relacionados con las violaciones o incumplimiento de la seguridad de la información. | 2020 |
| A.8.3.1 | Gestión de medios removibles | Definir formas de encripción en medios removibles - Validar con herramienta | 2020 |
| A.13.2.4 | Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. | Validar si es necesario fortalecer los controles y procedimientos actuales. | 2020 |
| A.14.1.3 | La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. | Ajustar los procedimientos para el uso de los servicios. | 2020 |
| A.15.1 | Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores | Reforzar las condiciones y entregables en los contratos con los proveedores de TI y que se puedan ampliar a todos los de la entidad | 2020 |
| A.15.2 | Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores | Realizar seguimiento al cumplimiento de los acuerdos establecidos. | 2020 |

| | | | |
|---|---|---|---|
| A.18.1.4 | Protección de los datos y privacidad de la información relacionada con los datos personales. | Realizar el seguimiento del cumplimiento en el uso de los datos personales | 2020 |
| A.18.1.4 | Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales. | Se debe establecer un mecanismo de autorización del tratamiento de los datos personales. | 2020 |
| A.18.2.1 | Revisión independiente de la seguridad de la información | Solicitar al área de control interno y planeación realizar auditoría, para establecer el avance y la madurez del modelo | 2020 |
| A.18.2.2 | Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional. | Realizar los seguimientos. | 2020 |

| VERSIÓN | FECHA | DESCRIPCIÓN DE LA MODIFICACIÓN |
|---|---|---|
| 001 | Enero 2020 | Creación de documento vigencia 2020 |

| Elaborado por: | Revisado por: | Aprobado por: |
|---|---|---|
| **MARIANA MARÍN RUIZ**<br>Contratista OIS<br><br>**SILVIA FERNANDA ALZATE PEREZ**<br>Jefe Oficina Informática y Sistemas | **Metodológica OAP**<br>**JENNY ANDREA RAMÍREZ OVIEDO**<br>**Contratista** | **COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO** |