CONTROL DE CAMBIOS		
VERSIÓN[1]	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**
1	28 de diciembre de 2015	Primera Emisión del Manual

[1] Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente está publicada en la intranet de la Secretaría Distrital de Gobierno

Elabora:	Revisa:	Aprueba:
Armando Rincón Bernal Rommel Hanz Preciado Rodríguez Profesionales Dirección de Planeación y Sistemas de Información	Sandra Patricia Orne López Luis Alejandro Vargas Profesionales de la Dirección de Planeación y Sistemas de Información Liliana Casas Revisión de Normalización (Grupo SIG-DPSI)	Juan Carlos Garzón Barreto Director de Planeación y Sistemas de Información

TABLA DE CONTENIDO

INTRODUCCIÓN

La información, en sus múltiples códigos y formas, así como los trámites y servicios que las entidades del Estado proveen a los ciudadanos se consideran un bien público. En ese sentido, los activos de información que conforman los bienes y servicios que proveen las entidades públicas son activos públicos y por lo tanto, deben protegerse adecuadamente.

La protección y seguridad de los activos de información, parte del concepto fundante de seguridad de la información la cual se desarrolla mediante el principio rector de la gestión de riesgo, y comprende el conjunto de medidas, procedimientos y controles establecidos para el correcto manejo, gestión y control de la información, en todo su ciclo de vida, así como para garantizar sus propiedades fundamentales; la preservación de la confidencialidad, integridad , disponibilidad, accesibilidad de la información que se complementan con otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad.

Consientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte tecnológico y legal de la Alta Dirección, y con el objetivo que estas sean una herramienta para la definición de los estándares y procesos internos de la Entidad, la Secretaría Distrital de Gobierno, a través de la Dirección de Planeación y Sistemas de Información, debe asegurar que la información disponible cumpla con los criterios de Confidencialidad, Integridad, Disponibilidad, Accesibilidad, Autenticidad, No Repudio, entre otros, mediante el resguardo de datos, la protección frente a accesos no autorizados, el control de acceso a otros sitios web y la adecuada utilización del correo electrónico de la Entidad. Así mismo, proporcionar hardware, software y equipos de comunicaciones en condiciones de seguridad y calidad; realizar revisiones periódicas de seguridad; y garantizar la propiedad de la Información y la buena manipulación de programas de software aplicativo.

Atendiendo a los lineamientos del Sistema Integrado de Gestión(SIG) y Conforme a lo establecido en la resolución 520 de Noviembre 12 de 2013 y Resolución 419 de 2014, por la cual se crea el Comité del Sistema Integrado de Gestión y los Subcomités Técnicos para la implementación y mejora de los Subsistemas de Gestión, en su artículo 11 establece: ***El Subcomité Técnico del Gobierno en Línea - Seguridad de la Información y Gestión Documental*** será el responsable de proponer a la Alta Dirección: i) el compromiso de la implementación del subsistema de gestión de seguridad de la información - SGSI, ii) Los lineamientos para la implementación del SGSI, iii) plan de acción anual con las metas, indicadores, actividades, responsables, recursos necesarios y iv) realizar periódicamente los reportes de avances, en atención a lo anterior, se elabora el actual Manual de Gestión de Seguridad de la Información de la Secretaría Distrital de Gobierno.

1. POLÍTICA DE SEGURIDAD DEL SUBSISTEMA DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DISTRITAL DE GOBIERNO

"La Secretaría Distrital de Gobierno considera la información como un bien público de vital importancia para el cumplimiento de su función pública y normal desempeño. En ese sentido, dicha información junto con las tecnologías y medios utilizados para su procesamiento, constituyen los Activos de Información de la Entidad, los cuales se deben proteger, preservar, administrar y gestionar objetivamente frente a los riesgos internos o externos, deliberados o accidentales.

Por lo tanto, la Secretaría Distrital de Gobierno está comprometida con la protección, preservación y aseguramiento de la confidencialidad, integridad, disponibilidad, accesibilidad, legalidad, confiabilidad y no repudio de los activos de información, en todo su ciclo de vida, mediante la Gestión del Riesgo, en las etapas de implementación, monitoreo y mejora continua. De igual forma, tiene un compromiso con el fortalecimiento de la cultura de la Seguridad de la Información, en los/as servidores/as públicos/as y el cumplimiento de los requisitos legales relacionados con la misma, todo lo anterior, enmarcado en el Sistema Integrado de Gestión de la Entidad."

1.1. POLÍTICAS DE SEGURIDAD QUE SOPORTAN EL SGSI DE LA SECRETARÍA DISTRITAL DE GOBIERNO

- La Secretaría Distrital de Gobierno ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los funcionarios, contratistas, proveedores, socios de negocio o terceros**.
- La Secretaría Distrital de Gobierno **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La Secretaría Distrital de Gobierno **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Secretaría Distrital de Gobierno **protegerá su información** de las amenazas originadas por parte **del personal**.
- La Secretaría Distrital de Gobierno protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Secretaría Distrital de Gobierno controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Secretaría Distrital de Gobierno implementará control de acceso a la información, sistemas y recursos de red.

- La Secretaría Distrital de Gobierno garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Secretaría Distrital de Gobierno garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Secretaría Distrital de Gobierno garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Secretaría Distrital de Gobierno garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2. GLOSARIO

Entiéndase para el presente documento los siguientes términos:

- ***Política:*** Son instrucciones mandatarias que indican la intención de la alta gerencia respecto al funcionamiento de la organización.
- ***Información:*** Se refiere a toda comunicación o representación de conocimiento con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, la cual puede estar digital, audiovisual, impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.
- ***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.
- ***Tecnología de la Información:*** Se refiere al hardware y software operados por la Entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la misma, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- ***Recurso Informático:*** Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan los servicios informáticos.
- ***Usuarios Terceros:*** Todas aquellas personas naturales o jurídicas, que no son funcionarios de la Entidad, pero que por las actividades que realizan en la misma, deban tener acceso a Recursos Informáticos.
- ***Ataque cibernético:*** Intento de penetración a un sistema informático por parte de un usuario no deseado, ni autorizado a accederlo, por lo general con intenciones insanas, perjudiciales o dañinas.
- ***Evaluación de Riesgos:*** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de

procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la Entidad.

- ***Administración de Riesgos:*** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- ***Comité de Seguridad de la Información:*** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas de la Entidad, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. Esto es; autoridades internas, como: Control Interno, Disciplinario, Recursos Humanos o externas, como: Fiscalía, Derechos de Autor, Contraloría, Procuraduría, Personería, etc.
- ***Responsable de Seguridad Informática:*** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los usuarios de la Entidad, que lo requieran**.**
- ***Incidente de Seguridad:*** Un incidente de seguridad es un evento adverso en un sistema o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, accesibilidad legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes

Respecto a la "CLASIFICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN" se deben atender los siguientes términos:

- ***Información Pública*****:** Información de dominio general, a la cual puede tener acceso cualquier persona.
- ***Información Privada:*** Información para uso interno solamente; solo los funcionarios de la Entidad que intervienen en un proceso y/o trámite o los que pertenecen al área de competencia de dicho trámite pueden conocerla.
- ***Confidencial:*** Información de uso exclusivo de un funcionario o grupo de funcionarios de la Entidad, que en caso de ser divulgada sin autorización afecta negativamente los intereses y deberes de la misma. Esta información requiere controles restrictivos y especial cuidado en el acceso, tránsito y almacenamiento.
- ***Reservada:*** Es aquella que por disposición legal expresa tiene reserva, sólo tienen acceso directo ciertas personas (sujetos calificados), en razón de su profesión u oficio.

De acuerdo con lo anterior y en cumplimiento de los requerimientos de seguridad y calidad de la información, en relación con los medios de distribución de información para clientes y partes interesadas, la Entidad ha adoptado en sus políticas los siguientes criterios de seguridad y calidad de la información:

Respecto a las "BASES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN" se deben atender los siguientes términos o características:

- ***Confidencialidad:*** La Secretaría Distrital de Gobierno establece para la información no autorizada o confidencial, la determinación de su no divulgación correspondiente.
- ***Integridad:*** La Secretaría Distrital de Gobierno procura que la información que circula y salvaguarda en la Entidad sea precisa, coherente y completa desde su creación hasta su destrucción o eliminación.
- ***Disponibilidad:*** La Secretaría Distrital de Gobierno determina la disponibilidad de la información en el momento que es solicitada, para el correcto funcionamiento de los procesos, para fundamentar decisiones gerenciales o requerimientos. Así mismo, garantiza los recursos necesarios para su uso.
- ***Accesibilidad:*** La Secretaría Distrital de Gobierno determina el acceso a la información con la limitaciones legales y establece el grado en el que los funcionarios y usuarios pueden utilizar los activos de la información de forma satisfactoria.

Adicionalmente, deberán considerarse los conceptos de:

- ***Autenticidad:*** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando al emisor para evitar suplantación de identidades.
- ***Auditabilidad:*** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- ***Protección a la duplicación:*** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- ***No repudio:*** Se refiere a evitar que una Unidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- ***Legalidad:*** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.
- ***Confiabilidad de la Información:*** Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Respecto a las "CALIDAD DE LA INFORMACIÓN" se deben atender los siguientes términos:

- ***Efectividad:*** La información es uno de los activos de mayor importancia para la Entidad, es pertinente y su entrega debe ser oportuna, correcta y consistente.
- ***Eficiencia:*** Es propósito de la Secretaría Distrital de Gobierno - SDG, que el procesamiento y suministro de información, se realice con el uso óptimo de los recursos tecnológicos con que cuenta la Entidad.
- ***Confiabilidad:*** La información que fluye en la Secretaría Distrital de Gobierno - SDG, es la apropiada para la administración de la Entidad y el cumplimiento de sus obligaciones, por lo tanto esta debe ser confiable y certera.

SIGLAS

ADTIC: Alta Consejería para las Tecnologías de la Información y las Comunicaciones
DPSI: Dirección de Planeación y Sistemas de información
IC: Cómputo intermedios
PSI: Políticas de seguridad de la información
SDG: Secretaría Distrital de Gobierno
SGSI: Subsistema de Gestión de Seguridad de la Información

3. OBJETIVO GENERAL DEL SGSI

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

La Secretaría Distrital de Gobierno está comprometida con la protección, preservación, y aseguramiento de la ***confidencialidad, Integridad, disponibilidad, accesibilidad, legalidad, confiabilidad y no repudio*** de los activos de información, en todo su ciclo de vida, mediante la Gestión del Riesgo, en las etapas de implementación, monitoreo y mejora continua. De igual forma, tiene un compromiso con el fortalecimiento de la cultura de la Seguridad de la Información, en los/as servidores/as públicos/as y el cumplimiento de los requisitos legales relacionados con la misma, todo lo anterior, enmarcado en el Sistema Integrado de Gestión de la Entidad.

3.1. OBJETIVOS ESPECÍFICOS

3.1.1. Integridad de la Información

Se debe proteger y garantizar que los activos de información, entre ellos los datos de la Secretaría Distrital de Gobierno no sufran cambios no autorizados, por lo tanto, la información debe ser protegida de modificaciones imprevistas, no autorizas, accidentales, internas o externas.

3.1.2. Confidencialidad de la Información

Se debe proteger y garantizar que los activos de información, entre ellos los datos o la información sensible de la Secretaría Distrital de Gobierno, no sean accesibles o divulgados por o a personas no autorizadas

3.1.3. Disponibilidad de la Información

Se debe proteger y garantizar que los activos de información, entre ellos los servicios asociados a los procesos de Tecnologías de la información y la comunicación, estén disponibles en todo momento, garantizando la continuidad del negocio para el cumplimento de los objetivos misionales de la entidad.

3.1.4. Accesibilidad de la Información

Se debe garantizar el acceso a la información con las limitaciones legales y establecer el grado en el que los funcionarios y usuarios pueden utilizar los activos de la información de forma satisfactoria.

3.1.5. Legalidad de la Información

Se debe propender por garantizar que los activos de información, de la Secretaría Distrital de Gobierno, cumplan con los parámetros legales, normativos nacionales e internacionales, así como con la reglamentación interna sobre la seguridad de la información de la entidad.

3.1.6. Confiabilidad de la Información

Se debe garantizar la confiabilidad de la Información de la Secretaría Distrital de Gobierno, es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones de la entidad.

3.1.7. No Repudio de la Información

Se debe garantizar que el no repudio de la información en la Secretaría Distrital de Gobierno, es decir que la información enviada, trasmitida y/o recibida en desarrollo de los servicios de red de la entidad se puede probar y no pueda ser negada posteriormente.

Integridad de la información

Se debe proteger y garantizar que los activos de información, entre ellos los datos de la Secretaría Distrital de Gobierno no sufran cambios no autorizados, por lo tanto, la información debe ser protegida de modificaciones imprevistas, no autorizas, accidentales, internas o externas.

Metas- Estrategia -Indicador

Meta 1. Contar con un Inventario y clasificación de los activos de la información

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

Realizar durante el primer trimestre del 2016, el inventario y clasificación de los activos de la información en todas las dependencias de la entidad a nivel central y local.

Indicadores de Gestión

- Aplicación de la guía y matriz para el levantamiento de activos de en toda la entidad.
- Clasificación de los activos de información de la entidad.
- Elaboración del informe contentivo del inventario y clasificación de los activos de la información

Meta 2. Copias de seguridad (Backup)

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

Normalizar durante el primer trimestre de 2016 las directrices y procedimientos para la realización y adecuada protección de las copias de seguridad (Backup) de la entidad.

Indicadores de Gestión

- Generar el instructivo para la elaboración de las copias de seguridad (Backup) de la entidad.
- Efectuar la socialización del instructivo y objetivos de la elaboración de las copias de seguridad (Backup) de la entidad.
- Efectuar un primer balance sobre la efectividad y cumplimiento de la elaboración de las copias de seguridad (Backup) de la entidad.

Meta 3. Definición y protección áreas sensibles

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

Definir y clasificar durante el primer semestre de 2016 de manera clara las áreas sensibles de activos de información de la entidad y tomar las medidas para su adecuada protección.

Indicadores de Gestión

- Establecer de manera precisa que áreas de la entidad a nivel central y local estarán clasificadas como sensibles.

- Tomar las medidas de protección necesarias para su protección física y lógica.
- Establecer los procedimientos para aplicar los controles de acceso físico y lógico para protección de los activos de información de la entidad.

Confidencialidad de la Información

Se debe proteger y garantizar que los activos de información, entre ellos los datos o la información sensible de la Secretaría Distrital de Gobierno, no sean accesibles o divulgados por o a personas no autorizadas.

METAS- ESTRATEGIA -INDICADOR

Meta 1. Designación de los propietarios o responsables de la información

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

De acuerdo con la clasificación de los activos de información, durante el primer semestre de 2016, se hará la distribución de roles asignando quienes en cada dependencia de la entidad serán propietarios o responsables de la información, indicando de manera precisa sus responsabilidades y atribuciones.

Indicadores de Gestión

- Elaborar el instructivo para la designación y funciones de los propietarios o responsables de la información.

- Efectuar la socialización del instructivo y objetivos a los funcionarios que serán designados como propietarios o responsables de la información.

- Designar los funcionarios que propietarios o responsables de la información

Meta 2. Contratos, manual de funciones, Gestión documental

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

De manera coordinada con la oficina asesora jurídica, la dirección de talento humano, durante el primer trimestre de 2016, se incluirán en los textos de los contratos y en los manuales de funciones, el tema de la confidencialidad y seguridad de la información, las obligaciones sobre el tema y las consecuencias de su incumplimiento. De igual manera se elaborara y normalizara un texto de acuerdo de confidencialidad que aplicara gestión documental cuando sea el caso

Indicadores de Gestión

- Inclusión de la cláusula de seguridad de la información en los contratos de Secretaría Distrital de Gobierno.

- Inclusión del tema de seguridad de la información en los procesos de inducción y reducción de los funcionarios y contratistas de la entidad.

- Elaboración y aplicación de los acuerdos de confidencialidad por parte de gestión documental.

Disponibilidad de la información

Se debe proteger y garantizar que los activos de información, entre ellos los servicios asociados a los procesos de Tecnologías de la información y la comunicación, estén disponibles en todo momento, garantizando la continuidad del negocio para el cumplimento de los objetivos misionales de la entidad.

Metas- Estrategia –Indicador

Meta 1. Plan de contingencia

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

El área de sistemas durante el primer trimestre de 2016 debe elaborar un plan de contingencia para dar respuesta oportuna y adecuada a los incidentes de seguridad de la información.

Indicadores de Gestión

- Elaborar el plan de contingencia de seguridad de la información, que contenga procedimientos de respuesta y responsables frente a incidentes de seguridad.

- Se deberá efectuar la socialización el plan de contingencia de seguridad de la información a todos los funcionarios y/o contratistas de la entidad del nivel central y local.

Meta 2. Plan de continuidad del negocio

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

El área de sistemas durante el primer trimestre de 2016 debe elaborar un plan de continuidad del negocio para dar respuesta oportuna y garantizar en caso de incidente el retorno a la normalidad en el menor tiempo posible

Indicadores de Gestión

- Elaborar el plan de continuidad del negocio, que contenga procedimientos de respuesta y responsables frente a incidentes de seguridad.

- Se deberá efectuar la socialización el plan de continuidad del negocio a todos los funcionarios y/o contratistas de la entidad del nivel central y local.

Legalidad de la información

Se debe propender por garantizar que los activos de información, de la Secretaría Distrital de Gobierno, cumplan con los parámetros legales, normativos nacionales e internacionales, así como con la reglamentación interna sobre la seguridad de la información de la entidad.

Metas- Estrategia -Indicador

Meta 1. Conocimiento de insumos legales

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

En coordinación con la oficina jurídica, la dirección de talento humano, durante el primer semestre de 2016, se deberá conocer, identificar y divulgar los aspectos legales relacionados con los activos de información, para garantizar su cumplimiento factor importante de la seguridad de la información de la entidad

Indicadores de Gestión

- Elaborar un nomograma contentito de todas las normas, reglamentos, instructivos, etc., internos y externos de la entidad que tengan relación directa con el tema de la legalidad de los activos de información

- Se deberá efectuar la socialización un nomograma elaborado, para que todos los funcionarios de la entidad, a nivel central y local, conozcan la normativa existente sobre el tema.

Confiabilidad de la información

Se debe garantizar la confiabilidad de la Información de la Secretaría Distrital de Gobierno, es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones de la entidad.

Metas- Estrategia -Indicador

Meta 1. Protección de información sensible

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

Una vez efectuada la clasificación de los activos de información de la entidad, se deben implementar las medidas necesarias para garantizar la seguridad de la información y activos sensibles, y que son vitales para el cumplimiento de sus objetivos misionales.

Indicadores de Gestión

- Adoptar las medidas necesarias para garantizar la seguridad física y lógica de los activos de información sensibles de la entidad.

- Evaluar los controles de acceso físico y lógico, para determinar su cumplimiento y eficiencia, y adoptar las medidas de mejoramiento necesarias,

No repudio de la información

Se debe garantizar que el no repudio de la información en la Secretaría Distrital de Gobierno, es decir que la información enviada, trasmitida y/o recibida en desarrollo de los servicios de red de la entidad se puede probar y no pueda ser negada posteriormente.

Metas- Estrategia -Indicador

Meta 1. Seguridad de las operaciones y servicios de red

MINIMA	75 – 80%	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

Estrategia

Durante el primer trimestre de 2016, desde el área de sistemas, se adoptaran todas las medidas de seguridad para garantizar el correcto funcionamiento de la red y sus servicios internos y externos.

Indicadores de Gestión

- Elaborar el cuadro de medias y controles para garantizar el funcionamiento continuo de la red y sus servicios tanto a nivel interno como externos

- Efectuar una auditoria interna para determinar el estado de la red y sus servicios que permita identificar fallas y fortalezas, y realizar las mejoras continuas requeridas.

4. ALCANCE

El Manual de Gestión de Seguridad de la Información, es una herramienta fundamental de la Política de Seguridad del Subsistema de Gestión de Seguridad de la Información, y es aplicable para todos los aspectos administrativos y de control, a la totalidad de los proceso internos o externos, del nivel central y local que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Secretaría Distrital de Gobierno, cualquiera sea su situación contractual, la dependencia a la cual se encuentren adscritos y el nivel de las tareas que desempeñe, para el adecuado y efectivo cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de los activos de la información de la entidad.

5. DESARROLLO DEL MANUAL

De acuerdo con los lineamientos establecidos por el Sistema Integrado de Gestión Distrital – SIGD, y teniendo en cuenta que la Resolución 419 de 2014, estableció que el Sistema Integrado

de Gestión de la Secretaría Distrital de Gobierno estará conformado entre otros por el subsistema de Gestión de Seguridad de la Información (SGSI), que la misma normativa estableció la creación del Subcomité Técnico de Gobierno en Línea, Seguridad de la Información y Gestión documental, estableciendo como una de sus responsabilidades: "Definir y diseñar los lineamientos, herramientas e instrumentos para la implementación y mantenimiento de los subsistemas a cargo en el nivel central y en las alcaldías locales."

En cumplimiento de lo anterior, de sus objetivos misionales, la Secretaría Distrital de Gobierno, responsable de la gestión política distrital, el desarrollo local y la formulación e implementación de políticas públicas de convivencia, seguridad, derechos humanos y acceso a la justicia, se compromete como co-responsable de la Gestión de la Seguridad de la Información a prevenir, proteger, preservar, administrar y gestionar objetivamente los activos de información de la entidad, junto con las tecnologías utilizada para su procesamiento, frente a los riesgos internos o externos, deliberados o accidentales, con el fin de asegurar la preservación de sus características fundamentales de confidencialidad, integridad, disponibilidad, accesibilidad, legalidad, confiabilidad y no repudio de la información, asociados al desarrollo de sus procesos institucionales, en todo su ciclo de vida, independientemente de los medios de soporte y tratamiento, desarrollando la gestión de riesgos a través de la implementación, monitoreo y mejoramiento continuo del conjunto de medidas, procedimientos y controles que minimicen dichos eventos, fortaleciendo la cultura de la seguridad en los servidores públicos y el cumplimiento de los requisitos legales vigentes acorde con la Política de Seguridad del Subsistema de Seguridad de la Información.

6. SITUACIÓN ACTUAL

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la Secretaría Distrital de Gobierno, no depende únicamente del Grupo de Infraestructura Tecnológica, sino de toda una cultura organizacional que permita la protección y resguardo de la información. Es tan claro este concepto para la Entidad, que se ha dado un gran paso en este sentido con la Resolución No.0177 del 23 de Marzo de 2007, firmada por la Alta Dirección y donde se establecen las políticas de seguridad para el manejo de la información, y se imparten instrucciones para el uso y administración del recurso tecnológico de la Secretaría Distrital de Gobierno.

Si bien estas políticas no están siendo aplicadas en su totalidad, es importante resaltar que durante el primer semestre de 2015 un equipo de trabajo designado por la Dirección de Planeación y Sistemas de Información adelantó la revisión y ajuste de las mismas, a las nuevas necesidades y situaciones que enfrenta la entidad debido al acelerado cambio tecnológico, logrando para finales del cuarto trimestre del 2015 la formalización del "Manual de Políticas de Uso y Seguridad de la Infraestructura Tecnológica."

Sin embargo dado que falta la socialización del mismo, la información crítica o no, personal o institucional, puede ser sustraída por los usuarios en cualquier medio magnético u óptico, lo cual implica una clara vulnerabilidad del manejo de la información que podría ser crítica para la

Entidad. Esto es claramente estipulado en la Resolución mencionada y se debe aplicar tanto tecnológicamente como contractualmente a cada usuario. En este sentido, solo existe filtro cuando el usuario solicita el backup de su información al Grupo de Infraestructura Tecnológica.

Actualmente, se tiene la topología de red indicada en la figura[2], es claro que dado la cantidad de usuarios y complejidad de un Datacenter Nivel Tier 2 con características de redundancia y suplencia nivel TIER 3, y cableado estructurado 6A.

La Secretaría Distrital de Gobierno cuenta con herramientas que le permiten asegurar la red de datos y protegerla contra los diferentes tipos de ataques a los que se está expuesto, así como virus informáticos, accesos no permitidos, control de contenido, control de aplicaciones entre otros, adicionalmente estas herramientas le permiten a la Entidad optimizar los recursos informáticos con que cuenta. La red de datos se encuentra segmentada en Vlan's (Red de área local virtual), lo cual es una ventaja en la administración y cambios que puedan presentarse en la red, mejora la seguridad, mejora el rendimiento de la red, disminuye el riesgo de propagación de virus en toda la red de la Entidad, permite perfilar a los usuarios para acceder a los diferentes servicios según los permisos establecidos por las políticas de la Entidad.

En cuanto a la solución de seguridad perimetral está implementada con equipos Fortinet los cuales se encuentran implementados de la siguiente forma:

Descripción	Localidad
Dos firewall Fortinet 1500 en alta disponibilidad	Edificio Bicentenario
Un firewall Fortinet 200D	Suba
Un firewall Fortinet 200D	Engativá
Un firewall Fortinet 200D	Cárcel Distrital
Un firewall Fortinet 200D	Kennedy
Un firewall Fortinet 200D	Santa Fe
Un firewall Fortinet 200B	Puente Aranda
Un firewall Fortinet 200B	Antonio Nariño
Un firewall Fortinet 200B	Candelaria

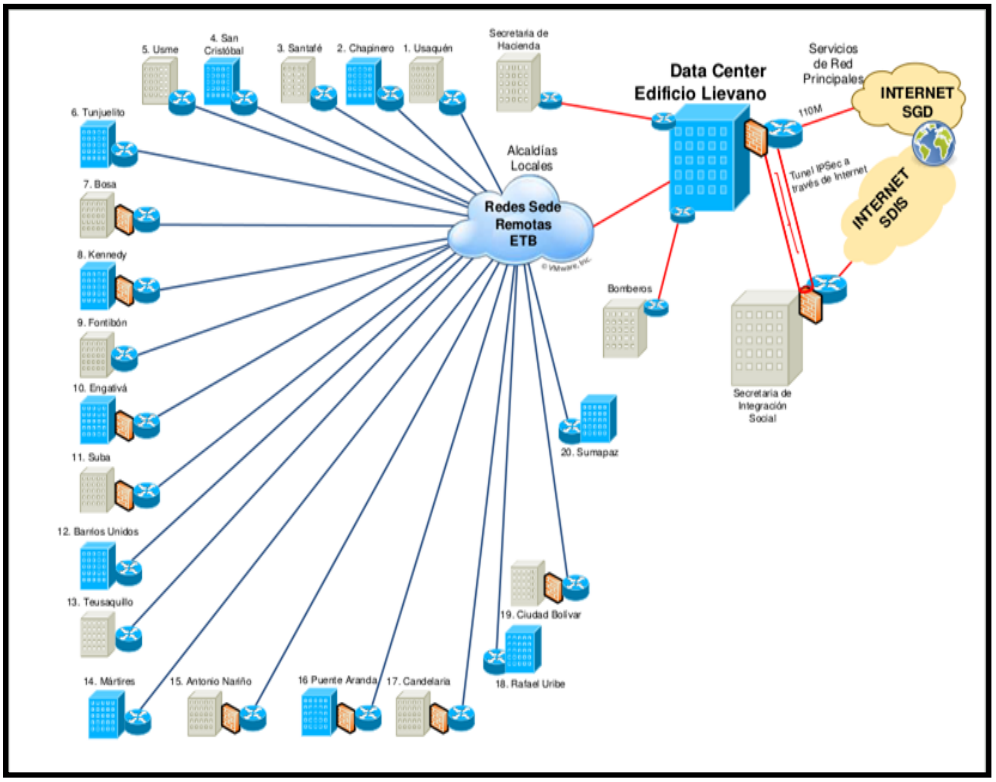
[2] *Información suministrada por el Grupo de Tecnología, perteneciente a la Dirección de Planeación y Sistemas de Información – SDG*

Un firewall Fortinet 200B	Ciudad Bolívar
Un firewall Fortinet 200B	Bosa
Un firewall Pfsense	Teusaquillo

Para el control de virus La Secretaría de Gobierno hace uso de Enterprise Security Suite de la compañía de seguridad Trend Micro para proteger los equipos de usuario final de ataques a la seguridad de la información local. Dicha solución es administrada por el grupo de infraestructura y está configurada en cada equipo host de la Secretaría Distrital de Gobierno y sus sedes anexas.

Esta solución está compuesta por los siguientes productos: Officescan (Antivirus clientes Windows), ScanMail (Antivirus Mail), InterScan, Serverprotect, consola de administración centralizada (Control Manager), Data Lost Prevention (DPL), Web Security.

La solución UTM cuenta con el módulo de Administración y Control de Contenido, con interface gráfica, permite el control de contenido basado en el catálogo y categorías establecidas por el fabricante de la solución, la cual se actualiza de manera periódica.
Existen tres grupos de usuarios definidos para el acceso a Internet:



- Usuarios Normales: Solo páginas autorizadas
- Redes Sociales: Acceso a todo menos a páginas con palabras prohibidas
- VIP: Acceso a todo.

Estos grupos deben ser revaluados a la luz de un sistema de administración que permita una mayor granularidad y que sea fácil de administrar. Se debe personalizar el mensaje que aparece al denegar el acceso a una página, pues aparece "Acceso denegado comuníquese con el administrador" y no arroja una página institucional, indicando al usuario que está violando las políticas corporativas y si cree que hay un error indicar un link o contacto.

No existen backups de usuarios de los equipos de cómputo y solo se hace sobre la información que estos coloquen sobre la unidad Z de la red (Disco Duro de 500Gb). La Secretaría Distrital de Gobierno no tiene esta cultura de proteger la información por lo que esta unidad se encuentra subutilizada. Por el contrario, el usuario puede grabar la información de su PC en un medio extraíble y retirarla de la Entidad sin autorización alguna.

A los usuarios se les asigna direccionamiento IP a través del servidor DHCP y a las conexiones inalámbricas (WI) se les asigna por DHCP asociado a la MAC del equipo. Existe un segmento de red para VoIP asociado a una VLAN del mismo enrutador (Stream PoE.[3])

La "Intranet" de la Secretaría Distrital de Gobierno se encuentra configurada con un administrador de contenidos (joomla) desactualizado, lo que quiere decir, que se mantiene un constante riesgo frente a la indisponibilidad del servicio y a una vulnerabilidad de la información interna de la entidad dado que la versión de joomla ya no se encuentra soportada por la comunidad y por ende no es posible realizar actualizaciones.

Cuando el usuario se retira antes de terminar su contrato, no se informa al Área de Tecnología de manera oportuna, lo cual genera una vulnerabilidad por un usuario que no existe y que puede haber entregado su clave a otra persona, esta situación se acentúa en las Alcaldías locales. Se deben establecer procedimientos entre las áreas implicadas para que se informe el retiro o las novedades en cuanto a personal se refiere.

No se cuenta con una documentación actualizada de la configuración de los equipos activos, ni estandarización de configuración para los mismos.

Es claro, que el esquema de seguridad informática de la Secretaría Distrital de Gobierno debe cambiar, dada la complejidad de la red de datos y que se requiere con urgencia terminar de implementar la Alta Disponibilidad, en todos los niveles, con el fin de contar con un Data Center Tier 2/3.

3 *PoE: Power Over Ethernet: Es una tecnología incorporada en los Switchs de redes LAN, mediante la cual los hilos de las conexiones LAN, proveen alimentación eléctrica a los dispositivos conectados al Switch.*

En aspectos de Seguridad de la Información, dada la complejidad mencionada, sumado a que dentro de la planta de la Secretaría Distrital de Gobierno no se cuenta con un Ingeniero de Seguridad de TI, es recomendable "tercerizar" esta administración de Seguridad Informática a una entidad especializada. En este sentido, la solución UTM[4] compuesta por los módulos IDS, IPS, Proxy, Antivirus, Antispam, Administración de Ancho de Banda tanto para el canal corporativo como para la WAN, Firewall (HW como un appliance y SW como ISA server), Administración de puertos y servicios sobre el Switch de Core para la red corporativa y Control de protocolos, puertos y servicios de acceso a internet para los usuarios, es recomendable para la SDG, contar con una solución de administración y gestión robusta.

7. DESCRIPCIÓN

7.1. ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas y terceros que laboran para la SDG, deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. Para esto, toda novedad en personal debe ser reportada por el área competente (Contratación, Recursos Humanos, etc.) a la Dirección de Planeación y Sistemas de Información

El otorgamiento de acceso a la información debe ser autorizado por el área solicitante y debe estar regulado mediante las normas y procedimientos definidos para tal fin, por el área de Tecnología.

Todos los privilegios para el uso de los Sistemas de Información de la Entidad, deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la misma.

Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas por el área implicada.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual se describe en el numeral A-8.2.1.[5]

7.2. ADMINISTRACIÓN DE CAMBIOS EN HARDWARE Y SOFTWARE DE LA RED SDG

Todo cambio como: creación, modificación de programas, pantallas, reportes configuraciones, instalaciones, etc., que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos, debe tener la facultad de aceptar o rechazar la solicitud.

---

[4] *UTM: Unified Threat Management, Administración Unificada de Amenazas. Dispositivo que controla, gestiona, administra y previene las amenazas y vulnerabilidades sobre una infraestructura informática.*

[5] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-8.2.1. Clasificación de la Informacion

Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.

Para la administración de cambios se debe efectuar el procedimiento correspondiente definido por la Dirección de Planeación y Sistemas de Información – Grupo de Infraestructura Tecnológica, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no reduzca la seguridad existente ni cree vulnerabilidades sobre el sistema o la infraestructura de red de la Entidad.

Toda la información histórica almacenada debe contar con los medios, procesos y programas capaces de manipularla sin inconvenientes, esto teniendo en cuenta la restructuración que sufren las aplicaciones y los datos a través del tiempo.

7.3. SEGURIDAD DE LA INFORMACIÓN

Los funcionarios públicos y contratistas de la Secretaría Distrital de Gobierno, son responsables de la información que manejan para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. Para ello, la Oficina de Comunicaciones debe desarrollar en conjunto con el área de Sistemas, programas de socialización y divulgación que sensibilicen a los usuarios, que la Seguridad Informática no es un tema exclusivo del área de sistemas.

En este punto, radica la oportunidad de concientizar a todos los usuarios tanto de nivel central como local, sobre el uso y protección de la información.

Cualquier tipo de información interna de la Entidad no puede ser vendida, transferida o intercambiada con terceros para ningún propósito.

Todos los datos de propiedad de la Entidad se deben clasificar dentro de las siguientes categorías: Primaria (la que proviene de fuentes externas), Secundaria (la generada por la Secretaría Distrital de Gobierno), Confidencial, Privada, Reservada o Pública.

Toda la información de la Entidad, física o en medio virtual debe ser codificada y salvaguardada de acuerdo a los lineamientos establecidos por el Proceso de Gestión y Adquisición de Recursos – componente de gestión documental.

La información como activo de la Entidad, debe ser protegida, salvaguardada y utilizada únicamente para los fines establecidos en concordancia con la función administrativa de la Secretaría Distrital de Gobierno.

7.4. SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS

El sistema de correo electrónico debe ser usado únicamente para el ejercicio de las funciones corporativas de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas o terceros.
La capacidad de almacenamiento del correo electrónico debe estar configurada de acuerdo a los roles de cada funcionario de la Entidad.[6]

La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, la entidad realizará las revisiones y/o auditorias respectivas directamente o a través de terceros.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Entidad.

Los funcionarios públicos, contratistas y personal temporal que hayan recibido aprobación para tener acceso a Internet a través de los recursos informáticos de la Entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

Para la administración del portal WEB, debe haber al menos una persona responsable en cada dependencia de la Entidad, y otra suplente, para administrar la información respectiva de su área.

El Jefe de la Dirección de Planeación y Sistemas de Información debe designar el Administrador de la página, encargado del manejo de la parte técnica de ésta.

La supervisión de la información que se maneje o publique en la página web deberá estar a cargo de un usuario principal en cada área y uno en el Grupo de Comunicaciones, y debe ser revisada regularmente para asegurar que refleje correctamente los desarrollos normativos y la evolución de las tecnologías de la información y comunicaciones.

6 ***Resolución No. 177 del 23 de Marzo de 2007*** *– Por la cual se adoptan las políticas de seguridad para el manejo de la información y la administración y uso del recurso tecnológico de la Secretaría Distrital de Gobierno.*

Se debe utilizar un mecanismo de control de flujos de documentos, como un sistema de información, que garantice la integridad, confidencialidad, autenticidad y aceptación de la información.

Todo software que comprometa la seguridad del sistema, se custodia y administra únicamente por personal autorizado.

7.5. SEGURIDAD EN RECURSOS INFORMÁTICOS

Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia de cambio de clave de los usuarios y los períodos de vigencia de las mismas, entre otras.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol administre todos los usuarios.

El control de acceso a todos los sistemas de información de la Entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos y contratistas de la Secretaría Distrital de Gobierno son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y backup, para garantizar que no sea descubierta, modificada, borrada o no recuperable.

Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad, accesibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Toda información contenida procesada o generada en los equipos de cómputo propio o colocado en cualquiera de las modalidades de arrendamiento es Propiedad de la Secretaría Distrital de Gobierno.

Si los usuarios sospechan que se produjo algún fallo a nivel de software o hardware, deben inmediatamente informar al personal de soporte, por ningún motivo el usuario debe manipular técnicamente el software o hardware asignados.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

7.6. SEGURIDAD EN COMUNICACIONES

La topología de red y direccionamiento, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.
La red de amplia cobertura geográfica (WAN) a nivel distrital debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Entidad, debe pasar a través de los sistemas de seguridad y verificación de datos, detección de ataques cibernéticos, detección de intrusos, administración de permisos de circulación y autenticación de usuarios.

Todo intercambio electrónico (pagos electrónicos) o interacción entre sistemas de información con Unidades externas deberá estar soportado con un acuerdo o documento de formalización.

7.7. SEGURIDAD PARA USUARIOS TERCEROS

Los dueños de los recursos informáticos que no sean propiedad de la Entidad y deban ser ubicados y administrados por éste, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente, debe definir un documento de acuerdo oficial entre las partes.

Los usuarios terceros tendrán acceso a los recursos informáticos, que sean estrictamente necesarios para el cumplimiento de sus actividades u obligaciones, servicios que deben ser aprobados por el jefe inmediato o coordinador. En todo, caso deberán firmar el acuerdo de buen uso de los Recursos Informáticos.

7.8. SOFTWARE UTILIZADO

Todo software que utilice la Secretaría Distrital de Gobierno debe ser adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios y contratistas de las implicaciones que tiene el instalar software ilegal en los computadores de la Secretaría Distrital de Gobierno, esta labor de divulgación debe ser constante y a cargo del área de prensa, donde se utilicen recursos como la Intranet, correo electrónico, mensajes de texto o redes sociales.

Debe existir un inventario de las licencias de software de la Secretaría Distrital de Gobierno que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

7.9. ACTUALIZACIÓN DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la Entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de cómputo (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada.

7.10. ALMACENAMIENTO Y RESPALDO

Los respaldos de información (backups) de valor o sensible debe tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.

El área dueña de la información en conjunto con la Dirección de Planeación y Sistemas de Información, definirá la estrategia a seguir para el respaldo de la información.

La información y datos de los aplicativos de misión crítica deben ser almacenados bajo un esquema estructurado de backup, que incluya almacenamiento en discos duros externos, en sitios externos a la entidad y con verificación periódica de su restauración.

Se debe utilizar una utilidad de copias de seguridad para programarlas, teniendo en cuenta la fecha, la hora, la frecuencia y el recurso de red donde se realiza la configuración.

Las copias de seguridad son programadas dependiendo la periodicidad de los cambios realizados en las aplicaciones (códigos fuentes, bases de datos, configuración del sistema).

Toda la información contable, de propiedad intelectual y de propiedad de la Entidad debe ser conservada de acuerdo con las normas de ley vigentes.

Todos los medios físicos donde la información de valor y crítica sea almacenada deben tener un control de acceso y custodia para evitar su pérdida o acceso no autorizado.

Los funcionarios públicos son responsables de los respaldos de su información en los computadores asignados, siguiendo las indicaciones técnicas dictadas por la Dirección de Planeación y Sistemas de Información y la Resolución 177 de 2007.

7.11. **CONTINGENCIA**

La Dirección de Planeación y Sistemas de Información debe contar con un plan de contingencia que permita a los servicios informáticos que se prestan en la Secretaría Distrital de Gobierno, estar disponibles en el evento de medianos o prolongados lapsos de tiempo de inoperatividad de los servidores, de las bases de datos, del servidor de seguridad y de aplicaciones, inoperatividad de los equipos de comunicación o desastres como terremoto, explosión, terrorismo, inundación etc.

7.12. **SEGURIDAD FÍSICA**

El Datacenter y los centros de cómputo intermedios (IC) deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá estar acompañada permanentemente por el personal especializado en estos lugares.

En los centros de cómputo deberán existir elementos de control de incendio, inundación y alarmas.

Los centros de cómputo deberán estar demarcados con zonas de circulación y zonas restringidas.

Los puntos de concentración de conexión (racks, cajas de paso, inspección, tableros, etc.) deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores portátiles, módems y equipos de comunicación se deben registrar al ingreso y a la salida, y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva.

Los equipos de cómputo (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no deberían estar autorizados para utilizar los recursos informáticos de la Entidad.

8. TRATAMIENTO DE VULNERABILIDADES Y MEJORES PRÁCTICAS PARA PSI (SGSI[7])

La información es un recurso que, como el resto de los activos, tiene mucho valor para la Secretaría Distrital de Gobierno y por consiguiente debe ser debidamente protegida.
Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Secretaría Distrital de Gobierno.

Es importante que las Políticas de Seguridad, sean parte de la cultura organizacional.

Las políticas de seguridad deben ser aplicadas al Recurso Humano, Datos, Software, Hardware, Instalaciones Físicas y Administración de Seguridad, entre otras, como conjunto y no de forma aislada.

Como complemento a la Resolución No. 177 de 2007 y la implementación de un SGSI, deben participar áreas como control interno, disciplinario, recursos humanos, contractual, entre otras, que generen los parámetros restrictivos y medidas que se tomarán frente al incumplimiento de la Resolución mencionada, clasificándolas como: faltas leves, intermedias, graves, etc. y sus respetivas consecuencias.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la Secretaría Distrital de Gobierno y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento las Políticas en mención.

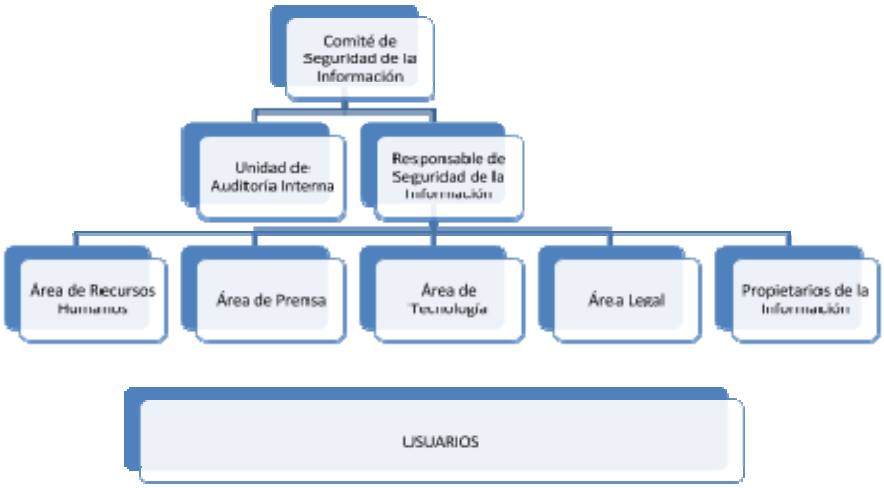
---

7 ***SGSI**: Sistema de Gestión de Seguridad de la Información, sistema de gestión que comprende la política, estructura organizativa, procedimientos, procesos y recursos necesarios para la seguridad de la información de acuerdo a la ISO 27001.* http://www.iso.org/iso/home/search.htm?qt=27001&sort=rel&type=simple&published=on

8.1. ROLES Y RESPONSABILIDAD

Las PSI deben ser conocida y cumplida por todos los funcionarios públicos, contratistas y de la Secretaría Distrital de Gobierno y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la Entidad, sea cual fuere su nivel jerárquico.

Las máximas autoridades de la Secretaría Distrital de Gobierno deben aprobar esta Política y son responsables de su implementación y sus modificaciones, por esta razón deben crearse dentro de la organización, los siguientes roles que garanticen su cumplimiento:



El **Comité de Seguridad de la Información** de la SDG, debe proponer a la alta Dirección de la Secretaría Distrital de Gobierno, para su aprobación, las acciones para cumplir con la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información:

- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes
- Tener conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área
- Acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información
- Garantizar que la seguridad sea parte del proceso de planificación de la información
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios
- Promover la difusión y apoyo a la seguridad de la información dentro de la Secretaría Distrital de Gobierno
- Coordinar el proceso de administración de la continuidad de las actividades de la Secretaría Distrital de Gobierno.

El **Responsable de Seguridad Informática** cumplirá funciones relativas a la seguridad de los sistemas de información de la Secretaría Distrital de Gobierno, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la PSI.

Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.
El **Responsable del Área de Recursos Humanos**, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan y las tareas de capacitación continua en materia de seguridad.

El **Responsable del Área de Prensa,** tendrá a su cargo la notificación de la PSI a todo el personal, de los cambios que en ella se produzcan, la implementación de los Compromisos de Confidencialidad, etc.

El **Responsable del Área de Tecnología,** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Secretaría Distrital de Gobierno. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de soluciones informáticas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El **Responsable del Área Legal,** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Secretaría Distrital de Gobierno con sus funcionarios y con terceros. Asimismo, asesorará en materia legal a la Secretaría Distrital de Gobierno, en lo que se refiere a la seguridad de la información.

Los **usuarios de la información de los sistemas,** son responsables de conocer y dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

La **Oficina de Control Interno**, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por la PSI y por las normas, procedimientos y prácticas que de ella surjan.
Aspectos Generales

Este ítem contempla una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

- ***Organización de la Seguridad:*** Orientado a administrar la seguridad de la información dentro de la Secretaría Distrital de Gobierno y establecer un marco gerencial para controlar su implementación.
- ***Clasificación y Control de Activos:*** Destinado a mantener una adecuada protección de los activos de la Secretaría Distrital de Gobierno.
- ***Seguridad del Personal:*** Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Secretaría Distrital de Gobierno o uso inadecuado de instalaciones.
- ***Seguridad Física y Ambiental:*** Destinado a impedir accesos no autorizados, daños e interferencia a las estaciones e información de la Secretaría Distrital de Gobierno.
- ***Gestión de las Comunicaciones y las Operaciones:*** Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.
- ***Control de Acceso:*** Orientado a controlar el acceso lógico a la información.
- ***Desarrollo y Mantenimiento de los Sistemas:*** Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
- ***Administración de la Continuidad del funcionamiento de la Secretaría Distrital de Gobierno:*** Orientado a contrarrestar las interrupciones del funcionamiento y proteger los procesos críticos de los efectos de fallas significativas o desastres.
- ***Cumplimiento:*** Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en las PSI, la Secretaría Distrital de Gobierno debe identificar los recursos necesarios y debe garantizar las partidas presupuestarias correspondientes para ejecutar las soluciones informáticas en aspectos de seguridad.

El Comité de Seguridad de la Información debe revisar periódicamente las PSI dados los continuos cambios tecnológicos y creación de nuevas amenazas informáticas, a efectos de mantenerla actualizada. Así mismo, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como son: cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

Sanciones Previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido (Ver 41.3.3. Sanciones Previstas por Incumplimiento)

8.2. ORGANIZACIÓN DE LA SEGURIDAD

Generalidades

Las PSI establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades del área de Tecnología de la Secretaría Distrital de Gobierno.

Por esta razón, debe tenerse en cuenta que ciertas actividades de la Secretaría Distrital de Gobierno pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos, se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

Administrar la seguridad de la información dentro de la Secretaría Distrital de Gobierno y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con entidades especializadas para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información o sistemas de información de la Secretaría Distrital de Gobierno.

Alcance

Este ítem se aplica a todos los recursos de la Secretaría Distrital de Gobierno y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

El Coordinador del Comité de Seguridad de la Información debe ser el responsable de implementar este ítem.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento de este ítem, ante la máxima autoridad de la Secretaría Distrital de Gobierno, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad Informática asistirá al personal de la Secretaría Distrital de Gobierno en materia de seguridad de la información y coordinará la interacción con entidades especializadas.

Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la Secretaría Distrital de Gobierno y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los Responsables de las Unidades Organizativas cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, debe ser responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

El Responsable del Área Legal, cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la PSI y de todas las normas, procedimientos y prácticas relacionadas.

8.3. INFRAESTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN

Comité de Seguridad de la Información

La seguridad de la información debe ser una responsabilidad de la Secretaría Distrital de Gobierno compartida por todas las áreas de Dirección, por lo cual se debe crear un Comité de Seguridad de la Información, integrado por representantes de todas las áreas mencionadas, destinado a garantizar el apoyo manifiesto de la Alta Dirección a las iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de las PSI.

Este Comité tendrá entre sus funciones:

- Revisar y proponer a la Alta Dirección de la Secretaría Distrital de Gobierno para su aprobación, las acciones de implementación de las PSI y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento, supervisar la implementación y monitoreo de los incidentes relativos a la seguridad.

- Aprobar las iniciativas más relevantes para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación Institucional.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos soluciones o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Secretaría Distrital de Gobierno.
- Coordinar el proceso de administración de la continuidad del funcionamiento de los sistemas y de la información de la Secretaría Distrital de Gobierno frente a interrupciones imprevistas (Planes de Contingencia).

8.4. ASIGNACIÓN DE RESPONSABILIDADES PARA SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información propondrá a la Dirección para su aprobación la definición y asignación de las responsabilidades.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas.

La delegación de la administración por parte de los propietarios de la información debe ser documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

8.5. PROCESO DE AUTORIZACIÓN PARA APLICATIVOS

Los nuevos aplicativos deben ser autorizados por los delegados de las Áreas Directivas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Área de Tecnología.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la Secretaría Distrital de Gobierno.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso debe ser evaluado en cada caso por el Área Informática y por el responsable del área al que se destinen los recursos.

8.6. ASESORAMIENTO ESPECIALIZADO EN SEGURIDAD DE LA INFORMACIÓN

El Responsable de Seguridad Informática debe ser el encargado de coordinar los conocimientos y las experiencias disponibles en la entidad fin de brindar ayuda en la toma de decisiones en materia de seguridad.

8.7. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de las PSI, a efectos de garantizar que las prácticas de la Secretaría Distrital de Gobierno reflejen adecuadamente sus disposiciones.

8.8. SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS

Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Secretaría Distrital de Gobierno, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- Clasificación de la información.
- Los controles aplicables a la tercera parte.
- La incidencia de este acceso en la seguridad de la información de la Secretaría Distrital de Gobierno.

En todos los contratos, cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Secretaría Distrital de Gobierno, se deben establecer los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

- Personal de mantenimiento y soporte de hardware y software.

- Limpieza, guardia de seguridad y otros servicios de soporte tercerizados.
- Pasantías y otras designaciones de corto plazo.
- Consultores e Interventores.

En ningún caso se debe otorgar acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

- Cumplimiento de las PSI de la Secretaría Distrital de Gobierno.
- Protección de los activos de la Secretaría Distrital de Gobierno, incluyendo:
  - Procedimientos para proteger los bienes de la Secretaría Distrital de Gobierno, abarcando los activos físicos, la información y el software.
  - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
  - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
  - Restricciones a la copia y divulgación de información.
- Descripción de los servicios disponibles.
- Nivel de servicio esperado y niveles de servicio aceptables.
- Permiso para la transferencia de personal cuando sea necesario.
- Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
- Existencia de Derechos de Propiedad Intelectual.
- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:
  - Métodos de acceso permitidos, control y uso de identificadores únicos como usuario y contraseñas.
  - Proceso de autorización de accesos y privilegios de usuarios.
  - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios, sus derechos y privilegios con respecto a dicho uso.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- Relación entre la Secretaría Distrital de Gobierno con contratistas y usuarios.

Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes, seguridad y/o mantenimiento de PC, etc de la Secretaría Distrital de Gobierno, deben contemplar además de los puntos especificados en el numeral 15.1.2 Tratamiento de la Seguridad dentro de los acuerdos con proveedores[8], los siguientes aspectos:

- Forma en que se cumplirán los requisitos legales aplicables.
- Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la Secretaría Distrital de Gobierno.
- Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la Secretaría Distrital de Gobierno.
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres (Contingencia).
- Niveles de seguridad física que se asignarán al equipamiento tercerizado.
- Derecho a la auditoría por parte de la Secretaría Distrital de Gobierno sobre los aspectos tercerizados en forma directa o a través de la contratación.

La Secretaría Distrital de Gobierno debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

9. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Generalidades

La Secretaría Distrital de Gobierno debe tener total control y conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

[8] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 15.1.2 Tratamiento de la Seguridad dentro de los acuerdos con proveedores.

- ***Recursos de información:*** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- ***Recursos de software:*** software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- ***Activos físicos:*** equipamiento informático (Servidores, Equipos de Almacenamiento, CPU, monitores, computadores de escritorio, computadoras portátiles, módems), equipos de comunicaciones (routers, PBX, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- ***Servicios:*** servicios informáticos y de comunicaciones, utilitarios generales (iluminación, energía eléctrica normal y regulada, voz, datos, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de indicar cómo ha de ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la entidad.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad, disponibilidad y accesibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección.
Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

Este ítem se aplica a toda la información administrada en la Secretaría Distrital de Gobierno, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Los propietarios de la información deben ser los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea ejecutado de acuerdo a lo establecido en este ítem.

9.1. INVENTARIO DE ACTIVOS

Se deben identificar los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo debe ser actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es el Responsable de cada Área Organizativa.

9.2. CLASIFICACIÓN DE LA INFORMACIÓN

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

Confidencialidad

0 – ***PÚBLICO:*** Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleada de la Secretaría Distrital de Gobierno o no.

1- ***RESERVADA - USO INTERNO:*** Información que puede ser conocida y utilizada por todos los funcionarios de la Secretaría Distrital de Gobierno y algunas Unidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad, el Sector Público Nacional o terceros.

2 - ***RESERVADA - CONFIDENCIAL:*** Información que sólo puede ser conocida y utilizada por un grupo de funcionarios, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la entidad, al Sector Público Nacional o a terceros.

3- ***RESERVADA - SECRETA:*** Información que sólo puede ser conocida y utilizada por un grupo muy reducido de funcionarios, generalmente de la alta dirección de la Secretaría Distrital de Gobierno, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros.

Integridad

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta el funcionamiento de la Secretaría Distrital de Gobierno.

1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la entidad, el Sector Público Nacional o terceros.

2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la entidad, el Sector Público Nacional o terceros.

3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la entidad, al Sector Público Nacional o a terceros.

Disponibilidad:

0- Información cuya inaccesibilidad no afecta el funcionamiento de la Secretaría Distrital de Gobierno.

1- Información cuya inaccesibilidad permanente durante un tiempo determinado podría ocasionar pérdidas significativas para la entidad, el Sector Público Nacional o terceros.

2- Información cuya inaccesibilidad permanente durante un tiempo determinado podría ocasionar pérdidas significativas a la entidad, al Sector Público Nacional o a terceros.

3- Información cuya inaccesibilidad permanente durante un tiempo determinado podría ocasionar pérdidas significativas a la entidad, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, direccionamiento de red, etc.).

Se debe asignar a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en categorías Baja, Media y Alta:

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma, identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

En adelante, en este documento, se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

10. SEGURIDAD DEL PERSONAL

Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad, disponibilidad y accesibilidad por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación laboral con la entidad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de las PSI, tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello, que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Ser explicito con las responsabilidades en materia de seguridad en la etapa del ingreso de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para cumplir las PSI de la Secretaría Distrital de Gobierno en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones relacionados con el manejo de la información de la Secretaría Distrital de Gobierno.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Alcance

Este ítem se aplica a todo el personal de la Secretaría Distrital de Gobierno, cualquiera sea su situación laboral, y al personal externo que efectúe tareas para la entidad.

Responsabilidad

El Responsable de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los funcionarios, informará a todo el personal que ingresa, sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto a la Política.

El Responsable de Seguridad Informática tendrá a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información.

El Comité de Seguridad de la Información debe ser responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participará en la construcción del Compromiso de Confidencialidad a firmar por los funcionarios, contratistas y terceros que desarrollen funciones en la entidad, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de las PSI y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal de la Secretaría Distrital de Gobierno debe ser responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

10.1. SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y LA ASIGNACIÓN DE RECURSOS

Incorporación de la Seguridad en los Puestos de Trabajo

Las funciones y responsabilidades en materia de seguridad deben ser incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación, el mantenimiento de las PSI, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos o la ejecución de procesos o actividades de seguridad determinadas.

Control y Política del Personal

La Secretaría Distrital de Gobierno realiza los controles previos de verificación del personal en el momento en que se solicita el puesto. Estos controles incluyen antecedentes disciplinarios, procuraduría, personería y judiciales y todos los aspectos que a tal efecto requiere a la entidad.

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas de Seguridad Informática.

Todos los usuarios de bienes y servicios informáticos de la Secretaría Distrital de Gobierno deben firmar la aceptación del Acuerdo de confidencialidad y uso adecuado de los recursos informáticos y de información de la Secretaría Distrital de Gobierno.

Todo empleado llámese funcionario, contratista o terceros nuevo de la Secretaría Distrital de Gobierno deberá de contar con la inducción sobre las Políticas de Seguridad Informática, a través de la Oficina Asesora de Planeación, Recursos Humanos y Jurídica, donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento

10.2. ACUERDO DE CONFIDENCIALIDAD

Como parte de sus términos y condiciones iniciales de empleo, los funcionarios de la Entidad, cualquiera sea su situación laboral, deben firmar un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Secretaría Distrital de

Gobierno. La copia firmada del Acuerdo deberá ser resguardada en forma segura por el Área de Recursos Humanos.

Asimismo, mediante el Acuerdo de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de cumplir con el Numeral 10.2 Acuerdos de Confidencialidad o de no divulgación– No expectativa de privacidad[9].

Se debe desarrollar un procedimiento para la suscripción del Acuerdo de Confidencialidad, donde se incluirán aspectos como:

- Suscripción inicial del Acuerdo por parte de la totalidad del personal.
- Revisión del contenido del Acuerdo periódicamente (no mayor a 1 año).
- Método de resuscripción en caso de modificación del texto del Acuerdo.

10.3. TÉRMINOS Y CONDICIONES DE EMPLEO

Los términos y condiciones de empleo establecerán la responsabilidad del funcionario, contratista o tercero en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede principal de la Secretaría Distrital de Gobierno y del horario normal de trabajo, en aras de tener acceso remoto y establecer sus condiciones.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

10.4. CAPACITACIÓN DEL USUARIO

Formación y Capacitación en Temas de Seguridad de la Información

Todos los servidores públicos de la Secretaría Distrital de Gobierno y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la entidad, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Secretaría Distrital de Gobierno.

9 *6.1. No expectativa de privacidad y 6.2. Renuncia a Derechos de Privacidad, "Los usuarios entienden y aceptan que la Secretaría Distrital de Gobierno puede utilizar procedimientos y recursos manuales o automáticos para monitorear la utilización de sus Recursos Tecnológicos".*

Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos debe ser el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada tiempo determinado (no mayor a seis meses) se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado de ese momento.

Las siguientes áreas deben ser encargadas de producir el material de capacitación

Áreas Responsables del Material de Capacitación

El personal que ingrese a la Secretaría Distrital de Gobierno recibirá el Manual de Políticas y Estándares de Seguridad Informática para Usuarios, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se habilitarán los medios técnicos necesarios para comunicar y socializar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

11. RESPUESTA A INCIDENTES Y ANOMALÍAS EN SEGURIDAD

Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a seguridad, deben ser comunicados a través de canales apropiados tan pronto como sea posible.

Se debe establecer un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tenido conocimiento. Este asignará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su seguimiento. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Sin perjuicio de informar a otras Entidades de competencia, el Responsable de Seguridad Informática, comunicará a la Jefatura de la Oficina Asesora de Planeación, todo incidente o violación de la seguridad, que involucre recursos informáticos.

Todos los funcionarios y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tenido conocimiento de su ocurrencia.

Comunicación de Debilidades en Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento, directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

Se prohíbe a los usuarios, realizar pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

Comunicación de Fallas del Software

Se deben establecer procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

- Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- Alertar inmediatamente al Responsable de Seguridad Informática.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación debe ser realizada por personal especializado y adecuadamente habilitado.

Base de conocimiento de Incidentes

Se debe definir un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto debe ser evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias y convencionales que rigen a los funcionarios de la Administración Publica Nacional, para los funcionarios que violen la Política, Normas y Procedimientos de Seguridad de la Secretaría Distrital de Gobierno (6.11 Cumplimiento).

12. SEGURIDAD FÍSICA Y AMBIENTAL

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y al funcionamiento de la Secretaría Distrital de Gobierno. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la Secretaría Distrital de Gobierno, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. En lo posible, deben contemplarse tanto los riesgos en las instalaciones de la Secretaría Distrital de Gobierno como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas de la Secretaría Distrital de Gobierno. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello, que el transporte y la disposición final, presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la Secretaría Distrital de Gobierno.

Proteger la infraestructura tecnológica de procesamiento de información crítica de la Secretaría Distrital de Gobierno, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo,

contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento de la infraestructura tecnológica informático que alberga la información de la Secretaría Distrital de Gobierno.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Secretaría Distrital de Gobierno: instalaciones, equipamiento, cableado, archivos, medios de almacenamiento, etc.

Responsabilidad

El Responsable de Seguridad Informática definirá junto con el área de Tecnología y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

El Área de Tecnología, asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento de la infraestructura tecnológica informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la Secretaría Distrital de Gobierno.

Los Responsables de las áreas Organizativas, definirán los niveles de acceso físico del personal de la Secretaría Distrital de Gobierno a las áreas restringidas bajo su responsabilidad.

La Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.
Todo el personal de la Secretaría Distrital de Gobierno es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

12.1. PERÍMETRO DE SEGURIDAD FÍSICA

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de los sitios críticos de almacenamiento de datos y procesamiento de información.

La Secretaría Distrital de Gobierno utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera, estarán definidas por la Oficina Asesora de Planeación con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

Se deben considerar e implementar los siguientes lineamientos y controles, según corresponda:

- Definir y documentar claramente el perímetro de seguridad.
- Ubicar las instalaciones de procesamiento de información (Datacenter) dentro del perímetro de un edificio o área de construcción físicamente sólida, por ej: no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción.
  Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, alarmas, controles biométricos, cerraduras, etc.
- Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
- Identificar claramente todas las puertas de incendio de un perímetro de seguridad. El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:
  - Identificación del Edificio y Área.
  - Principales elementos a proteger.
  - Medidas de protección física.

12.1.1. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, lo que debe ser determinado por el Responsable de Seguridad Informática junto con el área de Tecnología, a fin de permitir el acceso sólo al personal autorizado.

Estos controles de acceso físico deben tener, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso justificando propósitos específicos y autorizados e informando al visitante en el momento de ingreso, sobre los requerimientos de seguridad del área y los procedimientos de emergencia. (bitácora de registro de ingreso al Datacenter.)

- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.

- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

- Revisar y actualizar cada tiempo determinado (no mayor a 6 meses), los derechos de acceso a las áreas protegidas, los que debe ser documentados y firmados por el Responsable del área organizacional de la que dependa.

- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Protección de Oficinas, cuartos de equipos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta e riesgo o posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo y en lo posible se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la Secretaría Distrital de Gobierno:

- Datacenter Principal
- Centros de Cableado de Piso
- Todas las áreas donde se almacene o procese información crítica de la Entidad.

Se establecen las siguientes medidas de protección para áreas protegidas:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

- Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información debe ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- Ubicar las funciones y la infraestructura tecnológica de soporte, por ejemplo: impresoras, fotocopiadoras, scanners, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.
- Agregar protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
- Implementar mecanismos de control para la detección de intrusos:
  Los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
- Separar las instalaciones de procesamiento de información administradas por el Secretaría Distrital de Gobierno de aquellas administradas por terceros.
- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
- Almacenar los materiales peligrosos o combustibles en lugares seguros, a una distancia prudencial de las áreas protegidas de la Secretaría Distrital de Gobierno. Los suministros, como implementos de escritorio, no debe ser trasladados, ubicados o almacenados en las áreas protegidas.
- Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

12.1.2. Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
- Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, debe ser otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

- Instalar barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad y que están ubicadas dentro del mismo perímetro de seguridad.
- Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de la Oficina Asesora de Planeación y el Responsable de Seguridad Informática.
- Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

12.1.3. Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento debe ser ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- Ubicar la infraestructura tecnológica en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
- Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:
  - Robo o hurto
  - Incendio
  - Explosivos
  - Humo
  - Inundaciones o filtraciones de agua (o falta de suministro)
  - Polvo
  - Vibraciones
  - Efectos químicos
  - Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)
  - Radiación electromagnética
  - Derrumbes

- Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada tiempo determinado (no mayor a seis meses).
- Considerar asimismo el impacto de las amenazas citadas que tengan lugar en zonas próximas a la sede de la Secretaría Distrital de Gobierno.

13. SUMINISTROS DE ENERGÍA

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

- Contar con un suministro de energía ininterrumpido (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua de los dispositivos que soportan las operaciones críticas de la Secretaría Distrital de Gobierno. La determinación de dichas operaciones críticas, debe ser el resultado del análisis de impacto realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Las UPS deben ser inspeccionadas y probadas periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

- Instalar una planta eléctrica para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes deben ser abastecidos de energía alternativa. Dicho análisis debe ser realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que la planta eléctrica pueda funcionar por un período prolongado. Cuando el encendido de la Planta Eléctrica no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. La Planta debe ser inspeccionada y probada periódicamente para asegurar que funcionen según lo previsto.

- Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las áreas donde se encuentra la infraestructura tecnológica, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en el edificio y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

14. SEGURIDAD DEL CABLEADO

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra intercepción o daño, mediante las siguientes acciones:

- Cumplir con los requisitos, normas y estándares técnicos vigentes.

- Utilizar cableado embebido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.

- Proteger el cableado de red contra intercepción no autorizada o daño mediante controles como: el uso de conductos o evitando trayectos que atraviesen áreas públicas.

- Separar los cables de energía normal y regulada, de los cables de comunicaciones para evitar interferencias.

- Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

- Para los sistemas sensibles o críticos, se implementarán los siguientes controles adicionales:

    - Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
    - Utilizar rutas o medios de transmisión alternativos.

15. MANTENIMIENTO DE EQUIPOS

Se realizará el mantenimiento de la infraestructura tecnológica para asegurar su disponibilidad, accesibilidad e integridad permanentes. Para ello se debe considerar:

- Someter la infraestructura tecnológica a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal de la Oficina Asesora de Planeación. El área de Tecnología mantendrá un listado actualizado de la infraestructura tecnológica con el detalle de la frecuencia en que se realizará el mantenimiento preventivo (Elaborar HV de Equipos con Servicios Prestados, esta actividad debe ser controlada en lo posible por la mesa de ayuda).

- Establecer que sólo el personal de soporte autorizado puede brindar mantenimiento y llevar a cabo reparaciones en la infraestructura tecnológica.

- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

- Registrar el retiro de equipamiento de la sede de la Secretaría Distrital de Gobierno para su mantenimiento.

- Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

16. SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Secretaría Distrital de Gobierno, debe ser autorizado por la Oficina Asesora de Planeación. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma.

La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Secretaría Distrital de Gobierno para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante, respecto al cuidado de los dispositivos. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger la infraestructura tecnológica fuera del ámbito de la Secretaría Distrital de Gobierno, cuando sea conveniente.

16.1. DESAFECTACIÓN O REUTILIZACIÓN SEGURA DE LOS EQUIPOS.

La información puede verse comprometida por una desafectación o una reutilización descuidada de la infraestructura tecnológica. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, debe ser físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

17. POLÍTICAS DE ESCRITORIOS Y PANTALLAS LIMPIAS.

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Guardar bajo llave la información sensible o crítica de la Secretaría Distrital de Gobierno, preferiblemente en una caja fuerte o gabinete a prueba de incendios, cuando no está en uso, especialmente cuando no hay personal en la oficina.
- Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso, por ej: la utilización de protectores de pantalla con contraseña o bloqueo automático por inactividad.
- Bloquear las fotocopiadoras o protegerlas de alguna manera del uso no autorizado, fuera del horario normal de trabajo.
- Retirar inmediatamente la información sensible o confidencial, una vez impresa.

Retiro de los Bienes

El equipamiento, la información y el software no deben ser retirados de las sedes de la Secretaría Distrital de Gobierno sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Secretaría Distrital de Gobierno.

18. GESTIÓN DE COMUNICACIONES Y FUNCIONAMIENTO DE RED

Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Se deben separar los ambientes de desarrollo, prueba y producción de los sistemas normales de la Secretaría Distrital de Gobierno, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre si, tanto dentro de la Secretaría Distrital de Gobierno como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad, disponibilidad y accesibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información de la Secretaría Distrital de Gobierno.

Responsabilidad

El Responsable de Seguridad Informática tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para las aplicaciones de Gobierno Electrónico.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico de la Secretaría Distrital de Gobierno.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la Secretaría Distrital de Gobierno.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable del Área de Tecnología tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.

- Garantizar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de respaldo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos externos, tapes, USBs, celulares e informes impresos y para la eliminación segura de los mismos.
- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El Responsable de Seguridad Informática junto con el Responsable del Área de Tecnología y el Responsable del Área Legal de la Secretaría Distrital de Gobierno, evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad Informática y el Responsable del Área de Tecnología, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posible segregar.

Asimismo, revisará los registros de actividades del personal operativo.

19. PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS

Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en este ítem y sus cambios deben ser autorizados por el Responsable de Seguridad Informática.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- Procesamiento y manejo de la información.
- Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- Restricciones en el uso de utilitarios del sistema.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se debe preparar adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

- Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- Instalación y mantenimiento de las plataformas de procesamiento.
- Monitoreo del procesamiento y las comunicaciones.
- Inicio y finalización de la ejecución de los sistemas.
- Programación y ejecución de procesos.
- Gestión de servicios.
- Resguardo de información.
- Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- Remplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
- Uso del correo electrónico.

19.1. CONTROL DE CAMBIOS EN LAS OPERACIONES

Se deben definir procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad Informática debe controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área de Tecnología debe evaluar el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se debe retener un registro de auditoría, que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios deben contemplar los siguientes puntos:

- Identificación y registro de cambios significativos.
- Evaluación del posible impacto de dichos cambios.
- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambio.
- Prueba del nuevo escenario.
- Comunicación de detalles de cambios a todas las personas pertinentes.
- Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

19.2. **PROCEDIMIENTOS DE MANEJO DE INCIDENTES**

Se deben establecer funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad (Ver también 16..1 - Gestión de Incidentes y mejoras en la Seguridad de la Información). Se deben considerar los siguientes ítems:

- Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo:
  - Fallas operativas
  - Código malicioso
  - Intrusiones
  - Fraude informático
  - Error humano
  - Catástrofes naturales

- Comunicar los incidentes a través de canales apropiados, tan pronto como sea posible, de acuerdo a lo indicado en el numeral A-16.1 – "Gestión de Incidentes y mejoras en la Seguridad de la Información"[10].

- Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales, diseñados para recuperar sistemas y servicios tan pronto como sea posible):

  - Definición de las primeras medidas a implementar
  - Análisis e identificación de la causa del incidente.

[10] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-16.1 – "Gestión de Incidentes y mejoras en la Seguridad de la Información".

- Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
- Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
- Notificación de la acción a la autoridad o áreas pertinentes de ser necesario.

- Registrar pistas de auditoría y evidencia similar para:
  - Análisis de problemas internos.
  - Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial

- Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
  - Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
  - Documentación de todas las acciones de emergencia emprendidas en forma detallada.
  - Comunicación de las acciones de emergencia al titular del área organizacional y revisión de su cumplimiento.
  - Verificación de la integridad de los controles y sistemas de la Secretaría Distrital de Gobierno en un tiempo mínimo.

De ser requerido, se debe solicitar la participación del Responsable del Área Legal de la Secretaría Distrital de Gobierno en el tratamiento de incidentes de seguridad ocurridos.

19.3. **SEPARACIÓN DE FUNCIONES**

Se debe separar la gestión u operación de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas, o mal uso de la información o los servicios, por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se puede cumplir, se deben implementar controles como:

- Monitoreo de las actividades.
- Registros de auditoría y control periódico de los mismos.
- Supervisión por parte de la Oficina de Control Interno o en su defecto quien sea propuesto a tal efecto.

Se asegurará la independencia de las funciones de auditoría de seguridad, teniendo especial cuidado para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

- Separar actividades que requieren complicidad para defraudar, por ej: información sensible y crítica que deba ser compartida entre diversas personas.
- Diseñar controles, si existe peligro de complicidad, de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de riesgo por vulnerabilidades en la información.

Separación entre el Área de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y producción, siempre que sea posible, deben estar separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se deben tener en cuenta los siguientes controles:

- Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
- Separar las actividades de desarrollo y prueba, en entornos diferentes.
- Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
- Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
- Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles indicados en el punto 19.3 - Separación de Funciones.

20. PLANIFICACIÓN Y APROBACIÓN DE SISTEMAS

Planificación de la Capacidad

El Área de Tecnología, debe efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello, tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información de la Secretaría Distrital de Gobierno para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas que puedan identificar y evitar potenciales cuellos

de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento y puedan planificar una adecuada acción correctiva.

Aprobación del Sistema

Los responsables del Área de Tecnología y de Seguridad Informática, deben sugerir criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

- Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
- Garantizar la recuperación ante errores.
- Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
- Garantizar la implementación de controles de seguridad.
- Diseñar planes de continuidad para las actividades de la Secretaría Distrital de Gobierno.
- Asegurar que la instalación del nuevo sistema, no afecte negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
- Considerar el efecto que tiene el nuevo sistema en la seguridad global de la infraestructura tecnológica de la Secretaría Distrital de Gobierno.
- Realizar el plan de entrenamiento en la operación y/o uso de los nuevos sistemas.

21. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

El Responsable de Seguridad Informática, debe definir controles de detección y prevención para la protección contra software malicioso. El Área de Tecnología, implementará dichos controles.

El Responsable de Seguridad Informática debe desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

- Prohibir el uso de software no autorizado por la Entidad (Ver 18.1.2. Derecho de Propiedad Intelectual).
- Diseñar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
- Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida preventiva y rutinaria.

- Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles. En lo posible, probar dichas actualizaciones en un entorno de prueba previamente, si es que constituyen cambios críticos a los sistemas).
- Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Secretaría Distrital de Gobierno, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
- Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

21.1. **MANTENIMIENTO**

Resguardo de la Información

Los Responsable del Área de Tecnología y de Seguridad Informática, junto con los Propietarios de Información, deben determinar los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información y contingencia.

El Responsable del Área de Tecnología debe disponer y controlar la realización de dichas copias, así como la prueba periódica de su restauración. Para esto, se debe contar con instalaciones de resguardo que garanticen la disponibilidad y accesibilidad de toda la información y del software crítico de la Secretaría Distrital de Gobierno. Dichos sistemas, deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la Secretaría Distrital de Gobierno.

Se deben definir procedimientos para el resguardo de la información, que deben considerar los siguientes puntos:

- Definir un esquema de rotulación de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- Establecer un esquema de remplazo de los medios de almacenamiento de las copias de resguardo, una vez concluya la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados. (Ver 8.3. Manejo de Medios).
- Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal.

- Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la Entidad. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad (Ver 8.2 Clasificación de la información) y requisitos legales a los que se encuentre sujeta.
- Asignar a la información de resguardo, un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
- Probar periódicamente los medios de almacenamiento.
- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones del punto 8.1 Responsabilidad por los Activos y 12.4.3 Protección de la información de registro de la Secretaría Distrital de Gobierno.

21.2. **REGISTRO DE ACTIVIDADES DEL PERSONAL OPERATIVO**

El Responsable del Área de Tecnología debe asegurar el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

- Tiempos de inicio y cierre del sistema.
- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
- Ejecución de operaciones críticas
- Cambios a información crítica

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información deberá contrastar los registros de actividades del personal operativo con relación a los procedimientos operativos.

Registro de Fallas

El Responsable del Área de Tecnología, debe desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, incluyendo Reportes de Gestión Elaborados por el Área de Soporte. La MESA de Ayuda debe Garantizar la Gestión de la Resolución de Incidentes.

- Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
- Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
- Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

22. ADMINISTRACIÓN DE LA RED

El Responsable de Seguridad Informática debe definir controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Secretaría Distrital de Gobierno, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración de la infraestructura tecnológica remota, incluyendo los equipos en las áreas usuarias, la que debe ser llevada a cabo por el responsable establecido en el punto 6.1.1. Roles y Responsabilidades para la Seguridad de la Información.

- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad y accesibilidad de los servicios de red y computadoras conectadas.

- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura tecnológica.

El Área de Tecnología implementará dichos controles.

23. ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

El Responsable del Área de Tecnología, con la asistencia del Responsable de Seguridad Informática, debe implementar procedimientos para la administración de medios informáticos removibles, como memorias USB, cintas, discos Externos, CDs, DVDs e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al capítulo 9– Control de Accesos.

Se deben considerar las siguientes acciones para la implementación de los procedimientos:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Secretaría Distrital de Gobierno. (Ver 11.2.7 Disposición segura o reutilización de Equipos).
- Requerir autorización para retirar cualquier medio de la Secretaría Distrital de Gobierno y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

- Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización, de acuerdo con el capítulo A-8. Gestión de Activos[11].

Eliminación de Medios de Información

Los responsables del Área de Tecnología y de Seguridad Informática, deben definir procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

- Documentos en papel.
- Voces u otras grabaciones.
- Papel carbónico.
- Informes de salida.
- Cintas de impresora de un solo uso.
- Cintas magnéticas.
- Medios de almacenamiento óptico (CDs, DVDs, USBs, todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
- Listados de programas.
- Datos de prueba.
- Documentación del sistema.

Procedimientos de Manejo de la Información

Se deben definir procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida en el capítulo A-8. Gestión de Activos[12].

En los procedimientos se deben contemplarán las siguientes acciones:

- Incluir en la protección: documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, y cualquier otro ítem potencialmente sensible.
- Restringir el acceso solo al personal debidamente autorizado
- Mantener un registro formal de los receptores autorizados de datos

[11] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-8. Gestión de Activos.
[12] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-8. Gestión de Activos.

- Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se validan las salidas.
- Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se deben considerar los siguientes puntos para su protección:

- Almacenar la documentación del sistema en forma segura.
- Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso debe ser autorizado por el Propietario de la Información relativa al sistema.

24. INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE

Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre entidades para el intercambio de información y software, se debe especificar el grado de sensibilidad de la información de la Secretaría Distrital de Gobierno involucrada y las consideraciones de seguridad sobre la misma. Se deben tener en cuenta los siguientes aspectos:

- Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- Procedimientos de notificación de emisión, transmisión, envío y recepción.
- Normas técnicas para el empaquetado y la transmisión.
- Pautas para la identificación del prestador del servicio de correo o transporte de datos.
- Responsabilidades y obligaciones en caso de pérdida de datos.
- Uso de un sistema convenido para el rotulado de información clasificada o entidades certificadoras, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
- Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- Normas técnicas para la grabación, uso y lectura de la información y del software.
- Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

- La utilización de medios de transporte o servicios de mensajería confiables de acuerdo a la criticidad de la información a transmitir.
- Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
- La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:

    - Uso de recipientes cerrados.
    - Entrega en mano.
    - Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
    - En casos excepcionales, división de la información a enviar en más de una entrega y envío por diferentes rutas.

25. SEGURIDAD DEL GOBIERNO ELECTRÓNICO

El Responsable de Seguridad Informática, verificará que los procedimientos de aprobación de Software en el punto A- 14.2 Seguridad en los procesos de desarrollo y de soporte[13] incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

- ***Autenticación:*** Nivel de confianza recíproca suficiente sobre la identificación del usuario y la entidad.
- ***Autorización:*** Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar (física o digitalmente) documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica (entidades certificadoras).
- ***Procesos de oferta y contratación pública:*** Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
- ***Trámites en línea:*** Confidencialidad, integridad y no repudio de los datos suministrados y confirmación de recepción.
- ***Verificación:*** Grado de verificación apropiado para confirmar la información suministrada por los usuarios.
- ***Cierre de la transacción:*** Forma de interacción más adecuada para evitar fraudes.
- ***Protección a la duplicación:*** Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
- ***No repudio:*** Manera de evitar que la parte emisora o receptora que haya enviado o recibido información, alegue que no la envió o recibió.

[13] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 14.2 Seguridad en los procesos de desarrollo y de soporte.

- ***Responsabilidad:*** Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Las consideraciones mencionadas se implementarán mediante la aplicación de las técnicas criptográficas enumeradas en el punto 10 Controles Criptográficos y tomando en cuenta el cumplimiento de los requisitos legales emanados de toda la normativa vigente. Se deben dar a conocer a los usuarios, los términos y condiciones aplicables.

25.1. SEGURIDAD DEL CORREO ELECTRÓNICO

Riesgos de Seguridad

Se deben implementar controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

- La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
- La posible interceptación y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
- Las posibles vulnerabilidades a errores, por ejemplo, escritura incorrecta de la dirección o dirección errónea, y la confiabilidad, disponibilidad y accesibilidad general del servicio.
- La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
- El impacto de un cambio en el medio de comunicación en los procesos de la Secretaría Distrital de Gobierno.
- Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación (Ley 527 de 1999).
- Las implicaciones y riesgos de publicar al exterior, listados de personal, accesibles al público.
- El acceso de usuarios remotos a las cuentas de correo electrónico.
- El uso inadecuado por parte del personal.

Política de Correo Electrónico

Los Responsables de Seguridad Informática y del Área de Tecnología deben definir y documentar normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

- Protección contra ataques al correo electrónico, por ejemplo virus, interceptación, fishing, etc.
- Protección de archivos adjuntos de correo electrónico incluyendo los comprimidos.
- Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver A- 10.1 Controles Criptográficos).

- Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio o casos judiciales.
- Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
- Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
- Definición de los alcances, deberes y derechos del uso del correo electrónico, por parte del personal de la Secretaría Distrital de Gobierno.
- Potestad de la Secretaría Distrital de Gobierno para auditar los mensajes recibidos o emitidos por los servidores de la Secretaría Distrital de Gobierno, lo cual debe estar en el Compromiso de Confidencialidad (Numeral A 13.2.4 Acuerdos de confidencialidad o de no divulgación[14])

Estos dos últimos puntos, deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los funcionarios hacer uso indebido o con fines particulares del patrimonio estatal, sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento. (8.1.3 - Uso aceptable de los activos).

Entender al correo electrónico como una herramienta más de trabajo provista al empleado, con el fin de ser utilizada conforme el uso al cual está destinado. En este sentido, se faculta a la entidad a implementar los controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, debe ser informada claramente a todos los usuarios, dentro del marco de la Resolución 177 de 2007, así:

- Cuál es el uso que la entidad espera que los funcionarios hagan del correo electrónico provisto por la entidad; e
- Informar que todos los mensajes pueden ser objeto de control y monitoreo.

Seguridad de los Sistemas Electrónicos de Oficina

Se deben controlar los mecanismos de distribución y difusión tales como documentos, computadoras, portátiles, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, multifuncionales, etc.

Al interconectar dichos medios, se considerarán las implicaciones en lo que respecta a la seguridad y a las actividades propias de la Secretaría Distrital de Gobierno, incluyendo:

[14] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A - 13.2.4 Acuerdos de confidencialidad o de no divulgación.

- Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, las impresiones no retiradas, la apertura o distribución del correo.
- Procedimientos y controles apropiados para administrar la distribución de información, por ej: el uso de boletines electrónicos institucionales.
- Exclusión de categorías de información sensible de la Secretaría Distrital de Gobierno, cuando el sistema no brinde un adecuado nivel de protección.
- Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por Ej: aquellas que trabajan en proyectos sensibles o confidenciales.
- Categorías de personal, contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
- Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
- Identificación de la posición o categoría de los usuarios, por ejemplo funcionarios de la Secretaría Distrital de Gobierno o contratistas, en directorios accesibles por otros usuarios.
- Retención y resguardo de la información almacenada en el sistema.

25.2. **SISTEMAS DE ACCESO PÚBLICO**

Se deben tomar las precauciones necesarias para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación de la Secretaría Distrital de Gobierno que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica.

Se debe implementar un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciendo en todos los casos, los encargados de dicha aprobación.

Todos los sistemas de acceso público deberán prever que:

- La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley Colombiana de Protección de Datos Personales.
- La información sensible sea protegida durante el proceso de recolección y su almacenamiento.
- El acceso al sistema de publicación, no permita el acceso accidental a las redes a las cuales se conecta el mismo.
- Se registre al responsable de la publicación de información en sistemas de acceso público.
- La información se publique teniendo en cuenta las normas establecidas al respecto.
- Se garantice la validez y vigencia de la información publicada.

Otras Formas de Intercambio de Información

Se deben implementar normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, digital, impresa y vídeo, contemplando las siguientes acciones:

- Concientizar al personal sobre la toma de precauciones, por ejemplo no revelar información sensible, para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por:
  - Personas cercanas, en especial al utilizar teléfonos móviles.
  - Terceros que tengan acceso a la comunicación mediante la Intervención (chuzadas) de la línea telefónica, y otras formas de escucha ocultas, a través del acceso físico al aparato o a la línea telefónica, o mediante equipos de barrido de frecuencias al utilizar teléfonos móviles análogos.
  - Terceros en el lado receptor.
- Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.
- No dejar mensajes en contestadores automáticos sin clave, puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de marcado.

25.3. CONTROL DE ACCESOS

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información, es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad de los recursos informáticos.

Objetivos

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red de la Secretaría Distrital de Gobierno y otras redes públicas o privadas.

Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utilizan dispositivos móviles e instalaciones de trabajo remoto.

Alcance

Se aplica a todas las formas de acceso de aquellos a quienes se les hayan otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la Secretaría Distrital de Gobierno, cualquiera sea la función que desempeñe.
Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El Responsable de Seguridad Informática estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de dispositivos móviles, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios. Se deben elaborar Procedimientos, deberes y derechos para la Navegación en internet.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.

- Analizar y sugerir medidas a ser implementadas para optimizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios y contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, administración de puertos, segmentación de redes, control de conexiones a la red, control de enrutamiento de red, etc.
- Concientizar y socializar los usuarios, sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:

    - Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
    - Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.

- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- Definir un cronograma de depuración de registros y usuarios de auditoría en línea.

Los Propietarios de la Información junto con la Oficina de Control Interno, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los Responsables de las Unidades Organizativas, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable del Área de Tecnología cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de "enrutadores" o gateways adecuados para segmentar la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de enrutamiento de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las Áreas de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware, tokens, etc).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operación.
- Analizar las medidas a ser implementadas para optimizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

25.3.1. Requerimientos para el Control de Acceso

La Secretaría Distrital de Gobierno establecerá, mantendrá y actualizará medidas de control de acceso a nivel de red, instalaciones, sistemas operativos, bases de datos y aplicaciones, los controles deben estar soportados por una cultura de seguridad en la entidad y limitar el acceso de los usuarios hacia los activos de información al mínimo requerido (Principio de Mínimo privilegio) para la realización de su trabajo, de acuerdo con el tratamiento correspondiente al nivel de clasificación de cada activo. Además, deben permitir identificar de manera inequívoca cada usuario y hacer seguimiento de las actividades que éste realiza.

La Secretaría Distrital de Gobierno proporcionará a los funcionarios y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes, access point, que no sean autorizados por la Dirección de Planeación y Sistemas.

Solo usuarios designados por el Área de Información y Sistemas estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones la Secretaría Distrital de Gobierno.

La Secretaría Distrital de Gobierno suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

Todo trabajo que utilice los servidores de la Secretaría Distrital de Gobierno con información de la entidad, sus funcionarios o contratistas, se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del área de sistemas.

Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la Secretaría Distrital de Gobierno de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

Los usuarios al terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no esté en uso.

Las claves o contraseñas deben poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc. Las claves no deberán ser regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

25.3.2. Política de Control de Accesos

En la aplicación de controles de acceso, se deben contemplar los siguientes aspectos:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.

- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

25.3.3. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

- Indicar expresamente si las reglas son obligatorias u optativas
- Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".
- Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario (Ver A- 8. Gestión de Activos[15]).
- Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
- Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

25.3.4. Administración de Accesos de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Registro de Usuarios

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo usuario. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar y debido a razones operativas.
- Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.

[15] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-8. Gestión de Activos.

- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Secretaría Distrital de Gobierno.
- Entregar a los usuarios un detalle escrito de sus derechos de acceso. (Actas de Entrega de Servicio con responsabilidades de uso)
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Secretaría Distrital de Gobierno o sufrieron la pérdida/robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de:
  - cancelar identificadores y cuentas de usuario redundantes
  - inhabilitar cuentas inactivas por más de un periodo determinado (no mayor a 60 días)
  - eliminar cuentas inactivas por más de un periodo determinado (no mayor a 120 días)
- En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o terceros, que prestan un servicio intentan accesos no autorizados.

25.3.5. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ej: sistema operativo, de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados.

Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

- Establecer un período de vigencia para el mantenimiento de los privilegios, con base en la utilización que se le dará a los mismos, luego del cual los mismos deben ser revocados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios a los usuarios.

Los Propietarios de Información deben ser los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual debe ser supervisado por el Responsable de Seguridad Informática.

25.3.6. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración puede estar incluida en el Compromiso de Confidencialidad o el Acta de Entrega de Servicio o equipo.
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- Generar contraseñas provisionales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- Utilizar otras tecnologías de autenticación y autorización de usuarios, como puede ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (token), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad Informática conjuntamente con el Responsable del área de Tecnología y el Propietario de la Información lo determine necesario o lo justifique.
- Configurar los sistemas de tal manera que:
  - las contraseñas tengan determinada cantidad de caracteres (no menor a 8), incluyendo números, letras y caracteres especiales.
  - suspendan o bloqueen permanentemente al usuario después de una cantidad determinada de intentos (no mayor a 3) de tratar con una contraseña incorrecta. Deberá solicitar la rehabilitación al área de Tecnología,
  - solicitar el cambio de la contraseña cada determinado lapso de tiempo (no mayor a 60 días)
  - impedir que las últimas seis (6) contraseñas sean reutilizadas,

25.3.7. Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas, como: instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc., Dichas cuentas no deben ser de uso habitual (diario), sino que sólo deben ser utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad Informática debe definir procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
- Las contraseñas seleccionadas deben ser seguras, y su definición debe ser efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- Las contraseñas y los nombres de las cuentas críticas a las que pertenecen deben ser resguardadas debidamente.
- La utilización de las contraseñas críticas debe ser registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
- Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma debe ser renovada en caso de que no se haya utilizado.
- Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas.
-

Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información, debe revisar los derechos de acceso de los usuarios y se deberán contemplar los siguientes controles:

- Revisar los derechos de acceso de los usuarios en intervalos no mayores a 6 meses.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso en intervalos no mayores a 3 meses.
- Revisar las asignaciones de privilegios en intervalos no mayores a 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.

26. RESPONSABILIDADES DEL USUARIO

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y

consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- Mantener las contraseñas en secreto.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el responsable del activo de Información de que se trate, que:
  - No sean fáciles de recordar.
  - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
  - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisionales en el primer inicio de sesión ("log on").
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar de acuerdo a lo establecido en 16.1 – Gestión de Incidentes y mejoras en la seguridad de la información, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

27. EQUIPOS DESATENDIDOS EN ÁREAS DE USUARIOS

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ej: un protector de pantalla protegido por contraseña, ctrl+alt+supr + Enter

- Proteger los computadores contra usos no autorizados, mediante un bloqueo de seguridad o control equivalente, por ej: contraseña de acceso cuando no se utilizan.

28. CONTROL DE ACCESO A LA RED

28.1. POLÍTICA DE UTILIZACIÓN DE LOS SERVICIOS DE RED

Las conexiones no seguras a los servicios de red pueden afectar a toda la entidad, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de toda la infraestructura tecnológica.

El Área de Tecnología tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la Secretaría Distrital de Gobierno.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas, redes y servicios de red a los cuales se les otorgará el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.
- Este ítem debe ser coherente con el punto 9 - Control de Acceso).

28.2. CAMINO FORZADO

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de la Secretaría Distrital de Gobierno, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones debe ser controlado. Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

- Asignar números telefónicos o líneas, en forma dedicada.
- Establecer la conexión automática de puertos a gateways de seguridad o a aplicativos específicos.
- Limitar las opciones de menú y submenú de cada uno de los usuarios.
- Evitar la navegación ilimitada por la red.
- Imponer el uso de aplicativos y/o gateways de seguridad específicos para usuarios externos de la red.
- Controlar activamente las comunicaciones con origen y destino autorizados a través de un Gateway (firewalls).
- Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera de la Secretaría Distrital de Gobierno.

Los requerimientos relativos a caminos forzados se basarán en lo expuesto en el capítulo 9 - Control de Acceso. El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información, deben realizar una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

28.3. AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la Secretaría Distrital de Gobierno. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros.

El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información, deben realizar una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

- Un método de autenticación físico (por ej: tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
  - Asignación del dispositivo de autenticación.
  - Registro de los poseedores de los autenticadores.
  - Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
  - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.

- Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:
  - Establecimiento de las reglas con el usuario.
  - Establecimiento de un ciclo de vida de las reglas para su renovación.
- Utilizar líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

28.4. AUTENTICACIÓN DE NODOS

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Secretaría Distrital de Gobierno. Por consiguiente, las conexiones a sistemas informáticos remotos deben ser autenticadas. Esto es particularmente importante, si la conexión utiliza una red que está fuera de control de la gestión de seguridad de la Secretaría Distrital de Gobierno.

La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

28.5. PROTECCIÓN DE LOS PUERTOS (PORTS) DE DIAGNÓSTICO REMOTO

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado.

Por consiguiente, deben ser protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "Autenticación de Usuarios para Conexiones Externas". También para este caso deberá tenerse en cuenta el punto "Camino Forzado".

28.6. SEGMENTACIÓN DE REDES

Para controlar la seguridad en una red como la de la Secretaría Distrital de Gobierno, se deben dividir en dominios lógicos separados. Para esto, se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de gateways con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios (Ver 13.1 - Gestión de la seguridad de las redes) y para bloquear el acceso no autorizado de acuerdo a los Requerimientos para el Control de Acceso.

La Segmentación en dominios de la red, tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de agrupamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso (Ver A- 9.1. Requisitos del negocio para Control de Acceso[16]), el Área de Tecnología evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados (Ver 13.1 - Gestión de la seguridad de las redes) para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad Informática, el esquema más apropiado a implementar.

Acceso a Internet

El acceso a Internet debe ser utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos deben ser autorizados formalmente por el Responsable del área organizacional a cargo del personal que lo solicite.

Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios. Entre otras, pueden definirse técnicamente pantallazos institucionales que se generen cuando un usuario accede a páginas no autorizadas prohibiendo y explicando el porqué de la prohibición, e indicándole que si existe algún error se comunique con la línea de soporte, un link, o con el administrador WEB.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.

Dicho control debe ser comunicado a los usuarios de acuerdo a lo establecido en el punto 13.2.4 - Acuerdos de confidencialidad o de no divulgación. Para ello, el Responsable de Seguridad Informática junto con el Área de Tecnología, analizarán las medidas a implementar para optimizar dicho control, como ser la instalación de firewalls, proxies, Administradores de ancho de manda, etc.

28.7. CONTROL DE CONEXIÓN A LA RED

Se deben implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los gateways que separen los diferentes dominios de la red (Ver 13.1.3- Separación en las Redes).

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

- Correo electrónico.
- Transferencia de archivos.
- Acceso interactivo.

[16] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-9.1. Requisitos del negocio para control de acceso.

- Acceso a la red fuera del horario laboral.

28.8. CONTROL DE ENRUTAMIENTO DE RED

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites de la Secretaría Distrital de Gobierno, se incorporarán controles de enrutamiento, para asegurar que las conexiones informáticas y los flujos de información no violen el capítulo (9 - Control de Acceso).

Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de enrutamiento, enrutamiento estático, traducción de direcciones y listas de control de acceso.

28.9. SEGURIDAD DE LOS SERVICIOS DE RED

El Responsable de Seguridad Informática junto con el Área de Tecnología, definirán las pautas para garantizar la seguridad de los servicios de red de la Secretaría Distrital de Gobierno, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración debe ser revisada periódicamente por el Responsable de Seguridad Informática.

29. CONTROL DE ACCESO AL SISTEMA OPERATIVO

29.1. IDENTIFICACIÓN AUTOMÁTICA DE TERMINALES

El Responsable de Seguridad Informática junto con el Área de Tecnología, realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

- El método de identificación automática de terminales utilizado.
- El detalle de transacciones permitidas por terminal.

29.2. PROCEDIMIENTOS DE CONEXIÓN DE TERMINALES

El acceso a los servicios de información sólo debe ser posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático debe ser diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer soporte innecesario a un usuario no autorizado.

El procedimiento de identificación deberá:

- Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.
- Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
- Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
- Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
- Limitar el número de intentos de conexión no exitosos permitidos y:
  - Registrar los intentos no exitosos.
  - Impedir otros intentos de identificación, una vez superado el límite permitido.
  - Desconectar conexiones de comunicaciones de datos.
- Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
- Desplegar la siguiente información, al completarse una conexión exitosa:
  - Fecha y hora de la conexión exitosa anterior.
  - Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

29.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, desarrolladores y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para la Secretaría Distrital de Gobierno, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utiliza un método de autenticación físico, por ejemplo, tokens, deberá implementarse un procedimiento que incluya:

- Asignar la herramienta de autenticación.
- Registrar los poseedores de autenticadores.
- Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.
- Revocar el acceso del autenticador, en caso de compromiso de seguridad.

29.4. SISTEMA DE ADMINISTRACIÓN DE CONTRASEÑAS

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

- Imponer el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad según lo señalado en el punto "Uso de Contraseñas".
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto "Uso de Contraseñas".
- Obligar a los usuarios a cambiar las contraseñas provisionales en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de aplicativos.
- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- Modificar todas las contraseñas predeterminadas por el proveedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, switches, routers, etc.).
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

29.5. USO DE UTILITARIOS DE SISTEMA

La Secretaría Distrital de Gobierno tiene uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial, que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

- Utilizar procedimientos de autenticación para utilitarios del sistema.
- Separar entre utilitarios del sistema y software de aplicaciones.
- Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
- Evitar que personas ajenas a la Secretaría Distrital de Gobierno, tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
- Limitar la disponibilidad de utilitarios de sistema, por ej: durante el transcurso de un cambio autorizado.
- Registrar todo uso de utilitarios del sistema.
- Definir y documentar los niveles de autorización para utilitarios del sistema.
- Remover todo el software basado en utilitarios y software de sistema innecesarios.

29.6. ALARMAS SILENCIOSAS PARA LA PROTECCIÓN DE LOS USUARIOS

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de restricción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Responsable de Seguridad Informática junto con el Área de Tecnología. En este caso, se definirán y asignarán funciones y procedimientos para responder a la utilización de una alarma silenciosa.

29.7. DESCONEXIÓN DE TERMINALES POR TIEMPO MUERTO

El Responsable de Seguridad Informática, junto con los Propietarios de la Información, definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad de la Secretaría Distrital de Gobierno, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para los computadores de usuario, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un usuario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

29.8. LIMITACIÓN DEL HORARIO DE CONEXIÓN

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se

implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo, áreas públicas o externas que estén fuera del alcance de la gestión de seguridad de la Secretaría Distrital de Gobierno.

Entre los controles que se deben aplicar, se enuncian:

- Utilizar lapsos predeterminados, por ejemplo para transmisiones en batch, o sesiones interactivas periódicas de corta duración.
- Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
- Documentar debidamente los usuarios que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

30. CONTROL DE ACCESO A LAS APLICACIONES

30.1. RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

Los usuarios de aplicativos, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los mismos de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Resolución 177 de 2007 de la Secretaría Distrital de Gobierno para el acceso a la información, (Ver A- 9.4 - Control de Acceso a sistemas y aplicaciones[17]).

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

- Proveer una interfaz para controlar el acceso a las funciones de los aplicativos. El Propietario de la Información debe ser responsable de la autorización de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas deben ser llevadas a cabo por personal del área de tecnología, conforme a una autorización formal emitida por el Propietario de la Información.
- Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los aplicativos a las cuales no sean autorizados para acceder, con la adecuada edición de la documentación de usuario.
- Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- Garantizar que las salidas de los aplicativos que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

[17] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 9.4 - Control de Acceso a sistemas y aplicaciones.

- Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
- Restringir el acceso a la información, por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

30.2. **AISLAMIENTO DE LOS SISTEMAS SENSIBLES**

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos aplicativos son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el aplicativo debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con aplicativos confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

- Identificar y documentar claramente la sensibilidad de un aplicativo. Esta tarea debe ser llevada a cabo por el propietario y el desarrollador de la aplicación (Ver A- 6.4. Clasificación y Control de Activos[18]).
- Identificar y acordar con el propietario de la aplicación sensible cuando debe ejecutarse en un ambiente compartido, los aplicativos con los cuales ésta compartirá los recursos.
- Coordinar qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
- Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
- Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: la infraestructura tecnológica alternativo o las instalaciones de emergencia donde restablecer la aplicación.

30.3. **MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS**

30.3.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:
- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Identidad o ubicación de la terminal.
- Registros de intentos exitosos y fallidos de acceso al sistema.

[18] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 6.4. Clasificación y Control de Activos.

- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría deben ser archivados preferentemente en un equipo diferente al que los genere.

Los Propietarios de la Información junto con la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

30.4. **MONITOREO DEL USO DE LOS SISTEMAS**

30.4.1. Procedimientos y Áreas de Riesgo

Se deben desarrollar procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo (Ver A - 7.2 - Seguridad de los recursos humanos - Durante la ejecución del empleo[19]).

El alcance de estos procedimientos deberá corresponder a la evaluación de riesgos que realice el Área de Tecnología y el Responsable de Seguridad Informática.
Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

- Acceso no autorizado, incluyendo detalles como:
  - Identificación del usuario.
  - Fecha y hora de eventos clave.
  - Tipos de eventos.
  - Archivos a los que se accede.
  - Utilitarios y programas utilizados.

- Todas las operaciones con privilegio, como:
  - Utilización de cuenta de supervisor.
  - Inicio y cierre del sistema.
  - Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
  - Cambio de fecha/hora.
  - Cambios en la configuración de la seguridad.

[19] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A - 7.2 - Seguridad de los recursos humanos - Durante la ejecución del empleo.

- Alta de servicios.

- Intentos de acceso no autorizado, como:
  - Intentos fallidos.
  - Violaciones de la Política de Accesos y notificaciones para gateways de red y firewalls.
  - Alertas de sistemas de detección de intrusiones.

- Alertas o fallas de sistema como:
  - Alertas o mensajes de consola.
  - Excepciones del sistema de registro.
  - Alarmas del sistema de administración de redes.
  - Accesos remotos a los sistemas.

30.4.2. Factores de Riesgo

Entre los factores de riesgo que se deben considerar se encuentran:
- La criticidad de los procesos de aplicaciones.
- El valor, la sensibilidad o criticidad de la información involucrada.
- La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
- El alcance de la interconexión del sistema (en particular las redes públicas).

Los Propietarios de la Información deben manifestar la necesidad de registrar aquellos eventos que consideren críticos para el funcionamiento que se encuentra bajo su responsabilidad.

30.4.3. Registro y Revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y métodos utilizados.

La periodicidad de dichas revisiones debe ser definida por los Propietarios de la Información y el Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el responsable del Área de Tecnología, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros.

En la asignación de funciones en materia de seguridad de la información (Ver A- 6. 0rganizacion de la seguridad de la informacion[20]), se deberán separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

- La desactivación de la herramienta de registro.
- La alteración de mensajes registrados.
- La edición o supresión de archivos de registro.
- La saturación de un medio de soporte de archivos de registro.
- La falla en los registros de los eventos.
- La sobre-escritura de los registros.

La Oficina de Control Interno, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

31. SINCRONIZACIÓN DE RELOJES

A fin de garantizar la exactitud de los registros de auditoría, los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

32. COMPUTACIÓN MÓVIL Y TRABAJO REMOTO

32.1. COMPUTACIÓN MÓVIL

Cuando se utilizan dispositivos móviles, se debe tener especial cuidado en garantizar que no se comprometa la información de la Secretaría Distrital de Gobierno.

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Tablets, Ipads, Laptops o PDA, (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, USBs, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), cámaras digitales, etc.

[20] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 6. 0rganizacion de la seguridad de la informacion.

La lista mencionada no es exclusiva, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial de la Secretaría Distrital de Gobierno y por lo tanto, ser susceptibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

- La protección física necesaria
- El acceso seguro a los dispositivos
- La utilización de los dispositivos en lugares públicos.
- El acceso a los sistemas de información y servicios de la Secretaría Distrital de Gobierno a través de dichos dispositivos.
- Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- Los mecanismos de resguardo de la información contenida en los dispositivos.
- La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo pérdida, robo o hurto. En consecuencia, deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención acerca de portar un equipo valioso.
- No poner identificaciones de la Secretaría Distrital de Gobierno en el dispositivo, salvo los estrictamente necesarios.
- No poner datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la Secretaría Distrital de Gobierno, los que incluirán:

- Revocación de las credenciales afectadas
- Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

32.2. **TRABAJO REMOTO O TELETRABAJO**

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la entidad.

El trabajo remoto sólo debe ser autorizado por el Responsable del área organizacional, o superior jerárquico correspondiente a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad Informática y se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos deben ser de excepción y deben ser contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios de la Secretaría Distrital de Gobierno, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

- La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
- El ambiente de trabajo remoto propuesto.
- Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la Secretaría Distrital de Gobierno, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
- La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
- Evitar la instalación/desinstalación de software no autorizada por la entidad. Los controles y disposiciones comprenden:
    - Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.
    - Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red de la Secretaría Distrital de Gobierno, los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
    - Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
    - Incluir seguridad física.
    - Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
    - Proveer el hardware, soporte y mantenimiento del software.
    - Definir los procedimientos de backup y de continuidad de las operaciones.
    - Efectuar auditoría y monitoreo de la seguridad.
    - Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
    - Asegurar el reintegro del equipo en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que deben ser revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

33. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y desarrolladores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Este ítem se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Secretaría Distrital de Gobierno, en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad Informática junto con el Propietario de la Información y la Oficina de Control Interno, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad Informática junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Los Responsables de Seguridad Informática y del Área de Tecnología, definirán los métodos de encripción a ser utilizados.

Asimismo, el Responsable de Seguridad Informática, deberá:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Área de Tecnología, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en el presente capítulo. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Tecnología propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Área de Tecnología incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros para el desarrollo de software. El Responsable del Área Legal participará en dicha tarea.

33.1. ANÁLISIS Y ESPECIFICACIONES DE LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS

Este ítem se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

- Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
- Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
- Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener, aquellos incluidos durante o después de la implementación.

33.2. **SEGURIDAD EN LOS APLICATIVOS**

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

- La validación de datos de entrada.
- El procesamiento interno.
- La autenticación de mensajes (interfaces entre sistemas)
- La validación de datos de salida.

33.3. **VALIDACIÓN DE DATOS DE ENTRADA**

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.
Este procedimiento considerará los siguientes controles:

- Control de secuencia.
- Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
- Control de paridad.

- Control contra valores cargados en las tablas de datos.
- Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

- Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.
- Se definirá un procedimiento que especifique las alternativas a seguir para responder a errores de validación en un aplicativo.
- Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

33.4. **CONTROLES DE PROCESAMIENTO INTERNO**

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán procedimientos que:

- permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
- establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
- establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
- realicen la validación de los datos generados por el sistema.
- verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
- controlen la integridad de registros y archivos.
- verifiquen la ejecución de los aplicativos en un momento determinado.
- aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

33.5. AUTENTICACIÓN DE MENSAJES

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles expuestos en el numeral A-10.1 - Controles Criptográficos[21].

33.6. VALIDACIÓN DE DATOS DE SALIDAS

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

- Comprobaciones de la razonabilidad para probar si los datos de salida son verídicos.
- Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
- Provisión de información suficiente, para que sea posible determinar la exactitud, totalidad, precisión y clasificación de la información.
- Procedimientos para responder a las pruebas de validación de salidas.
- Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

34. CONTROLES CRIPTOGRÁFICOS

Se deben utilizar sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

Utilización de Controles Criptográficos.

La Secretaría Distrital de Gobierno debe establecer una política para el uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

- Se utilizarán controles criptográficos en los siguientes casos:
  - Para la protección de claves de acceso a sistemas, datos y servicios.
  - Para la transmisión de información clasificada, fuera del ámbito de la Secretaría Distrital de Gobierno.
  - Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.

- Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al remplazo de las claves de cifrado.

[21]Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-10.1 - Controles Criptográficos.

- El Área de Tecnología propondrá la siguiente asignación de funciones:
  - Función
  - Cargo
  - Implementación de la Política de Controles
  - Criptográficos
  - Administración de Claves

- Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:
  - Cifrado Simétrico
    - Algoritmo Longitud de Clave
    - AES 128/192/256
    - 3DES 168 bits
    - IDEA 128 bits
    - RC4 128 bits
    - RC2 128 bits

  - Cifrado Asimétrico
    - Casos de Utilización Algoritmo Longitud de
    - Clave

  - Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)
    - RSA 2048 bits
    - DSA 2048 bits
    - ECDSA 210 bits
    - Para certificados de sitio seguro RSA 1024 bits

  - Para certificados de Certificador o de información de estado de certificados
    - RSA 2048 bits
    - DSA 2048 bits
    - ECDSA 210 bits

  - Para certificados de usuario (personas físicas o jurídicas)
    - RSA 1024 bits
    - DSA 1024 bits
    - ECDSA 160 bits
    - Para digesto seguro SHA-1 256 bits

Los algoritmos y longitudes de clave mencionados son los que a la fecha se consideran seguros. Esta condición debe ser verificada periódicamente con el objeto de efectuar las actualizaciones correspondientes.

34.1. **CIFRADO**

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad Informática, se debe identificar el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al momento de implementar la Política de la Secretaría Distrital de Gobierno en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica (Ver A- 18.1.5. Reglamentación de Controles Criptográficos[22]).

34.2. **FIRMA DIGITAL**

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se tomarán las precauciones necesarias para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.
Los algoritmos de firma utilizados, como así también la longitud de clave a emplear, son las enumeradas en el punto 10.1- Controles Criptográficos, en el cuadro de cifrado asimétrico.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Al utilizar firmas y certificados digitales, se considerará la legislación vigente y el conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos, que describan las condiciones bajo las cuales una firma digital es legalmente válida. (Ver 18.1.5 - Reglamentación de Controles Criptográficos).

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se deberá obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar. (Ver 18 - Cumplimiento).

[22] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 18.1.5. Reglamentación de Controles Criptográficos.

34.3. SERVICIOS DE NO REPUDIO

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

34.4. ADMINISTRACIÓN DE CLAVES - PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Se debe implementar un sistema de administración de claves criptográficas para respaldar la utilización por parte de la Secretaría Distrital de Gobierno de los dos tipos de técnicas criptográficas, a saber:

- Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

- Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública que puede ser revelada a cualquier persona utilizada para cifrar y una clave privada que debe mantenerse en secreto utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves deben ser protegidas contra modificación y destrucción, y las claves secretas y privadas deben ser protegidas contra copia o divulgación no autorizada.

Se aplicarán con éste propósito los algoritmos criptográficos enumerados en el punto 10.1 - Controles Criptográficos.

Se proporcionará una protección adecuada al equipo de cómputo utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
Normas, Procedimientos y Métodos

Se deben redactarán las normas y procedimientos necesarios para:

- Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- Generar y obtener certificados de clave pública de manera segura.
- Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
- Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
- Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.

- Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula de la Secretaría Distrital de Gobierno, en cuyo caso las claves también deben archivarse.
- Recuperar claves pérdidas o alteradas como parte de la administración de la continuidad de las actividades de la Secretaría Distrital de Gobierno, por ejemplo para la recuperación de la información cifrada.
- Archivar claves, por ejemplo, para la información archivada o resguardada.
- Destruir claves.
- Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de un tiempo determinado, no mayor a 12 meses.

Además de la administración segura de las claves secretas y privadas, deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

En consecuencia es importante que el proceso de administración de los certificados de clave pública, sea absolutamente confiable. Este proceso es llevado a cabo por una Entidad denominada Autoridad de Certificación (AC) o Certificadora.

35. SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

Se debe garantizar que los desarrollos y actividades de soporte a los sistemas, se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

Control del Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

- Toda aplicación, desarrollada por La Secretaría Distrital de Gobierno o por un tercero tendrá un único Responsable designado formalmente por el Área de Tecnología.
- Ningún desarrollador o analista, o personal de mantenimiento de aplicaciones, podrá acceder a los ambientes de producción.
- El Área de Tecnología, asignará a quien corresponda la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:

    - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

- Asegurar que los aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
- Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del área encargada de la prueba y del usuario final.
- Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

- Otros controles a realizar son:
  - Guardar sólo los ejecutables en el ambiente de producción.
  - Llevar un registro de auditoría de las actualizaciones realizadas.
  - Retener las versiones previas del sistema, como medida de contingencia (Rollback).
  - Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones pertinentes, las pruebas previas a realizarse, etc.
  - Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
  - Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

35.1. **PROTECCIÓN DE LOS DATOS DE PRUEBA DEL SISTEMA**

Las pruebas de los sistemas se harán sobre datos extraídos del ambiente de producción.

Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos en producción. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base en producción, como base de prueba, llevando registro de tal autorización.
- Eliminar inmediatamente, una vez realizadas las pruebas, la información operativa utilizada.

35.2. **CONTROL DE CAMBIOS A DATOS OPERATIVOS**

La modificación, actualización o eliminación de los datos operativos deben ser realizadas a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos (Ver A- 9.2 - Gestión de Acceso de Usuarios[23]).

[23] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 9.2 - Gestión de Acceso de Usuarios.

Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación del presente punto, se considerarán como excepciones. El Responsable de Seguridad Informática definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

- Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
- El Propietario de la Información afectada y del Responsable de Seguridad Informática aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
- Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas deben ser protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas (Ver 9.2 - Gestión de Acceso de Usuarios). y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
- Se designará un encargado de implementar los cambios, el cual no debe ser personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en 6.1.2 - Separación de Deberes.
- Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro debe ser revisado posteriormente por el Responsable de Seguridad Informática.

35.3. CONTROL DE ACCESO A LAS BIBLIOTECAS DE PROGRAMAS FUENTES

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

- El área de Tecnología, asignará la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y deberá:
  - Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
  - Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, desarrollador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
  - Registrar cada solicitud aprobada.
  - Administrar las distintas versiones de una aplicación.
  - Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

- Denegar al "administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.

- Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
- Desarrollar un procedimiento que garantice, que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
- Evitar que la función de "administrador de programas fuentes" sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.
- Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
- Prohibir el acceso a todo operador y/o usuario de aplicaciones, a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
- Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la Secretaría Distrital de Gobierno en los procedimientos que surgen del presente ítem.

35.4. **SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE**

Este punto provee seguridad al software y a la información del aplicativo, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

35.4.1. Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello, se debe establecer un procedimiento que incluya las siguientes consideraciones:

- Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
- Revisar los controles y los procedimientos de integridad para garantizar que no deben ser comprometidos por los cambios.

- Obtener aprobación formal por parte del área de Tecnología, para las tareas detalladas, antes de iniciarlas.
- Solicitar la revisión del Responsable de Seguridad Informática para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Obtener la aprobación de pruebas en el ambiente correspondiente.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Garantizar que la implementación se llevará a cabo minimizando la suspensión de las actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operación.
- Garantizar que sea el implementador quien efectúe el traslado de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en el numeral A-12.5 - Control del Software Operacional[24].

En el Anexo al presente capítulo se presenta un esquema modelo de segregación de ambientes de procesamiento.

35.4.2. Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

En este sentido, se redactarán normas y procedimientos que incluyan:

- Adquirir programas a proveedores acreditados o productos ya evaluados.
- Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
- Controlar el acceso y las modificaciones al código instalado.
- Utilizar herramientas para la protección contra la infección del software con código malicioso.

Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

[24] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A-12.5 - Control del Software Operacional.

A continuación se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de la Secretaría Distrital de Gobierno, teniendo en cuenta las capacidades instaladas, los recursos y la infraestructura tecnológica existente.

35.5. **AMBIENTE DE DESARROLLO**

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o desarrollador tiene total dominio sobre el ambiente. Puede recibir alguna fuente para modificar, quedando registrado en el sistema de control de versiones que administra el "administrador de programas fuentes".

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

35.6. **AMBIENTE DE PRUEBAS**

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto.

El "testeador" realiza las pruebas con los datos de la base de pruebas. Si no detecta errores de ejecución y los resultados de las rutinas de seguridad son correctas de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

35.7. **AMBIENTE DE PRODUCCIÓN**

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El "implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de

las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

36. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO SECRETARÍA DISTRITAL DE GOBIERNO

Generalidades

La Continuidad del Negocio, es un proceso crítico que debe involucrar a todos los niveles de la Secretaría Distrital de Gobierno.

El desarrollo e implementación de planes de contingencia y continuidad, es una herramienta básica para garantizar que las actividades de la Secretaría Distrital de Gobierno puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la Secretaría Distrital de Gobierno y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales de la Secretaría Distrital de Gobierno (sean éstas resultado de desastres naturales, accidentes, fallas en la infraestructura tecnológica, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia de la Secretaría Distrital de Gobierno con el establecimiento de planes que incluyan al menos las siguientes etapas:

- Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
- Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la Secretaría Distrital de Gobierno y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Este punto se aplica a todos los procesos críticos identificados de la Secretaría Distrital de Gobierno.

Responsabilidad

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información (Ver A- 6.1.1 Roles y Responsabilidades para la Seguridad de la Información[25]) y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar los riesgos y amenazas que puedan ocasionar interrupciones de los procesos y/o funcionamiento de la Secretaría Distrital de Gobierno.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Secretaría Distrital de Gobierno.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Secretaría Distrital de Gobierno.

Los Responsables de Procesos revisarán periódicamente los planes de su incumbencia, como también, identificar cambios en las disposiciones relativas a las actividades de la Secretaría Distrital de Gobierno aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad del funcionamiento de los sistemas de tratamiento de información de la Secretaría Distrital de Gobierno frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades de la Secretaría Distrital de Gobierno.

[25] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 6.1.1 Roles y Responsabilidades para la Seguridad de la Información.

- Asegurar que todos los integrantes de la Secretaría Distrital de Gobierno comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la Secretaría Distrital de Gobierno.
- Elaborar y documentar una estrategia de continuidad de las actividades de la Secretaría Distrital de Gobierno consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la Secretaría Distrital de Gobierno de conformidad con la estrategia acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la Secretaría Distrital de Gobierno.
- Proponer las modificaciones a los planes de contingencia.

36.1. PROCESO DE CONTINUIDAD DEL NEGOCIO SECRETARÍA DISTRITAL DE GOBIERNO

El Comité de Seguridad de la Información, debe ser el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la Secretaría Distrital de Gobierno.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad del funcionamiento de los sistemas de información y comunicaciones de la Secretaría Distrital de Gobierno frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades de la Secretaría Distrital de Gobierno.
- Asegurar que todos los integrantes de la Secretaría Distrital de Gobierno comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la Secretaría Distrital de Gobierno.
- Elaborar y documentar una estrategia de continuidad de las actividades de la Secretaría Distrital de Gobierno consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la Secretaría Distrital de Gobierno de conformidad con la estrategia acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad del negocio de la Secretaría Distrital de Gobierno.
- Proponer las modificaciones a los planes de contingencia.

36.2. CONTINUIDAD DEL NEGOCIO Y ANÁLISIS DE LOS IMPACTOS

Con el fin de establecer un Plan de Continuidad del Negocio de la Secretaría Distrital de Gobierno se deben contemplar los siguientes puntos:

- Identificar las amenazas que puedan ocasionar interrupciones en el funcionamiento, por ejemplo, fallas en los equipos centrales del Datacenter, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
  Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad debe ser llevada a cabo con la activa participación de los dueños de los procesos y recursos de información implicados y el Responsable de Seguridad Informática, considerando todos los procesos de las actividades de la Secretaría Distrital de Gobierno y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Secretaría Distrital de Gobierno. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la alta dirección de la Secretaría Distrital de Gobierno para su aprobación.

36.3. ELABORACIÓN E IMPLEMENTACIÓN DE LOS PLANES DE CONTINUIDAD

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, deben elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Secretaría Distrital de Gobierno.

Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información.

El proceso de planificación de la Continuidad del Negocio considerará los siguientes puntos:

- Identificar y acordar todas las funciones y procedimientos de emergencia.
- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.

- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos.
- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
  - Objetivo del plan.
  - Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
  - Procedimientos de divulgación.
  - Requisitos de la seguridad.
  - Procesos específicos para el personal involucrado.
  - Responsabilidades individuales.
- Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades de la Secretaría Distrital de Gobierno requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

36.4. MARCO PARA LA PLANIFICACIÓN DE CONTINUIDAD DEL NEGOCIO

Se mantendrá un solo marco para los planes de continuidad del negocio de la Secretaría Distrital de Gobierno, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad, debe especificar claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad debe ser el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deberán ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad del negocio de la Secretaría Distrital de Gobierno, tendrá en cuenta los siguientes puntos:

- Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
- Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la Secretaría Distrital de Gobierno y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, con la policía, autoridades locales y otras de emergencia.
- Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la Secretaría Distrital de Gobierno o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.
- Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la Secretaría Distrital de Gobierno.
- Definir un cronograma de mantenimiento que especifique cómo y cuándo debe ser probado el plan, y el proceso para el mantenimiento del mismo.
- Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan.

36.5. ENSAYO, MANTENIMIENTO Y REEVALUACIÓN DE LOS PLANES DE CONTINUIDAD.

Debido a que los planes de continuidad de las actividades de la Secretaría Distrital de Gobierno pueden fallar, por suposiciones incorrectas, errores o cambios en la infraestructura tecnológica, se establecen las siguientes pautas de acción:

- El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
- El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y revelar el resultado obtenido al citado Comité.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionen ante un hecho real, y éstas incluirán por lo menos:

- Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).
- Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información y comunicaciones puedan ser restablecidos eficazmente).
- Realizar ensayos completos probando que la entidad, el personal, la infraestructura tecnológica, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas de la Secretaría Distrital de Gobierno se tomarán en cuenta, además, los siguientes mecanismos:

- Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades de la Secretaría Distrital de Gobierno en paralelo, con operaciones de recuperación fuera del sitio principal).
- Realizar pruebas de instalaciones y servicios de proveedores, garantizando que los productos y servicios de los mismos cumplan con los compromisos contraídos.

Los planes de continuidad del negocio de la Secretaría Distrital de Gobierno, deben ser revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se deben incluir procedimientos en el programa de administración de cambios de la Secretaría Distrital de Gobierno para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

Las revisiones periódicas deben ser revisadas por los responsables de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas al funcionamiento de la Secretaría Distrital de Gobierno aún no reflejadas en dichos planes.

Deberá prestarse atención, especialmente, a los cambios de:

- Personal.
- Direcciones o números telefónicos.
- Estrategia de la Secretaría Distrital de Gobierno.
- Ubicación, instalaciones y recursos.
- Legislación.
- Contratistas, proveedores y clientes críticos.
- Procesos nuevos / eliminados.
- Tecnologías.
- Requisitos operacionales.
- Requisitos de seguridad.
- Hardware, software y otros equipos (tipos, especificaciones, y cantidad).

- Requerimientos de los sitios alternativos.
- Registros de datos vitales.

Todas las modificaciones efectuadas, deben ser propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso debe ser dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

36.6. NOTAS IMPORTANTES PLAN DE CONTINUIDAD

La Secretaría Distrital de Gobierno debe considerar fuertemente la importancia de poseer planes informáticos para garantizar la continuidad del negocio (BCP, DRP), de tal forma que la gestión de la contingencia, llegue a ser una variable muy importante, con el fin de lograr que la Entidad sobreviva en un ambiente cada vez más dinámico y con alto riesgo.

Por otra parte, todos sabemos que los desastres pueden ocurrir en cualquier momento y Bogotá esta propensa a este riesgo, es por eso, que se requiere un plan detallado que proteja las personas, infraestructura tecnológica, Aplicativos misionales, servicios, etc., con el fin de poderlos retornar a su normal operación tan pronto como sea posible.

Por medio de la implantación de medidas o controles que puedan mitigar el impacto producido por una catástrofe, se puede lograr confianza por parte de la comunidad. En este punto es importante considerar que no sólo debemos tener en cuenta aspectos económicos, sino otros temas como la reputación y la credibilidad de la Secretaría Distrital de Gobierno, que se pueden poner en peligro, si ante un desastre o evento adverso no se responde con la adecuada estrategia y acciones soportadas por un plan previamente concebido.

Clases de desastres

Es posible plantear la siguiente clasificación de los desastres:

- Desastres naturales
  - Terremotos
  - Inundaciones
  - Fallas de potencia prologadas
- Accidentales
  - Falla en la base de datos
  - Falla de la estructura física
- Intencionales Externas
  - Terrorismo
  - Hackers
- Intencionales Internas

- Huelga, sabotaje, borrado de datos

36.6.1. Etapas de un BCP o DRP

Las etapas tradicionalmente consideradas son:

1. Inicio del proyecto: Establece un equipo para el proyecto y una estrategia para desarrollar el plan.
2. Análisis de impacto sobre el negocio (AIN) o BIA: Identifica los aspectos críticos relacionados con el máximo tiempo en que un proceso puede estar no disponible.
3. Estrategia de recuperación: Identifica y selecciona las apropiadas alternativas de recuperación para lograr los tiempos requeridos definidos en el AIN.
4. Diseño del plan y desarrollo: Documenta las estrategias de recuperación.
5. Prueba, Mantenimiento, y capacitación: Probar las estrategias de recuperación anteriormente definidas, manteniendo actualizado el plan y dándolo a conocer a todos los funcionarios de la Entidad.

36.6.2. Análisis del impacto sobre el negocio de un BCP, DRP

El análisis del impacto sobre el negocio (BIA) es uno de los aspectos más importantes a considerar en el desarrollo de un plan de continuidad del negocio. Se trata pues, de identificar los diversos eventos que pudieran afectar la continuidad del funcionamiento de la Entidad. En este sentido. También es importante determinar, cuales son los máximos tiempos tolerables de caída (MTD).

36.6.3. Estrategias de Recuperación BCP, DRP

Las estrategias de recuperación están basadas obviamente en los resultados obtenidos del punto anterior, en donde también se consideraron los valores de los tiempos máximos permitidos de no disponibilidad (MTD).

Los elementos tecnológicos a considerar son:

- Redes
- Servidores de aplicaciones
- Bases de datos
- Sistemas telefónicos
- Redes Locales
- Data centers

36.6.4. Restablecimiento de la Información

Busca asegurar el respaldo de la información crítica para que los sistemas de información operen normalmente.

Los medios magnéticos que contienen el backup de la información deben ser debidamente protegidos contra riesgos de tipo físico, accidental o intencional. Se debe tener una copia de dichos backups en una entidad externa a la organización, procedimiento que será realizado periódicamente.

Pruebas (BCP, DRP)

Estos son algunos tipos de pruebas a realizar al BCP:

- Revisión estructurada del plan
- Prueba de la lista de verificación
- Simulaciones
- Prueba en paralelo
- Prueba de interrupción completa

Adiestramiento en BCP, DRP

Finalmente, es importante que toda la Secretaría Distrital de Gobierno conozca en forma detallada los objetivos del plan de continuidad del negocio. Esto con el fin que, en caso de activarse el plan, cada uno de los funcionarios conozca las actividades que debe ejecutar y el plan sea ejecutado efectiva y eficientemente.

Definiciones[26]

Plan de continuidad del negocio (BCP-Business Continuity Plan): Plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio.

Plan de Contingencia: Contempla como reaccionar ante una contingencia que pueda afectar la disponibilidad, accesibilidad o los servicios ofrecidos por los sistemas informáticos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de software o hardware, errores humanos, intrusión etc.

Plan de recuperación frente a desastres (DRP): Es aquella parte del plan de contingencia y del plan de continuidad de negocio, que aborda aquellas contingencias que, por su gravedad, no permiten continuar prestando el servicio desde el centro local y debe continuarse el servicio desde un nuevo centro. Este plan debe contemplar la vuelta atrás cuando, tras arreglar las consecuencias del desastre, el servicio pueda ser reanudado en el centro local.

---

26 *Definiciones extractadas del link* http://www.sisteseg.com/sindustrial.html

Business Impact Analysis (BIA): Documento que ayuda a entender el impacto que un desastre pueda tener sobre un negocio en particular. Contempla los siguientes objetivos fundamentales:

- Priorizar procesos críticos del negocio.
- Calcular el "Maximun Tolerable Downtime", (MTD) Tiempo máximo sin servicio que una organización puede soportar y seguir siendo una entidad que cumple con sus objetivos de negocio.

37. CUMPLIMIENTO

Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a los sistemas de información y comunicaciones deben estar debidamente definidos y documentados.

El Área Legal de la Secretaría Distrital de Gobierno, debe ser responsable de blindar jurídicamente la formulación e implementación de la política.

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas para la entidad y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la Secretaría Distrital de Gobierno.

Revisar la seguridad de los sistemas de información y comunicaciones periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Secretaría Distrital de Gobierno.

Alcance

Se aplica a todo el personal de la Secretaría Distrital de Gobierno, cualquiera sea su situación laboral. Asimismo, se aplica a los sistemas de información, redes y comunicaciones, normas, procedimientos, documentación y plataformas técnicas de la Secretaría Distrital de Gobierno y a las auditorías efectuadas sobre los mismos.

Responsabilidad

El Responsable de Seguridad Informática cumplirá las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- Realizar revisiones periódicas de todas las áreas de la Secretaría Distrital de Gobierno a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información y comunicaciones cumplan la política, normas y procedimientos de seguridad establecidos.
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

Los responsables del Área Legal y de Seguridad Informática de la Secretaría Distrital de Gobierno, cumplirán las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los Responsables de las áreas Organizativas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos dentro de su área de responsabilidad.

Todos los funcionarios de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la política y la normativa vigente.

37.1. CUMPLIMIENTO DE REQUISITOS LEGALES

37.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los

controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

37.1.2. Derechos de Propiedad Intelectual del Software

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los funcionarios únicamente podrán utilizar material autorizado por la Secretaría Distrital de Gobierno.

La Entidad solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deberán tener presentes las siguientes normas:

- *Ley 44 de 1993 sobre Propiedad Intelectual y Derechos de Autor y Decreto 1360 de 1989*: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.
- *Ley 1343 de 2009 sobre ley de marcas*: Protege la propiedad de una marca y la exclusividad de su uso.
- *Ley de Patentes de Invención*: Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

El software es considerado una obra intelectual que goza de la protección de la Ley 1360 de 1989 sobre Propiedad Intelectual.

Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente, bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

Los Responsables de Seguridad Informática y del Área Legal, deben analizar los términos y condiciones de la licencia, e implementará controles como:

- Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
- Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
- Mantener un adecuado registro de licenciamiento.
- Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
- Implementar controles para evitar el exceso del número máximo permitido de usuarios.
- Verificar que sólo se instalen productos con licencia y software autorizado.
- Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
- Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
- Utilizar herramientas de auditoría adecuadas.
- Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.
- Proteger a la entidad con relación al software que utilizan terceros en equipos que no son de propiedad de la Secretaría Distrital de Gobierno.

37.1.3. Protección de los Registros críticos de la Secretaría Distrital de Gobierno

Los registros críticos de la Secretaría Distrital de Gobierno se deben protegerse contra pérdida, destrucción y falsificación.

Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la Secretaría Distrital de Gobierno.

Los registros se deben clasificar en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo impresos, medios magnéticos u ópticos.

- Tipo de Registro Sistema de Información
- Período de Retención
- Medio de Almacenamiento
- Responsable

Las claves criptográficas asociadas con archivos cifrados se deben mantener en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario (Ver A- 10.1.Controles Criptográficos[27]).

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante. (Ver A- 10.1.1.Política sobre el uso de Controles Criptográficos[28]).

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos deben ser seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable en una investigación judicial, por ejemplo, que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para la entidad.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

- Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
- Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
- Mantener un inventario de programas fuentes de información clave.
- Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

38. PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL

Todos los funcionarios deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

[27] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 10.1.Controles Criptográficos.
[28] Norma Técnica NTC-ISO-IEC Colombiana, 2701:2013, A- 10.1.1.Política sobre el uso de Controles Criptográficos.

La Entidad redactará un "Acuerdo de Confidencialidad", el cual deberá ser suscrito por todos los servidores públicos y contratistas. La copia firmada del compromiso debe ser retenida en forma segura por la entidad.

Mediante este instrumento, el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, esparcir o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable de la información de que se trate. A través del "Acuerdo de Confidencialidad" se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas de acuerdo a la Resolución 177 de 2007.

39. PREVENCIÓN DEL USO INADECUADO DE LOS RECURSOS INFORMÁTICOS

Los recursos de procesamiento de información de la Secretaría Distrital de Gobierno, se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.
Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo, so pena de aplicar las leyes que para este fin están incluidos en la legislación colombiana.

40. REGULACIÓN DE CONTROLES PARA EL USO DE CRIPTOGRAFÍA

Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley 527 de 1999, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, la entidad debe garantizar que sus sistemas de información y comunicaciones cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma.

Esta pista se establecerá cumpliendo las siguientes condiciones:

- Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién, dónde, cómo y cuándo se encontró y quién presenció el hallazgo.
- Cualquier investigación debe garantizar que los originales no sean alterados.
- Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivara en una demanda legal, por lo tanto se deben tomar todas las precauciones establecidas para la obtención y preservación de la evidencia.

41. REVISIONES DE LA POLÍTICA DE SEGURIDAD Y LA COMPATIBILIDAD TÉCNICA

41.1. CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD

Cada Responsable de la entidad, debe velar por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad Informática, debe realizar revisiones periódicas de todas las áreas de la Secretaría Distrital de Gobierno a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- Sistemas de información.
- Redes y comunicaciones
- Equipos de seguridad, firewall, antivirus
- Proveedores de sistemas.
- Propietarios de información.
- Usuarios.

Los Propietarios de la Información, deben brindar apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

41.2. VERIFICACIÓN DE LA COMPATIBILIDAD TÉCNICA

El Responsable de Seguridad Informática debe verificar periódicamente que los sistemas de información y comunicaciones, cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación, se plasmará en un informe técnico para su interpretación posterior por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional

experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que deben ser interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en la infraestructura tecnológica y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán las precauciones necesarias en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo deben ser realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

41.3. CONSIDERACIONES DE AUDITORÍAS DE SISTEMAS

Con relación a las auditorías, deben ser de aplicación las Normas de Control Interno, disciplinario y otras estipuladas para las conductas de los usuarios de la Secretaría Distrital de Gobierno.

41.3.1. Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se deben tomar precauciones en la planificación de los requerimientos y tareas, y se deben acordar, con las áreas involucradas, los procedimientos para minimizar el riesgo de interrupciones en el funcionamiento de la Secretaría Distrital de Gobierno.

Se deben contemplar los siguientes puntos:

- Acordar con el Área que corresponda los requerimientos de auditoría.
- Controlar el alcance de las verificaciones. Esta función debe ser realizada por el responsable de auditoría.
- Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán las precauciones necesarias a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
  - Eliminar archivos transitorios.
  - Eliminar volúmenes ficticios (de prueba) y datos incorporados en archivos maestros.
  - Revertir transacciones.
  - Revocar privilegios otorgados
- Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales deben ser puestos a disposición de los auditores.
- Identificar y acordar los requerimientos de procesamiento especial o adicional.
- Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar, deben incluir como mínimo:

- Fecha y hora.
- Puesto de trabajo.
- Usuario.
- Tipo de acceso.
- Identificación de los datos accedidos.
- Estado previo y posterior.
- Programa y/o función utilizada.

- Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

41.3.2. Protección de los Elementos Utilizados por la Auditoría de Sistemas

Las herramientas de protección y aseguramiento, deben estar separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

41.3.3. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en las Políticas de Seguridad y sus anexos conforme a lo dispuesto por las normas colombianas y la Resolución 0177 de 2007 de la Secretaría Distrital de Gobierno y en caso de ser pertinente, se realizarán las acciones correspondientes ante el o las entidades que sean necesarias.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales demás normativas específicas aplicables.

De acuerdo con las sanciones disciplinarias o administrativas, el agente que no da debido cumplimiento a sus obligaciones, pueden incurrir también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado, y/o en responsabilidad penal, cuando su conducta constituye un comportamiento considerado delito por el Código Penal Colombiano.

42. DOCUMENTOS RELACIONADOS

42.1. DOCUMENTOS INTERNOS

CÓDIGO SIG	NOMBRE DEL DOCUMENTO
1D-GAR-F119	Formato de “plan de pruebas”
1D-GAR-F147	Formato de “requerimientos técnicos”
1D-GAR-F175	Formato solicitud cuentas de usuario
1D-GAR-I034	Instructivo para el monitoreo de infraestructura de red de datos
1D-GAR- I036	Instructivo para el préstamo de equipos de cómputo
1D-GAR-I039	Instructivo para la creación, modificación y eliminación de cuentas en el directorio Activo

CÓDIGO SIG	NOMBRE DEL DOCUMENTO
1D-GAR-I052	Instructivo para el control de versiones y despliegue de sistemas de información
1D-GAR-I054	Instructivo para la realización de backup para bases de datos
1D-GAR-I055	Instructivo para la realización de pruebas de carga y estrés
1D-GAR- P003	Procedimiento para la gestión de servicios de tecnologías de la información y las comunicaciones.
1D-PGE-M001	Manual del SIG
1D-PGE-M004	Manual de gestión del riesgo
2L-GAR-P001	Procedimiento para la adquisición y administración de bienes y servicios local

42.2. NORMATIVIDAD VIGENTE

NORMA	AÑO	EPÍGRAFE	ARTICULO (S)
Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, y se dictan otras disposiciones.	
Ley 1341	2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC	
Decreto Nacional 2573	2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009	
Directiva Presidencial 002	2002	Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).	
Acuerdo 057	2002	Por el cual se dictan disposiciones generales para la implementación del sistema distrital de información -SDI-, se organiza la Comisión Distrital de Sistemas.	
Resolución Secretaría Distrital de Gobierno 177	2007	Por la cual se adoptan las políticas de seguridad para el manejo de la información y se imparten instrucciones para el uso y administración del recurso tecnológico de la Secretaría de Gobierno Distrital.	
Resolución Secretaría Distrital de Gobierno	2011	Por la cual se crea La Política de Seguridad del Subsistema de Gestión de Seguridad de la Información es aplicable para todos los aspectos administrativos y de control, a la totalidad de los	

NORMA	AÑO	EPÍGRAFE	ARTICULO (S)
1120		proceso internos o externos, del nivel central y local que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Secretaría Distrital de Gobierno, cualquiera sea su situación contractual, la dependencia a la cual se encuentren adscritos y el nivel de las tareas que desempeñe, para el adecuado y efectivo cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de los activos de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de este documento. El Comité del Sistema Integrado de Gestión y los Subcomités Técnicos para la implementación y mejora de los Subsistemas de Gestión, y se dictan otras disposiciones.	
Resolución Secretaría Distrital de Gobierno 520	2013	Por la cual se crea el Comité del Sistema Integrado de Gestión y los Subcomités Técnicos para la implementación y mejora de los Subsistemas de Gestión.	
Resolución Secretaría Distrital de Gobierno 419	2014	Conformación del Subcomité Técnico de Gobierno en Línea – Seguridad de la Información y Gestión Documental, integrantes y Responsabilidades	
Directiva 005	2005	Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital.	
Directiva 042	2007	Políticas de seguridad de los activos de información para la Secretaría General de la Alcaldía.	

42.3. DOCUMENTOS EXTERNOS

NOMBRE	FECHA DE PUBLICACIÓN O VERSIÓN	ENTIDAD QUE LO EMITE	MEDIO DE CONSULTA
Norma Técnica NTC-ISO-IEC Colombiana 27001	2013-12-11	Instituto Colombiano De Normas Técnicas y certificación ICONTEC	INTERNET

NOMBRE	FECHA DE PUBLICACIÓN O VERSIÓN	ENTIDAD QUE LO EMITE	MEDIO DE CONSULTA
Anexo 5: Formato Política SGSI Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0	Versión 2.0.112/07/2011	Ministerio de Tecnologías de la Información y las Comunicaciones	INTERNET