PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

Contenido

1. OBJETIVOS 3
2. ALCANCE 3
3. TERMINOS Y DEFINICIONES 3
4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CONTRALORIA DE CUNDINAMARCA 6
5. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ... 7
6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI 8
7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 8
8. PLANES DESARROLLADOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9
9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9
10. MARCO LEGAL 9
11. REQUISITOS TÉCNICOS 10
12. DOCUMENTOS ASOCIADOS 10
13. RESPONSABLE DEL DOCUMENTO 10

1. OBJETIVOS

Establecer los lineamientos básicos que permitan mantener en óptimas condiciones de funcionamiento los recursos de TI (tecnología informática: equipos de cómputo, software, información, entre otros) asegurando el control y seguridad de la información.

Describir las actividades del plan de Seguridad y Privacidad de la Información, con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de la Contraloría de Cundinamarca

Controlar y soportar los recursos de datos de cómputo, software y hardware en la entidad, buscando una adecuada administración ante las amenazas técnicas, físicas, tecnológicas y de inoperancia que las afecta

2. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a los procesos de La Contraloría de Cundinamarca , en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI, en los cuales establece los lineamientos que en materia de Seguridad informática son aplicadas a todos los funcionarios públicos, pasantes y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la Contraloría de Cundinamarca. Estos lineamientos están dados para proteger la información y los recursos tecnológicos, así como su recuperación con el fin de responder a los requerimientos de los procesos de la entidad.

3. TERMINOS Y DEFINICIONES

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información*; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información.* Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Activo: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Aplicaciones críticas: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

Brecha: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.

Buenas prácticas: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

Ciclo de vida de la información digital: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la misma clasificación que varía conforme su valor con el tiempo.

Clasificación de las aplicaciones: Las aplicaciones se clasifican conforme los procesos de la entidad y son: Misional, Estratégico y de Apoyo.

Clasificacion de la información: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

Clientes: Persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la organización.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

Corriente electrica regulada: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la Entidad.

Dato: Es una letra, número o símbolo que tiende a convertirse en información.

Dependencias: Son los grupos que conforman la estructura organizacional de la Entidad.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Documento: Es el medio físico que contiene la información que se quiere transmitir.

Dueño de la información: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o reducción de la calidad del servicio.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y que es guardada en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Información Digital: Cuando la información está almacenada en un medio magnético porque cuando se imprime se convierte en documento físico y en este último caso existe en el SGC la dependencia que define los lineamientos, normas, guías y estándares.

Información sensible: Es la tipificación que recibe la información que no se considerada de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Política TIC: Documento que contiene los lineamientos que define la organización para reglamentar el desarrollo de los proyectos y recursos TIC de la Entidad; como las acciones que deben permanecer en el tiempo para alcanzar los objetivos de su negocio.

Politica de seguridad: Es el documento de normas y lineamientos de seguridad de la información que define la Entidad para evitar que surja vulnerabilidades que puede afectar el negocio de la Entidad.

Procesos criticos: Concepto que se utiliza para definir el conjunto de actividades o eventos que se ejecutan bajo ciertas circunstancias que inciden en los productos misionales de la entidad y en la satisfacción de los clientes.

Proveedores: Negocio o empresa que ofrece servicios a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, alojamiento de aplicaciones web etc.

Propietario de la información: Se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

Repositorio de documentos: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

Requerimiento: Necesidad de un servicio TIC que el usuario solicita a través del mecanismo definido por la organización en los procedimientos normalizados.

Servicio: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware; así como de la Plataforma Tecnológica.

Servicios TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo. Los elementos del Servicio TIC son:

Los dispositivos: PC, portátiles, agendas electrónicas, impresoras, teléfonos, sistemas de videoconferencia, etc.

La Red de Área Local corporativa (LAN). Así como las comunicaciones de voz incluyendo el teléfono y ahora llega el momento de proporcionar y gestionar los PC y la electrónica de red necesarios para las comunicaciones de datos.

Las comunicaciones de voz y datos WAN (Red de Área Remota), que incluyen tanto las redes privadas corporativas como el acceso a redes públicas como Internet. La integración de las comunicaciones WAN y estas cada vez se requieren con las comunicaciones LAN.

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TIC: Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás, se realice de manera distribuida y remota. El procesamiento remoto, además de incorporar el concepto de telecomunicación, hoy día hace referencia a un dispositivo como un teléfono móvil o una computadora ultra-portátil, con capacidad de operar en red mediante Comunicación inalámbrica.

Usuario: Persona que utiliza los recursos TIC y que interactúan de forma activa en un proceso, secuencia, código etc.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CONTRALORIA DE CUNDINAMARCA

El Sistema de Seguridad y Privacidad de la Información y de los Sistemas de Información de la Contraloría Departamental de Cundinamarca se desarrollará partiendo del principio de que éste se convierte en el eje propulsor de la Seguridad, mecanismo de garantía para la continuidad y desarrollo de las labores misionales como ente estatal de control y vigilancia, logrando el adecuado nivel de confidencialidad, privacidad, integridad, control, vigilancia,

disponibilidad, y auditabilidad en la infraestructura de la información y sus sistemas.

Para su desarrollo se deberá contar con el compromiso irrestricto de todo el personal directivo de la Institución, el cual irrigará estos preceptos hacia todo el personal que labora en la institución, entre los cuales se cuentan: Personal de Planta, Contratistas, Entidades Públicas o de naturaleza privada, y/o Personas Naturales quienes utilizan los servicios de la Contraloría, como quiera que gran parte de éstos se convierten en elementos muy valiosos dentro del engranaje institucional cual corresponde a convertirse en Activos de la Información.

De esta forma la gestión administrativa de toda la Contraloría se basará en una continua y permanente observancia y administración de los riesgos así como la consolidación de una cultura de seguridad.

La Contraloría de Cundinamarca implementará de manera transversal esta política de tal forma que se alinee con los objetivos de seguridad de la información:

- Minimizar el riesgo el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Contraloría de Cundinamarca.
- Garantizar la continuidad del negocio frente a incidentes.

5. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. Administrar los eventos de seguridad de la información de la Contraloría de Cundinamarca.
2. Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica acorde con la declaración de aplicabilidad aprobada.
3. Cumplir con los requisitos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
4. Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, pasantes y agentes externos).
5. Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI

EL SGSI es aplicable a los activos de información de todos los procesos de la Contraloría de Cundinamarca, verificándolo y aplicándolo a las respectivas áreas de la entidad, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad avalada por el Comité de Seguridad de la Información.

7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información, el cual es el mismo conformado por el comité directivo, y el cual tiene dentro de sus funciones la de impulsar, hacer seguimiento y/o verificación de la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, de la Contraloría de Cundinamarca

Las funciones del Comité de Seguridad de la Información son:

- **Impulsar la implementación del Sistema de Gestión de Seguridad de la Información SGSI.**
- **Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SGSI.**
- **Supervisar la integración del Sistema de Gestión de Seguridad de la Información - SGSI con el Sistema Integrado de Gestión-**
- **Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información.**
- **Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos de la seguridad de la información para Contraloría de Cundinamarca, con el fin de tomar y establecer las medidas necesarias.**
- **Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de Información de la entidad.**
- **Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.**

- Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
- Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- Las demás funciones inherentes a la naturaleza del Comité.

8. PLANES DESARROLLADOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con el desarrollo del Sistema de Gestión de Seguridad de la Información – SGSI de La Contraloría de Cundinamarca , se han desarrollado las actividades hacia el plan de seguridad y privacidad de la información, las cuales se encuentran documentadas en la - (Norma NTC-ISO-IEC 27001:2013),

9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2019 se definen las siguientes actividades para Seguridad y Privacidad de Información, las cuales se encuentran enmarcadas en el plan estratégico:

SE ENCUENTRA EN CONSTRUCCIÓN

10. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

- **Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles "entre otras disposiciones.**

- **Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.**

- **Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.**

- **Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública**

- **Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea.**

11. REQUISITOS TÉCNICOS

- **Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.**
- **Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información tic.**

12. DOCUMENTOS ASOCIADOS

- **Lineamientos para la Administración del Riesgo.**
- **Manual de Políticas de Seguridad de la Información.**

13. RESPONSABLE DEL DOCUMENTO

Grupo de funcionarios área de tecnología.
Jefe Área de la Oficina Asesora de Planeación Sistemas e Informática