FONDECUN

FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CUNDINAMARCA ¡REGIÓN Que Progresa!

Contenido

1. INTRODUCCIÓN.

Dentro de las organizaciones sin importar su área o contexto de desarrollo se presenta la información como uno de los activos más valiosos y primordiales, aportando en el desarrollo de cada proceso interno con el fin de cumplir los objetivos y alcanzar el éxito de la organización.

Por lo cual es importante contar con infraestructura de tecnologías de la información para soportar cada proceso de la entidad, manteniendo disponible la información de todo tipo que requieran los usuarios con calidad y oportunidad, ya que, asegurando el acceso a esta de una forma rápida y segura, la entidad podrá responder cualquier requerimiento en un momento dado, cumpliendo con objetivos estratégicos. Por lo que se hace indispensable contar con un plan de administración de riesgos metodológico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear los riesgos permitiendo minimizar perdidas y maximizar oportunidades.

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

2. NORMATIVIDAD

El plan estratégico de privacidad de la información, se define teniendo en cuenta el siguiente marco normativo:

Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital, define la seguridad de la información como principio de la Política de Gobierno Digital
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015,	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1494 de 2015	Por el cual se corrigen yerros en la Ley 1712 de 2014
Manual gobierno en línea 3.1 ver 2014 – 06 - 12.	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2693 de 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
Ley estatutaria 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Constitución Política de Colombia 1991 - Artículo 15	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

3. DISPOSICIONES GENERALES DEL MANEJO DE LA INFORMACIÓN.

La presente política partiendo de la importancia de la seguridad y del derecho que tienen los titulares de la información, tiene en cuenta la ley 1266 de 2008, "*Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*", con el fin de que se tenga derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellos en las bases de datos y archivos de la entidad.

4. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

4.1 Objetivo General

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de Fondecún, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

4.2 Objetivos Específicos

- Verificar los alcances establecidos en el Modelo de Privacidad y Seguridad de la Información (MPSI) y la documentación base con la que cuenta la entidad. Revisada esta documentación se realiza el cruce con los lineamientos establecidos en la Política de Gobierno Digital.

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.

- Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.

- Establecer los lineamientos, optimización e implementación de la política se Seguridad y Privacidad de la Información, que se deben aplicar en Fondecún.

- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.

- Optimizar la gestión de la seguridad de la información al interior de la entidad.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

El Fondo de Desarrollo de Proyectos de Cundinamarca- Fondecun, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El presente documento describe el Plan de Seguridad y Privacidad de la entidad, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, de tal forma que se asegure la confidencialidad, integridad y disponibilidad los componentes de información.

Aplica a todos los niveles de Fondecún, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por Fondecún, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

7. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Imagen 1. Ciclo de Operación Modelo de Seguridad y privacidad de la información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- Fase de Diagnóstico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

8. PLAN DE IMPLEMENTACIÓN

8.1 Fase De Diagnóstico

En esta fase mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital del Gobierno Nacional (u otros modelos de seguridad de la información aplicables y reconocidos), y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado en la entidad.

Actividad	Descripción
Realizar la evaluación de diagnóstico de seguridad y privacidad de la información bajo criterios reconocidos tales como, el MSPI - Modelo de Seguridad y privacidad de la información de Gobierno Digital, al igual que bajo la ISO/IEC 27001:2013.	Obtener un informe con la identificación del estado de cumplimiento y conformidad de los aspectos de seguridad de la información bajo el (los) modelos evaluados.
Definir las acciones y actividades a implementar orientadas a la planificación e implementación del modelo de seguridad y privacidad de la información acorde con el informe de diagnóstico resultado del diligenciamiento de la herramienta de diagnóstico proporcionada por MINTIC.	Registro de las fases, actividades, recursos y tiempos necesarios para la planeación e implementación del modelo de seguridad y privacidad de la información.
Identificar el nivel de madurez de seguridad de la entidad	De acuerdo a los resultados de la herramienta de diagnóstico identificar la madurez de seguridad de la entidad.

8.2 Fase De Planificación

Definir la estrategia metodológica, que permita establecer la justificación, el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del Modelo de Seguridad y Privacidad de la Información (MSPI).

Actividad	Descripción
Definir el alcance del SGSI de la entidad	Definir los límites sobre los cuales se implementará la seguridad y privacidad de la información
Definir Roles y Responsables de seguridad de la información.	Adicionar las funciones de seguridad de la información al Comité de Riesgos de la entidad y formalizarlas mediante acto administrativo.
Elaborar políticas de seguridad y privacidad de la información	Elaborar Política General de Seguridad y Privacidad la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad.
Identificar y valorar activos de información	Identificación, clasificación y valoración de activos de información, validarlo y aprobarlo.
Identificar y valorar los riesgos de seguridad de la información	Realizar la valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI, definiendo las acciones que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos.
Diagnóstico Plan de IPv4 a IPv6	Realizar el diagnóstico para la transición de la entidad de IPv4 a IPv6. Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6.

8.3 Fase De Implementación

En esta fase se busca llevar a cabo la implementación de la fase de planificación y de los aspectos requisitos presentados tanto por el Modelo de Seguridad y privacidad de la información – MSPI, como los presentados por la norma ISO/IEC 27001:2013; de igual manera, la implementación de los controles de seguridad de la información, que por normativa o por resultado de la valoración de riesgos deban ser implementados.

Actividad	Descripción
Implementar planes de acción resultado de las auditorias	Ejecución de auditorías del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección.
Ejecutar plan de tratamiento de riesgos	Ejecutar el tratamiento de los riesgos transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riegos
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.	Desarrollar actividades para la transición de IPv4 a IPv6.
Realizar e implementar procedimiento de gestión de eventos e incidentes de seguridad	Elaborar los procedimientos para la gestión de eventos e incidentes de seguridad.
Implementar procedimiento de gestión de vulnerabilidades	Elaborar los procedimientos para la gestión de vulnerabilidades.
Ejecutar plan de capacitación y sensibilización de seguridad	Programar y realizar capacitaciones para la sensibilización de seguridad de la información.
Ejecutar pruebas anuales de vulnerabilidades.	Realizar pruebas orientadas a verificar aspectos como: (i) los protocoles internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y de sus empleados.

a. Fase Evaluación Del Desempeño

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

Actividad	Descripción
Ejecución de auditorías de seguridad de la información	Realizar auditorías de seguridad de la información con la finalidad de verificar que los objetivos de control, procesos y procedimientos.

b. Fase De Mejora Continua

Una vez se conozca el estado de cumplimiento de los objetivos de seguridad de la información, mediante las evaluaciones, se procederá a diseñar los planes de mejoramiento que permitan corrección en los procesos.

Actividad	Descripción
Diseñar plan de mejoramiento	Diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI.

9. TÉRMINOS Y REFERENCIAS

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Standardización - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado "Anexo SL", que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Causa: Razón por la cual el riesgo sucede.

Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.

Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Responsables del Activo: Personas responsables del activo de información.
Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza. 20

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

Aprobó. Comité Insitucional de Gestión y Desempeño
Revisó: Ángela Andrea Forero Mojica-Subgerente Administrativa y Financiera
Elaboró Nelson Reina –Responsable de la Gestión Infraestructura y tecnológica