SECRETARÍA JURÍDICA DISTRITAL
ALCALDÍA MAYOR DE BOGOTÁ, D.C.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. OBJETIVO

Establecer las políticas de seguridad de la información y los datos personales para la Secretaría Jurídica Distrital, con el fin de cumplir con los requisitos de seguridad, definidos en el SGSI y el MSPI que ayudarán mediante su implementación, a preservar la confidencialidad, integridad y disponibilidad de la información.

La Seguridad de la Información es una prioridad para la Secretaría jurídica Distrital, por lo tanto, es responsabilidad de todos los funcionarios y contratistas de la entidad velar por el continuo cumplimiento de las políticas definidas.

1.1. Objetivos Específicos

La Secretaría Jurídica Distrital, para el cumplimiento de su misión, visión, objetivo estratégicos y alineados a sus valores corporativos, estableces la función de Seguridad de la Información de la Información en la entidad, con el objetivo de:

a. Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad, mediante la implementación de controles en los procesos de la entidad de manera coordinada con las partes interesadas.

b. Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios, contratistas respecto al correcto manejo y protección de la información que es gestionada y resguardada en la Secretaría Jurídica Distrital.

c. Gestionar los riesgos asociados con la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información dentro del alcance del Subsistema de Gestión de Seguridad de la Información. (SGSI).

d. Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de derechos.

e. Sensibilizar y entrenar al personal de la entidad en el Subsistema de Gestión de Seguridad de la Información (SGSI).

2. ALCANCE

La Política de Seguridad de la Información, aplica a toda la entidad, sus funcionarios, contratistas que tengan relación directa con las entidades que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica, canales de comunicación de la entidad, bases de datos y en general los archivos informáticos que conforman el Sitio Web, Subsistemas de Información y documentos físicos de la Secretaría Jurídica Distrital.

Todas las políticas contenidas en este documento, las cuales están basadas en los lineamientos de la norma ISO 27001:2013 y los lineamientos del Modelo de Seguridad y Privacidad de Información (MSPI) y sus correspondientes guías de apoyo, serán aplicadas a los procesos estratégicos, misionales y de apoyo de toda la Secretaría Jurídica Distrital.

3. GLOSARIO

Activos: Todo lo que tiene valor para la Organización. Hay varios tipos de activos entre los que se incluye: Información; Software; como un programa de cómputo; Físico, como un computador; Servicios; Personas, sus calificaciones habilidades y experiencias e intangibles tales como a reputación y la imagen.

Administrador de base de datos personales. Funcionario, contratista o encargado que tiene a cargo y realiza tratamiento a una más base de datos que tiene la información personal.

Análisis de riesgos: Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

Archivo: Conjunto de datos almacenados en la memoria de una computadora que puede manejarse con una instrucción única de un lenguaje de programación.

Autorización: Consentimiento precio, expreso e informado del titular para llegar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generado por el Responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que serán aplicadas, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar los a los datos personales.

Base de Datos: Conjunto organizado de datos.

Clave: Contraseña, clave o password es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquello a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave, si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso. En ocasiones clave y contraseña se usan indistintamente.

Capacity Planning: Es el proceso para determinar la capacidad de los recursos de las plataformas tecnológicas que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Confidencial: Significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

Control: Una forma para manejar el riesgo, incluyendo políticas, procedimientos, guías estructuras organizacionales, buenas prácticas y que pueden ser de carácter administrativo, técnico o legal.

Correo electrónico Institucional: Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por la Secretaría jurídica Distrital, para los funcionarios, contratistas y prácticas autorizados para su acceso. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

Cuenta Institucional: Cuenta de la entidad que no hace referencia al nombre de un usuario si no de un área, grupo o de acuerdo a una necesidad.

Custodio de la Información: Es el encargado de la administración de seguridad de información, es el responsable de promover la seguridad de información en toda la entidad con el fin de incluirla en el planteamiento y ejecución de los objetivos institucionales.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato personal público: Toda información personal que es de conocimiento libre y abierto para el público en general.

Dato personal privado: toda la información personal que tiene conocimiento restringido, y en principio privado para el público en general.

Dato público: Es el dato que no sea semiprivado, probado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a si profesión u oficio ya su calidad de comerciante o de servidor público, por su naturaleza, los datos públicos pueden estar contenidos entre otros en registros públicos documentos públicos, boletines oficiales y sentencias judiciales que no tenga reserva.

Dato sensible: Aquellos que afectan la intimidad del titular o cuyo uso indebido genere discriminación racial, orientación política, convicciones sociales, morales o fisiológicas, la pertenencia a sindicatos, organizaciones sociales de derechos humanos o partidos políticos, así como los datos relativos a la salud, a la vida sexual y datos biométricos.

Declaración de aplicabilidad: Listado de que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la entidad, tras el resultado del proceso de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27011.

Disponibilidad de la información: La disponibilidad es la característica, cualidad o condición de la información de encontrarse disposición de quienes deben acceder a ella, ya sean

personas, proceso o aplicaciones. A gros modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Disponibilidad de Documento electrónico: Es la capacidad actual y futura de que tanto el documento como sus metadatos asociados pueden ser consultados, localizados, recuperados, presentados, interpretados, legibles y por tanto estar en condiciones de uso.

Dispositivo Móvil: Se entiende por todo dispositivo incluido dentro del concepto de movilidad, debido a que es portable y utilizable durante su transporte. Dentro de estos dispositivos se incluyen: teléfonos celulares, Smartphone, computadores portátiles, tabletas, etc.

Documento electrónico: Se define como la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

Escritorio Limpio: Protección de los papeles y dispositivos removibles de almacenamiento de información, almacenado y manipulado en los equipos de cómputo de acceso no autorizados, perdida o daño de la información.

Estrategia de Gobierno Digital: Estrategia definida por el Gobierno Nacional que busca apoya y homologar los contenidos y servicios ofrecidos por cada una de las entidades públicas para el cumplimiento de los objetivos de un Estado más eficiente, transparente y participativo, donde se presten servicios más eficientes a los ciudadanos a través del aprovechamiento de las tecnologías de información.

Evento de Seguridad de la Información: Se considera un evento de Seguridad de la información a cualquier situación identificada que indique una posible brecha en las políticas de seguridad o falla en los controles y/o protecciones establecidas.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgos dados para determinar la importancia del riesgo.

Gestión de incidentes de seguridad de la información: proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Habeas Data: Derecho de una persona a conocer, actualizar y rectificar las informaciones que se tenga sobre ellas en el banco de datos y en archivos de datos de entidades públicas o privadas.

Incidente de Seguridad de la Información: Se considera un incidente de seguridad de la información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, l plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Información: Se refiere a u conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligada en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá se negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privadas consagradas en el artículo 18 de esta Ley.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta Ley.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.}

Intranet: Una Intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

Lugar seguro: Es aquel que protege el activo de información de acceso de personas no autorizadas de manera oportuno.

Malware: El malware es la descripción general de un programa informático que tiene efectos o maliciosos, incluye virus, gusanos troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación como el correo electrónico y la mensajería instantánea y medios magnéticos extraíbles, como dispositivos USB.}

Mecanismos de bloqueo: Son los mecanismos necesarios para impedir que los usuarios, tanto de los sistemas de información como los servicios, tengan acceso a estos sin previa autorización, ya sea por razones de seguridad, falta de permisos, intentos malintencionados o solicitud de los propietarios de la información.

Memoria USB: La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar la información.

Mensajería Instantánea Institucional: Comúnmente conocido como CHAT es un canal de comunicación provisto por la Secretaría Jurídica Distrital para facilitar una forma de comunicación en tiempo real entre los funcionarios, contratistas y practicantes autorizados creando un espacio virtual de encuentro especifico.

Mensajes de datos: Información generada, enviada, recibida, almacenada, comunicada por medios electrónicos, ópticos o similares, entre otros. Por lo general, se extiende a comunicaciones efectuadas mediante intercambio electrónico de datos EDI, telegrama, telefax.

Oficial de Seguridad: Es el responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información.
Pantalla limpia: Protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en estaciones de trabajo, de accesos no Autorizados, pérdida o daño de la información.

Phishing: Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas de WEB falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial.

Plan de Continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o críticas del negocio en el caso de un evento improvisto que las ponga en peligro.

Plan de Tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Política: Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación y que guíen el desarrollo de reglas y criterios específicos sobre situaciones concretas. Las políticas deben ser apoyadas y aprobadas por las directivas de la entidad son de obligatorio cumplimiento.

Propietario de la Información: En tecnologías de la información y la comunicación (TIC) es el responsable de preservar y disponer de la información de acuerdo a los lineamientos de la entidad.

Puntos de entrada y salida: Cualquier dispositivo (distinto de la memoria RAM) que intercambie datos con el sistema lo hace a través de un "puerto", por esto se denominan también puertos de E/S ("I/O ports"). Desde el punto de vista del software, un puerto es una interfaz con ciertas características; se trata por tanto de una abstracción (no nos referimos al enchufe con el que se conecta físicamente un dispositivo al sistema), aunque desde el punto

de vista del hardware, esta abstracción se corresponde con un dispositivo físico capaz de intercambiar información (E/S) con el bus de datos.

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el tratamiento de los datos.

Seguridad de la Información: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

SGSI: La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Sistemas de Información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE).

Tecnología de la información T.I.: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Transferencia: La transferencia de datos tiene lugar cuando el responsable o encargado del tratamiento de datos personales ubicado en la entidad, envía la información o los datos personales a un receptor que es el responsable del tratamiento de los datos y se puede encontrar al interior o exterior de la entidad.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Usuario de la información: Para la informática es un usuario aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos. A menudo es un usuario aquel que adquiere una computadora o dispositivo electrónico y que lo emplea para comunicarse con otros usuarios, generar contenido y documentos, utilizar software de diverso tipo y muchas otras acciones posibles. El usuario no es necesariamente uno en particular instruido o entrenado en el uso de nuevas tecnologías, ni en programación o desarrollo, por lo cual la interfaz del dispositivo en cuestión debe ser sencilla y fácil de aprender. Sin embargo, cada tipo de desarrollo tiene su propio usuario modelo y para algunas compañías el parámetro de cada usuario es distinto.

4. MARCO LEGAL Y/O NORMATIVO

ACTO ADMINISTRATIVO	OBJETO
Constitución Política de Colombia de 1991	Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
Ley 23 de 1982	Derechos de Autor.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000	Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Ley 603 de 2000	Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
Ley 962 de 2005	Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150 de 2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009|	Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Decreto 2952 de 2010	Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.
Decreto 2364 de 2012	Firma Electrónica.
Decreto 2609 de 2012	Expediente electrónico.
Ley Estatutaria 1581 de 2012	Entró en vigencia la Ley 1581 del 17 de octubre 2012 de Protección De Datos Personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional. Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y

	reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.
Decreto 1377 de 2013	Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012.
Decreto 2573 de 2014	Establece como lineamiento la Seguridad y privacidad de la información y comprende acciones transversales además de componentes enunciados, a proteger la información y sistemas de información del acceso, divulgación, interrupción o destrucción no autorizada.
Circular 16 de 2016	CONPES 3854 Política Nacional al de Seguridad.
Circular 28 de 2016	Levantamiento de información infraestructura Seguridad Informática.
Circular 01 de 2017	Lineamiento de Avance del Modelo de Seguridad de la Información.
Circular 37 de 2018	Incidentes de ciberseguridad y modelo de seguridad y privacidad de la información MPSI del MINTIC.
Circular 60 de 2018	Presentación estudios Seguridad y Privacidad de la Información para las entidades del Distrito dirigida a directores de TI, Oficiales de Seguridad de la Información, Jefes de Oficinas de Planeación, Jefes de Oficina de Jurídica y Jefes de Oficina Control Interno.
Código Penal	Art. 199. Espionaje Art. 258. Utilización indebida de información Art. 418. Revelación de Secreto Art. 419. Utilización de asunto sometido a secreto o reserva Art. 420. Utilización indebida de información oficial Art. 431. Utilización indebida de información obtenida en el ejercicio de la función pública Art 463. Espionaje
. ISO 27002:2005	Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.

NTC 27001:2006	Sistema de Gestión de Seguridad de la Información (SGSI). En 2005, con más de 1700 empresas certificadas en BS7799-2, ISO publicó este esquema como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799 y esta última norma se denomina ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de revisión.

5. POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.

5.1. Creación de Políticas

En la Secretaría Jurídica Distrital las políticas son creadas por la oficina de Tecnologías de la Información y Comunicaciones, que es la encargada de la seguridad y privacidad de la información, estas son respaldadas y aprobadas por la Alta Dirección de la entidad.

Las políticas de seguridad de la información se encuentran escritas de forma clara, sencilla y específica. Las políticas de Seguridad de la información que contempla la norma son:

a. Política de Seguridad de la Información
b. Política para dispositivos móviles
c. Política de Control de Acceso
d. Política sobre el uso de controles criptográficos
e. Política de escritorio Limpio y Pantalla limpia
f. Políticas y procedimientos de transferencia de Información
g. Política de desarrollo seguro
h. Política de Seguridad de la Información para la relación con los proveedores

5.2. Política de Seguridad de la Información

La Seguridad de la Información es una prioridad para la Secretaría Jurídica Distrital, por lo tanto, es responsabilidad de todos los funcionarios y contratistas de la Entidad velar por el continuo cumplimiento de la Política de Seguridad de la Información http://secretaria.juridica.gov.co/transparencia/atención-cidadano/políticas

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Organización Interna

La Secretaría jurídica Distrital garantiza el soporte operativo para las actividades de la Información, para ello debe mantener un esquema de seguridad de la información en donde existan roles y responsabilidades que consideren actividades de administración, operación y gestión de la información.

6.1.1. Roles Y Responsabilidades

ROL	RESPONSABILIDADES
Secretaria Jurídica Distrital	Aprobación y Verificación del cumplimiento de las políticas de seguridad de la información. Hacer que los miembros del Comité Directivo sean conscientes de la criticidad de los activos de información. Divulgar las responsabilidades de seguridad de la información.
Nivel Directivo	Liderazgo y apoyo continúo para la aplicación del SGSI. Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguida de la información para los roles definidos en cada área (Gestores de Calidad). Proveer los recursos necesarios para la implantación del SGSI. Aplicar la capitación y entrenamiento. Aplicar el proceso disciplinario ante los incidentes de seguridad de la información originado por un funcionario del área correspondiente.
Oficial de Seguridad	Es responsable por el SGSI, reportando al nivel directivo. Definición, actualización y mantenimiento de los activos de información. Análisis de riesgos de seguridad de la información.

	Definición del Plan de tratamiento de riesgos. Definición y generación de métricas de seguridad de información. Definición de planes de entrenamiento y sensibilización para funcionarios.
Comité Operativo de Seguridad de la información	Validar la documentación propia del SGSI en cada dueño del proceso. Apoyar la identificación y actualización de activos y riesgos de seguridad de la información. Apoyar la identificación de controles para la mitigación de riesgos de la información.
Propietario del Activo	Gestión requerida para la que la entidad asigne los recursos necesarios para la implementación de los controles definidos en el SGSI protegiendo la Confidencialidad, Integridad y Disponibilidad de la información del activo. Actualización permanente de la información del activo Implementación de controles definidos en el SGSI para la protección del activo.
Custodio del Activo	Comunicación permanente con el Propietario del active para generar reportes de los resultados de la aplicación de los controles. Hacer cumplir la Política de Uso Aceptable del Activo. Reporte inmediato e incidentes de seguridad de la información.
Funcionarios	Serán responsables del cumplimiento de las políticas, procedimientos y estándares definidos por la Entidad. Responsable de proteger la integridad, confidencialidad y disponibilidad de la información de la entidad. Deben mantener especial cuidado de no divulgar información CONFIDENCIAL o RESERVADA en lugares

	públicos o privados, mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la organización.
Contratistas, proveedores y terceros	Serán responsables del cumplimiento de las políticas, procedimientos y estándares definidos por la Entidad. Responsable de proteger la integridad, confidencialidad y disponibilidad de la información de la entidad.

6.1.2. Contacto con las Autoridades

La Secretaría Jurídica Distrital debe mantener contacto con todas las entidades que representan autoridad en temas de seguridad de la información con el fin de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, se mantendrán contactos con las siguientes entidades especializadas en temas relativos a la seguridad de la información:

MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones (y particularmente con:

FIRST – Forum of Incident Response and Security Teams. (www.first.org).
Es la primera organización global reconocida en respuesta a incidentes, tanto de manera reactiva como proactiva. Reúne una variedad de equipos de respuesta de incidentes de seguridad informática para las entidades gubernamentales, comerciales y académicas.

COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia. (http://www.colcert.gov.co/).
Tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual está enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia. (http://www.cert.org.co/). CSIRT-CCIT es un centro de coordinación de atención a incidentes de seguridad informática colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas. En conclusión, el

CCP – Centro Cibernético Policial. (http://www.ccp.gov.co/). El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

SIC: Superintendencia de Industria y Comercio. A la Superintendencia de Industria y Comercio, corresponde la Protección de la Competencia, Propiedad Industrial, Protección.

6.1.3. Contactos con Grupos de Interés Social

La Secretaría Jurídica Distrital, mantendrá contactos apropiados con grupos de interés especiales, otros foros especializados y asociaciones de profesionales en seguridad de la información, con el fin de estar actualizado en temas de seguridad de la información (Alta Consejería, Oracle etc.

Oficina de la Alta Consejería de las TIC Secretaria General- Alcaldía Mayor de Bogotá	María del Pilar Niño	Tel 3813000 Ext 3061
Oracle de COLOMBIA Transversal- Calle 127 A No.53 45 Torre 2 Piso 9	Jairo Espejo	Tel 6119600
Ministerio de Tecnologías de la Información. Edificio Murillo Toro	Ivonne Johana Univio	Tel 3443460

6.1.4. Seguridad de la Información en Gestión de Proyectos

La Secretaría Jurídica Distrital integrará la Seguridad de la Información al desarrollo de cualquier tipo de proyecto de la entidad y en el desarrollo de los proyectos se deben definir las responsabilidades, para asegurar que los riesgos de seguridad de la información se identifiquen y se traten como parte de un Proyecto, se debe incluir una identificación y evaluación de los mismos, para los cuales se deben definir controles de seguridad que aporten a su mitigación.

En las etapas iníciales de un proyecto como parte de los riesgos asociados al proyecto, se debe incluir una identificación y evaluación de riesgos de seguridad de la información, para los cuales se deben definir controles de seguridad que aporten a su mitigación.

Como parte de los objetivos definidos para los proyectos desarrollados, se deben incluir objetivos de seguridad de la información acordes con la información que se va a manejar a lo largo del proyecto.

La responsabilidad sobre la implementación y la efectividad de los controles de seguridad aplica sobre el gerente de proyectos o supervisor del contrato de implementación.

En la metodología de gestión de proyectos empleada por el Secretaría Jurídica Distrital se considera la seguridad de la información como un componente transversal y por lo tanto es incluida desde el inicio del proyecto hasta la finalización del mismo.

6.2 Política de Dispositivos Móviles y Teletrabajo

La Secretaría Jurídica garantiza la seguridad de Teletrabajo y el uso de dispositivos móviles.

6.2.1. Política para dispositivos móviles

La Secretaría Jurídica Distrital, controla, gestiona y aprueba el manejo de los dispositivos móviles (teléfonos inteligentes, portátiles, discos duros, USB, DVD) institucionales que hagan uso de los sistemas de información y/o equipos de la entidad. (El acceso a los medios informáticos será expresamente autorizado por el Jefe de Tecnologías de la Información y las Comunicaciones).

El Ingeniero designado por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones TIC, debe activar la opción de cifrado por los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el desbloqueo.

El ingeniero designado de la Oficina de Tecnologías de la Información y las Comunicaciones TIC debe garantizar las copias de seguridad de la información contenida en los dispositivos móviles institucionales.

Los usuarios de los dispositivos móviles institucionales, deben evitar el uso de los mismos en lugares que no les ofrezcan garantías de seguridad física para evitar pérdida o hurto.

Los usuarios de los dispositivos móviles institucionales, no deben modificar las configuraciones de seguridad, ni desinstalar software o instalar programas en los dispositivos móviles institucionales bajo su responsabilidad.

Al conectar un dispositivo móvil a la red de la SJD, el propietario del dispositivo acepta las políticas definidas en el presente manual.

6.2.2. Teletrabajo

La Secretaría Jurídica Distrital, controla gestiona y aprueba el Teletrabajo, de acuerdo a la Ley 1221 de 2008, la Oficina de Tecnologías de la Información y las comunicaciones designará un técnico con el fin de que realice la inspección técnica a los puestos de trabajo con el fin de garantizar que la comunicación sea eficiente, a los funcionarios que diga la Dirección de Gestión Corporativa.

En la modalidad de teletrabajo se debe velar por garantizar la seguridad de la información, tanto de los equipos como de los teletrabajadores. Estos últimos trasladan numerosos datos y contenidos a dispositivos electrónicos con nuevas ubicaciones físicas generando nuevos riesgos que se deben mitigar estableciendo protocolos adecuados. Tales políticas de seguridad se establecen como planes de acción encargados de afrontar, mitigar y prevenir los riesgos originados con la implementación del teletrabajo.

Con relación a la información, dado que esta se considera como el recurso intangible de mayor importancia, es necesario que a fin de prevenir cualquier anomalía se establezcan servicios de antivirus, respaldo o backup, acceso seguro a través de VPN (Virtual Private Network - Red Privada Virtual) y acceso restringido a aplicaciones. Por otro lado, la definición de las políticas de seguridad debe garantizar:

- Confidencialidad: asegurar el acceso a la información únicamente por las personas autorizadas, que son los teletrabajadores.
- Integridad: mantener los datos libres de modificaciones no autorizadas.
- Disponibilidad: garantizar que la información esté en disposición para los teletrabajadores en cualquier momento, de tal forma que puedan desarrollar sus actividades.
- Autenticación: identificar al usuario generador de la información.

De igual forma como se debe propender por reducir las amenazas relacionadas con los recursos intangibles, también se deben establecer los procedimientos relacionados con la protección de los recursos tangibles a través de un análisis de riesgos ocasionados por la implementación de teletrabajo, como por ejemplo establecer procesos de manejo de equipos, pólizas de seguros, mantenimiento de equipos, entre otros.

Se considera conveniente que se establezcan patrones de seguridad adecuados con la implementación del teletrabajo contemplando objetivamente tanto las necesidades de la entidad como las del teletrabajador, así como se consideren los posibles riesgos exógenos y endógenos que realmente pueden afectar el desarrollo de las labores del teletrabajador.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

La Secretaría Jurídica Distrital debe proteger la información por medio de la validación y concientización del recurso humano que hará uso de la misma.

7.1. Selección de personal

Dentro de los procesos de contratación de personal o prestación de servicios se deberá realizar, la verificación de antecedentes cuando así lo amerite y en los casos que se considere necesario, se realizar el estudio de seguridad del personal que va a ingresar a laborar en la entidad.

La Dirección Corporativa es el área encargada de realizar la verificación de los antecedentes, de estudios, de experiencia, de referencia laborarles y revisar que estén acordes con los estudios previos.

7.1.1. Términos y condiciones Laborales

Los funcionarios de la Secretaría Jurídica Distrital deben cumplir con los requerimientos de seguridad de la información, deben conocer y aceptar la Política de Seguridad de la Información y Protección de Datos que la encuentra en:
http://secretaria.juridica.gov.co/transparencia/atención-cidadano/políticas

Es importante anotar que en los contratos debe existir una cláusula en la que se garantice la confidencialidad e integridad de la información que ellos manejen. Así mismo cumplir con la cláusula de Derechos de Autor de acuerdo con el artículo 20 de la Ley 23 de 1982, modificado pro el artículo 28 de la Ley 1450 de 2011.

7.2. Durante la ejecución del empleo

Los funcionarios de la Secretaría Jurídica Distrital son entrenados y capacitados para las funciones/actividades y cargos a desempeñar con el fin de proteger adecuadamente los recursos y la información de la entidad. Esta capacitación o reinducción será responsabilidad de la Dirección de Gestión Corporativa.

7.2.1. Responsabilidad de la Dirección

Garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá extenderse al personal de contratistas o terceros, cuando sus responsabilidades así lo exijan.

7.2.2. Toma de conciencia, educación y formación del Seguridad de la Información.

Los funcionarios de la Secretaría Jurídica Distrital son entrenados y capacitados para las funciones/actividades y cargos a desempeñar con el fin de proteger adecuadamente los

recursos y la información de la entidad. Esta capacitación o reinducción será responsabilidad de cada Director o Jefe de la respectiva dependencia o a quien asigne para esta actividad.

Garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá extenderse al personal de contratistas o terceros, cuando sus responsabilidades así lo exijan.

7.2.3 Proceso Disciplinario

A todos los incidentes de seguridad de la información ocurridos en la Secretaría Jurídica Distrital, se le debe dar el tratamiento respectivo con el fin de determinar sus causas y responsables.

De los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta la gravedad y responsabilidades identificadas, se tomarán acciones y se realizará el respectivo trámite ante las instancias correspondientes. La Dirección Distrital de Asuntos Disciplinarios será la encargada de investigar y se ser necesario iniciar el Proceso Disciplinario de acuerdo a la información enviada por la Oficina de TIC.

7.3. Política de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios y personal provisto por terceros

La Dirección de Gestión Corporativa debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la entidad llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Cada Supervisor de Contrato, Director y Jefe de Oficina debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a la Dirección de Gestión Corporativa.

La Dirección de Gestión Corporativa debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a la Oficina de Tecnologías de la Información y las Comunicaciones.

Se debe informar al colaborador saliente la continuidad de los acuerdos de confidencialidad, que debe ser mantenida de acuerdo con la sensibilidad o criticidad de la información a la que haya accedido o que estaba siendo manipulada durante la prestación de sus servicios.

En caso de que el equipo de cómputo empleado sea propiedad del colaborador se deberán utilizar los métodos tecnológicos apropiados para garantizar su completa transferencia y eliminación de la información entregada, labor que realiza el ingeniero designado por la Oficina de Tecnologías de la Información y Comunicaciones.

8. GESTIÓN DE ACTIVOS

8.1. Responsabilidad

La Secretaria Jurídica Distrital, con el fin de contribuir a la protección de los activos de la Entidad, elaboró un Registro de Activos de Información identificando propietario y custodios designados por la entidad.

8.1.2. Propiedad

Los propietarios de los activos de información son responsables de establecer y revisar periódicamente las restricciones y privilegios de acceso lógico y físico de proveedores, contratistas y los usuarios.

El Propietario de un activo de información es responsable de validar que los activos a su cargo cuenten con los controles requeridos para preservar los objetivos de legalidad, finalidad, integridad, confidencialidad y disponibilidad.

El propietario de cada activo de información es responsable de actualizar periódicamente la valoración e información de los mismos a su cargo, determinando y comprobando las necesidades del control, manteniéndolos actualizados en el Sistema de Medición, Análisis y Mejora para la Toma de Decisiones - SMART.

8.1.3 Política de Uso Aceptable de los Activos

Los usuarios, son responsables de un adecuado y racional uso de los activos de información que se usan en los procesos de la Secretaría Jurídica Distrital, es decir, no se pueden usar para propósitos diferentes para los cuales fueron definidos o para temas personales.

Los usuarios, aceptan no compartir las contraseñas o permitir el acceso no autorizado a las cuentas otorgadas para utilizar los servicios brindados por la Entidad, así mismo es responsable por el manejo adecuado de la información y las acciones que por mal uso se deriven de esos accesos.

Los datos de acceso, son un elemento personal e intransferible, los usuarios asumen la responsabilidad sobre el buen o mal uso que se dé sobre los sistemas de información de la entidad.

La información de la entidad, debe ser respaldada de forma frecuente y de acuerdo a las políticas de backups definidas y su almacenamiento debe estar en un lugar apropiado y adecuado, en los cuales se garantice que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes presentados.

La Secretaría Jurídica clasifica la información en: información pública, de uso interno, restringido y reservado.

8.1.4. Devolución de los Activos

Todo activo de propiedad de la Secretaría Jurídica Distrital, asignado a un funcionario de la entidad o a un tercero, deberá ser entregado al retirarse o por cambio de cargo de los funcionarios o a la finalización del contrato. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.

8.2. Clasificación de la Información

La Secretaría Jurídica Distrital debe asegurar que la información es tratada y protegida adecuadamente de acuerdo al nivel de clasificación otorgado. La información física es clasificada de acuerdo a las tablas de retención documental de la entidad.

8.2.1. Esquema de Clasificación

Toda Información perteneciente a la Secretaría Jurídica Distrital deberá ser identificada y clasificada de acuerdo a los siguientes niveles:

1. Público
2. Uso Interno
3. Confidencial
4. Reservado

La Oficina de Tecnologías de la Información y Comunicaciones en conjunto con la Oficina Asesora de Planeación y la Oficina de Gestión Documental, son los responsables de definir las directrices de clasificación de la información y las medias de tratamiento o manejo que deben darse de acuerdo al nivel de clasificación al que pertenecen.

Para ello se debe tener en cuenta:

1. Restringir el acceso solo al personal debidamente autorizado
2. Mantener un registro formal de los receptores autorizados da datos o información
3. Conservar los medios de almacenamiento seguro.

8.2.2. Etiquetado y Manejo de la Información

El nivel de confidencialidad requerido para la información tratada por la Secretaría Jurídica Distrital, debe estar marcado en todas las páginas que contengan información confidencial y/o sensible y siempre de forma que resulte fácilmente legible.

Cada funcionario de la entidad deberá mantener organizado el archivo de gestión, acatando los lineamientos establecidos por la Dirección de Corporativa - Gestión Documental.

Los Directores, Jefes de Oficina deberán establecer mecanismos para el control de la reprografía de los documentos, con el fin de mantener la integridad y confidencialidad de la información.

Los funcionarios de la Secretaría Jurídica Distrital son responsables de la Organización, conservación, uso y manejo de los Documentos.

Las diferentes dependencias de la Secretaría Jurídica Distrital deberán enviar al Archivo Central la documentación en forma ordenada y organizada, de acuerdo a los tiempos de vigencia estimados en la Tabla de Retención documental de la entidad, acompañada del documento formato utilizado para realizar las Transferencias documentales, y en medio magnético.

El Archivo Central recibirá las transferencias documentales de acuerdo al calendario anual de transferencias documentales.

Los archivos de gestión de las dependencias u oficinas de la entidad, deberán custodiar sus documentos de acuerdo a lo especificado en la correspondiente tabla de Retención Documental.

La tecnología utilizada para salvaguardar, facilitar y conservar la información de los documentos en soportes informáticos debe garantizar la seguridad de no permitir alteraciones o consultas de personas no autorizadas.

8.3. GESTIÓN DE MEDIOS DE ALMACENAMIENTO

La Secretaría Jurídica Distrital protege toda la información que se encuentra en unidades de almacenamiento evitando posibles afectaciones a su confidencialidad, integridad y disponibilidad.

8.3.1. Gestión de Medios Removibles

Los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD’s, DVD’s, dispositivos personales “USB”, discos duros externos, IPod’s, cámaras fotográficas, cámaras de video, celulares, entre otros, estarán controlados en cuanto a su acceso y uso como medio de almacenamiento.

La información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles, debe cumplir con las disposiciones de seguridad indicadas por la

Oficina de Tecnologías de la Información y las Comunicaciones, específicamente aquellas referentes al empleo de técnicas de cifrado.

La Oficina de Tecnologías de la Información y las Comunicaciones puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de la Secretaría Jurídica Distrital o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción conducente a evitar la fuga de información de la Secretaría Jurídica Distrital por medio de medios removibles.

Los medios de almacenamiento removibles que se conecten a los equipos de cómputo que sean propiedad de la Secretaría Jurídica Distrital o que estén bajo su custodia, pueden estar sujetos a monitoreo por parte de la Oficina de Tecnologías de la Información y las Comunicaciones.

El retiro de medios de almacenamiento de las instalaciones de la Secretaría Jurídica Distrital, tales como discos duros externos, está sujeto a la aprobación del propietario del proceso misional, estratégico o de apoyo, definidos de acuerdo al mapa de procesos de la Secretaría Jurídica Distrital.

Los medios de almacenamiento removibles deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante. Adicionalmente, se debe hacer seguimiento al deterioro que sufren los medios de almacenamiento para garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible.

8.3.2. Transferencia de Medios de soporte físicos

La información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles y estos sean transportados fuera de las instalaciones de la Secretaría Jurídica Distrital, debe cumplir con las disposiciones de seguridad indicadas por la Oficina de Tecnologías de la Información y las Comunicaciones, específicamente aquellas referentes al empleo de técnicas de cifrado.

En el caso de que los medios físicos se transporten utilizando los servicios de una empresa transportadora, se deben tomar las precauciones necesarias para garantizar que los medios de almacenamiento sean transportados con precaución para evitar una afectación a la

integridad y usabilidad del medio de almacenamiento y asegurar que se identifica adecuadamente al funcionario de la empresa transportadora responsable de la recepción y/o entrega del medio de almacenamiento.

9. CONTROL DE ACCESO

9.1 Política de Control de Acceso

La Secretaría Jurídica Distrital propende por limitar el acceso a información y a sus instalaciones de procesamiento de información (centro de cómputo) con fines de protección de datos personales, seguridad de la información y continuidad del negocio.

La Oficina de Tecnologías de la Información y las Comunicaciones, validara todo acceso a nivel de red, sistemas operativos, bases de datos y aplicaciones. Los controles asociados al Sistema de Gestión de Seguridad y Privacidad de la información deben estar soportados por una cultura de riesgos y seguridad.

Limitar el acceso a la información de la entidad al mínimo requerido (principio del mínimo privilegio), para la realización de los roles o funciones.

Identificar de manera inequívoca cada parte interesada y hacer un seguimiento periódico o aleatorio de las actividades que estos realizan para la entidad.

La Oficina de Tecnologías de la Información y las Comunicaciones definirá los lineamientos para la configuración de contraseñas seguras que aplicarán sobre los usuarios en todos los sistemas de información.

Cada dueño de proceso o dependencia deberá realizar la solicitud a la Oficina de Tecnologías de la Información y las Comunicaciones para crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información de la entidad, acorde con el procedimiento establecido por el SGSI.

No están autorizadas en compartir sus cuentas de usuario y contraseñas con otros usuarios, por lo que, si se detecta esta situación, será gestionado como un incidente de seguridad de la información y con las sanciones pertinentes.

La Secretaría Jurídica Distrital, utiliza identificadores de usuario (ID) únicos para permitir la trazabilidad de acciones generadas por los colaboradores y evitar la existencia de identificadores relacionados a múltiples servidores o proveedores.

Los controles de acceso deberán contemplar:

1. Requerimientos de seguridad de cada una de las aplicaciones.
2. Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo al perfil.

La Oficina de Tecnologías de la Información y las Comunicaciones establece procedimientos para controlar las asignaciones de derechos de acceso a los diferentes sistemas de la entidad.

La Oficina de Tecnologías de la Información y las Comunicaciones, debe mantener los registros de cada uno de los líderes responsables de los procesos a los que haya autorizado, igualmente el de terceros.

Los datos de acceso a los sistemas de información deben estar compuestos por un ID o nombre del usuario y una contraseña.

Cuando se retire o cambie de contrato cualquier funcionario o contratista, se debe aplicar la eliminación o cambios de privilegios en los sistemas de información a los que estaba autorizado, todo esto lo realiza el Ingeniero de Sistemas designado.

Las contraseñas de acceso deben cumplir con un mínimo de 8 caracteres, deben tener combinación de números, mayúsculas minúsculas y caracteres especiales.

Las contraseñas se deben cambiar cada tres meses y esto se realizará de forma automática, es decir si el usuario no la cambia en la fecha establecida, no podrá ingresar al sistema y debe comunicarse con el Ingeniero de sistemas de la Oficina TIC.

Cuando un funcionario o contratista vaya a iniciar sesión, o intente entrar a los sistemas de información se bloquean de forma permanente, si el usuario realiza 5 Intentos fallidos, por lo tanto, debe comunicarse con el Ingeniero de sistemas de la Oficina TIC.

Los usuarios del sistema y de los diferentes aplicativos deben cumplir con:

1. Mantener los datos de acceso en secreto
2. Contraseñas fáciles de recordar y difíciles de adivinar
3. Notificar de acuerdo a los establecidos cualquier incidente de seguridad relacionado con la contraseña, como olvido o indicio de pérdida de confidencialidad.

Los usuarios deben:

1. Bloquear el equipo cada vez que se retire del puesto de trabajo
2. Bloqueo automático si la inactividad es superior a cinco minutos
3. Apagar el equipo al finalizar la jornada laboral.

9.1.2. Acceso a redes y servicios en red

La Secretaría Jurídica Distrital suministra a los usuarios las claves respectivas para el acceso a los servicios de red y de sistemas de información a los que haya sido autorizado, es importante recordar que son de uso personal e intransferible.

El servicio de correo electrónico debe ser utilizado exclusivamente para actividades laborales, la navegación en internet deber ser monitorea por la Oficina de TIC, y el tiempo está definido de acuerdo a los privilegios asignados por la misma.

Para tener acceso a cualquier red inalámbrica de la entidad los funcionarios, contratistas o terceros deben:

1. Conectarse a través de protocolos seguros
2. Acceder mediante la asociación de las direcciones MAC de los portátiles y las direcciones IP asignadas.
3. La autenticación de los usuarios remotos debe ser aprobada por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones
4. Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

Para mantener la seguridad en los servicios de Red solo se deben mantener instalados y habilitados los que sean utilizados por los sistemas de información de la entidad.

El Ingeniero designado por la Oficina de Tecnologías de la Información y Comunicaciones controla el acceso lógico a los servicios, tanto de uso como de administración mediante el bloqueo de puertos en el firewall.

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores, administradores de bases de datos) tendrán un identificador ID y existe un proceso de autenticación que valida los usuarios.

9.2. GESTION DE ACCESO A USUARIOS

9.2.1. Registro y Cancelación de Usuarios

La Secretaría Jurídica, debe controlar el acceso a los sistemas y servicios de información estableciendo un procedimiento de novedades de los usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información.

Se debe mantener evidencia de cambios realizados a los identificadores de usuario (ID), perfiles y estado de las cuentas de usuario.

Se debe retirar o bloquear inmediatamente los derechos de acceso a los funcionarios y/o contratistas que cambian de funciones o responsabilidades, de aquellos a los cuales se revoca la autorización de acceso, vinculación contractual o sufren pérdida o robo de credenciales de acceso.

Se deben efectuar revisiones periódicas a los Identificadores de Usuarios (ID) identificando y cancelando cuentas redundantes o inactivas y comprobando la integridad de accesos modificados por las novedades de usuario reportadas.

9.2.2. Suministro de Acceso a Usuarios

Cada uno de los Directores, jefes de Oficina de la entidad debe aprobar el acceso a los sistemas de información que le competen, de acuerdo con la matriz de roles y perfiles establecida para los usuarios y validada por la Oficina de TIC.

El administrador de cada sistema de información monitorear periódicamente los roles y perfiles definidos y los privilegios asignados a los usuarios y si necesitan realizar alguna modificación deben solicitarlo a la Oficina de TIC.

La Oficina de TIC debe mantener un registro de todos los privilegios asignados y debe establecer un periodo de vigencia para el mantenimiento de los privilegios basados en la utilización de los mismos.

Los privilegios especiales de administrador del sistema se otorgan solo a los responsables de la infraestructura tecnológica.

9.2.3. Revisión de los Derechos de Acceso a Usuario

La Oficina de Tecnologías de la Información y Comunicaciones debe revisar periódicamente el acceso a los usuarios de información que fueron asignados para saber qué cambios se realizaron.

9.2.4. Cancelación o ajuste a los derechos de usuario

La Dirección de Corporativa es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo a la Oficina de Tecnologías de la Información y las Comunicaciones. Cuando se solicite una cuenta institucional se debe justificar e informar de la persona responsable de dicho buzón. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella, la Oficina de Tecnologías de la Información y las Comunicaciones podrán eliminar dicha cuenta.

Los funcionarios, en el desarrollo de sus tareas habituales u ocasionales que utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que provea el Secretaría Jurídica Distrital, son responsables del cumplimiento y seguimiento de esta política.

9.3. RESPONSABILIDAD DE LOS USUARIOS

Los funcionarios y contratista son responsables del usuario asignado y de su contraseña, por lo tanto, cualquier acción que se realice utilizando su usuario es responsabilidad del funcionario o contratista.

Las contraseñas son de uso personal e intransferible, deben estar compuestas por 8 caracteres, incluido mayúsculas. Minúsculas y caracteres especiales.

Los usuarios deben cambiar su contraseña la primera vez que se usen las cuentas asignadas igualmente lo deben hacer cada que el periodo este próximo a vencer, ya que una vez pasado el tiempo dado por la Oficina de TIC, se bloqueara automáticamente.

9.3.1. Uso de Información Secreta

La Secretaría Jurídica Distrital debe utilizar una herramienta o software de administración de usuarios para cada sistema de información, la (el) cual se debe configurar para que todas las contraseñas cumplan con las características de complejidad y longitud definida por la Oficina de Tecnologías de Información y Comunicaciones.

La Oficina de Tecnologías de la Información y Comunicaciones debe definir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuarios, el cual debe tener:

1. Identificadores de usuarios únicos de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo funcionario.
2. Verificar que el usuario tiene autorización del propietario de la información para el uso del sistema, base de datos o servicios de información.
3. Mantener un registro formal de todas las personas registradas para utilizar el servicio.
4. Cancelar inmediatamente los derechos de acceso a los usuarios que cambiaron sus tareas o aquellos a los que se les revoco la autorización, o se desvincularon.
5. Efectuar revisiones periódicas con el objeto de cancelar identificadores y cuentas de usuario redundantes, inhabilitando así las cuentas que estén inactivas por más de 30 días.

9.4. Control de Acceso y Aplicaciones

9.4.1. Restricción de Acceso a Información

La Oficina de Tecnologías de la Información y Comunicaciones, designara un Ingeniero que será el responsable de definir el acceso a la información a los usuarios de acuerdo al perfil que tenga asignado según los aplicativos que maneje.

9.4.2. Sistema de Gestión de Contraseñas

El Ingeniero asignado por la Oficina de Tecnologías de la Información y Comunicaciones 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:

1. Identificadores de usuarios únicos de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo funcionario.
2. Verificar que el usuario tiene autorización del propietario de la información para el uso del sistema, base de datos o servicios de información.
3. Mantener un registro formal de todas las personas registradas para utilizar el servicio.
4. Cancelar inmediatamente los derechos de acceso a los usuarios que cambiaron sus tareas o aquellos a los que se les revoco la autorización, o se desvincularon.
5. Efectuar revisiones periódicas con el objeto de cancelar identificadores y cuentas de usuario redundantes, inhabilitando así las cuentas que estén inactivas por más de 30 días.

10. CRIPTOGRAFIA

10.1. Controles Criptográficos

La Secretaría Jurídica Distrital debe proteger la confidencialidad, integridad y disponibilidad de la información por medio de técnicas criptográficas apropiadas.

Se contemplará la evaluación e implementación de controles criptográficos en la medida que un determinado servicio de procesamiento de información o acceso lo requiera. Se verificarán los medios y herramientas criptográficas que mejor se acoplen a las necesidades de la entidad.

Antes de la implementación del tipo de control criptográfico seleccionado, se debe definir y comunicar el procedimiento para la gestión de las llaves públicas o privadas, según el caso, entre las partes interesadas.

Las características de los controles criptográficos, incluyendo el tipo, fortaleza y calidad, al igual que las herramientas y mecanismos a emplear para implementar los controles, serán definidas por la Oficina de Tecnologías de la Información y las Comunicaciones en función de la clasificación de la información.

Se debe garantizar que el uso de controles criptográficos no entorpezca aquellos controles de seguridad basados en inspección de contenido, tales como filtrado web, antimalware, antispyware, etc. La Oficina de Tecnologías de la Información y las Comunicaciones deberá validar dicha condición y determinar las mejores condiciones de aplicabilidad de los controles criptográficos.

10.2. Gestión de Claves

El tamaño de las llaves criptográficas privadas y públicas debe proveer el nivel de seguridad requerido en La Secretaria Jurídica Distrital y estar alineadas con estándares internacionales y buenas prácticas.

Los instructivos para protección y control del ciclo de vida de las llaves criptográficas deben tener como mínimo la siguiente información: un identificador o consecutivo único para el control centralizado, tipificación y estado del certificado o llave criptográfica, identificación del emisor, identificación de propietario, fecha de emisión, fecha de revocación, propósito, limitaciones e identificación de recursos o servicios cubiertos.

Todas las llaves criptográficas de la entidad se deben proteger contra modificación, pérdida, divulgación o uso inadecuado.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

11.1. Áreas Seguras

La Secretaría Jurídica Distrital debe evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que generen afectaciones a la confidencialidad, integridad o disponibilidad de la información.

11.1.1. Perímetro de Seguridad Física

Todos los ingresos que utilizan sistemas de control de acceso deben permanecer cerrados y es responsabilidad de todos los funcionarios autorizados evitar que las puertas se dejen abiertas.

Se deberá exigir a todos los visitantes, sin excepción, el porte de la tarjeta de identificación de visitante o escarapela en un lugar visible. Así mismo, todos los funcionarios deberán portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de la Secretaría Jurídica Distrital.

Los visitantes deberán permanecer acompañados de un funcionario de la Secretaría Jurídica Distrital, cuando se encuentren en las oficinas o áreas donde se maneje información.

Es responsabilidad de todos los funcionarios de la Secretaría Jurídica Distrital borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo.

Igualmente, no se deberán dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

Los visitantes que requieran permanecer en las oficinas de la Secretaría Jurídica Distrital por periodos superiores a dos (2) días deberán ser presentados al personal de oficina donde permanecerán.

El horario autorizado para recibir visitantes en las instalaciones de la Secretaría Jurídica Distrital es de 7:00 AM a 4:30 PM. En horarios distintos se requerirá de la autorización del Director, Jefe de Oficina correspondiente.

Los equipos portátiles, así como toda información CONFIDENCIAL de la Secretaría Jurídica Distrital, independientemente del medio en que se encuentre, deberán permanecer guardados bajo llave durante la noche o en horarios en los cuales el funcionario responsable no se encuentre en su sitio de trabajo.

11.1.2. Control de Acceso Físico de Entrada

Las áreas seguras, dentro de las cuales se encuentran el Centro de Cómputo, centros de cableado, áreas de archivo y áreas de recepción y entrega de correspondencia, deberán contar con Mecanismos de protección física y ambiental, y controles de acceso que pueden ser mediante tarjeta de proximidad o puertas con cerradura.

En las áreas seguras, bajo ninguna circunstancia se podrá fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deberán ser controladas y supervisadas por un funcionario del proceso. El personal de limpieza deberá ser instruido acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohibirá el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

11.1.3. Protección Contra Amenazas Ambientales

Para protección contra daños físicos por amenazas como incendios, inundaciones, terremotos entre otros se requiere:

1. Identificar y almacenar elementos que puedan ser combustibles o que contribuyan a una conflagración bajo los niveles de almacenamiento recomendados por el proveedor.
2. Identificar y asegurar muebles y elementos que puedan causar daño físico a funcionarios o visitantes en caso de movimientos geográficos o conmociones.
3. Desarrollar planes de respuesta y supervivencia del personal para casos de emergencia.

11.1.4. Seguridad en Oficinas y Áreas de Trabajo

En las áreas de acceso restringido debe haber una continua supervisión del trabajo realizado, especialmente por terceros, se debe limitar el uso de quipos como cámaras fotográficas, de

video, celulares. En caso de ser requerido solo podrá ser autorizado mediante autorización previa.

El acceso está restringido y el personal debe estar debidamente identificado y autorizado.

11.1.5. Áreas de Despacho y Carga

El acceso está restringido y el personal debe estar debidamente identificado y autorizado.

Estas áreas deben estar aisladas y/o controladas de tal manera que desde éstas no se pueda acceder a otras áreas no autorizadas.

El material que ingresa a estas áreas debe ser inspeccionado.

11.2 Ubicación y Protección de Equipos

La Secretaría Jurídica tiene un formato para el retiro de equipos de la entidad, evitando así la perdida de los mismos.

A la salida de la entidad se debe registrar en el libro de vigilancia la marca del equipo que se retira, con el número de serie.

11.2.1 Ubicación y Protección de Equipos

La infraestructura tecnológica (hardware, software y comunicaciones) deberá contar con medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

11.2.2. Seguridad de los Equipos Fuera de las Instalaciones

Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deberán ser controlados mediante el cifrado de la información almacenada en sus discos duros, utilizando la herramienta definida por la Oficina de Tecnologías de la Información y las Comunicaciones.

Los equipos portátiles no deberán dejarse a la vista en el interior de los vehículos. En casos de viaje siempre se deberán llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se deberá informar inmediatamente a la Dirección de Corporativa y se deberá poner la denuncia ante la autoridad competente y allegar copia de la misma.

Los equipos portátiles deben estar asegurados (cuando los equipos estén desatendidos) con una guaya, dentro o fuera de las instalaciones de la Secretaría Jurídica Distrital.

Los puertos de transmisión y recepción de infrarrojo y “Bluetooth” deberán estar deshabilitados. Cuando un equipo de cómputo deba retirarse de las instalaciones de la Secretaría Jurídica Distrital se deberá utilizar el formato y procedimiento correspondiente.

11.2.3. Retiro de Activos

Los equipos de cómputo, la información o el software no deben ser retirados de la entidad sin una autorización formal. Periódicamente se deben llevar a cabo por parte de la Dirección de Corporativa, comprobaciones puntuales para detectar el retiro no autorizado de activos de la entidad.

11.2.4. Seguridad del Cableado

Se debe proteger el cableado tanto de energía como de comunicaciones en los servicios de procesamiento de información tanto de daños como de interceptaciones.

Se debe tener separadas las rutas de cableado de energía y comunicaciones con el fin de evitar interferencias.

En el caso de elementos críticos se deben considerar protegerlos mediante controles como blindaje, cajas de cableado bloqueadas, amplio uso de fibra óptica, inspecciones técnicas regulares para detectar dispositivos no autorizados, accesos controlados a puntos de distribución.

El cableado debe estar debidamente marcado y debe encontrar con un plano para hacer correcciones o inserciones de manera efectiva**.**

11.2.5. Mantenimiento a los Equipos

Se deben realizar las siguientes acciones:

1. Efectuar mantenimiento preventivo y correctivo a intervalos de tiempo definido a los equipos y solo por personal autorizado. Esta labor se debe hacer tanto a aquellos equipos que procesen información como aquellos que soporten estos activos.

2. Se deben conservar los registros de los mantenimientos realizados.

3. Se debe tener un cronograma de mantenimientos.

11.2.6. Política de Escritorio y Pantalla Limpia

El objetivo de esta política es prevenir la perdida, daño, robo o compromiso de la información durante y fuera de las horas laborales, en los equipos de cómputo de los funcionarios de la entidad.

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

Para el personal que esté ubicado en zonas de atención al público, al ausentarse de su puesto deberá guardar también los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada.

El personal de la Secretaría Jurídica Distrital debe bloquear la pantalla de su computador con el protector de pantalla designado por la entidad, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo. Al finalizar sus actividades diarias, deberán salir de todas las aplicaciones y apagar la estación de trabajo.

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deberá reutilizar papel que contenga información CONFIDENCIAL.

En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar la información CONFIDENCIAL protegida bajo llave. Esto incluye: documentos impresos, CD´s, dispositivos de almacenamiento USB y medios removibles en general.

Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad, definido por el ingeniero de TIC.

Al activarse el protector de pantalla debe bloquear la sesión en los equipos de cómputo y dispositivos móviles de la SJD, este deberá activarse después de 5 minutos de inactividad de cualquiera de estos equipos.

Los equipos de reproducción de información (impresoras, fotocopiadoras, escáneres, etc.), deben estar ubicados en lugares de acceso controlado y cualquier documentación con información pública clasificada o pública reservada se debe retirar inmediatamente del equipo y ser puesta en un lugar seguro.

12. SEGURIDAD DE LAS OPERACIONES

12.1. Procedimientos de Operación Documentados

Se debe documentar y mantener actualizados todos los procedimientos de operación, teniendo en cuenta los ya existentes en la entidad, asegurando la disponibilidad de la información.

Se documentarán y mantendrán actualizados los procedimientos operativos identificados y sus cambios serán autorizados por el responsable de la Seguridad de la Información.

12.1.1. Gestión de Cambios

La Secretaría Jurídica Distrital debe asegurar que los cambios de alto impacto realizados sobre la organización, los procesos de negocio, las instalaciones o los sistemas de procesamiento de información se realicen de forma controlada.

Toda solicitud de cambio en los servicios de procesamiento de información, se deben realizar siguiendo el Procedimiento de Análisis, Diseño, Desarrollo e Implementación de Soluciones, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información, e igualmente tener una trazabilidad de este tipo de solicitudes.

El procedimiento de gestión de cambios especifica los siguientes canales autorizados para la recepción de solicitudes de cambios: soporte@secretariajuridica.gov.co, (Recepción de documentación Software), correo electrónico o memorando dirigido al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones.

Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, bien sea porque se trate de actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad del aplicativo o a los componentes que soportan el sistema de información, tales como el sistema operativo o cambios en hardware. Existe sin embargo una situación especial para cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada. (Ver Procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones).

Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los funcionarios que por sus actividades tienen relación con el sistema de información.

Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información. Estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantienen las condiciones de operatividad del sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema, y que el propósito del cambio se cumplió satisfactoriamente.

Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

12.1.2. Gestión de Capacidad

La Secretaría Jurídica Distrital debe asegurar la disponibilidad de los recursos necesarios para la operatividad de los sistemas de información contemplando necesidades actuales y futuras.

La Oficina de Tecnologías de la Información y las Comunicaciones definirá las actividades específicas para monitorear, proyectar y asegurar la capacidad de la infraestructura de procesamiento de información, con el objeto de garantizar el buen desempeño de los recursos tecnológicos necesarios para la ejecución de los procesos.

La capacidad de los recursos debe ser ajustada periódicamente para garantizar la disponibilidad y eficiencia requerida de acuerdo a las necesidades actuales y futuras de la Secretaría Jurídica Distrital.

El monitoreo y gestión de la capacidad debe hacerse considerando la criticidad de la información y los sistemas que soportan, para lo cual se utilizará la criticidad determinada durante el levantamiento del inventario de activos de información. Aquellos componentes que soporten activos con criticidad alta siempre deben estar sujetos a monitoreo y gestión de capacidad.

Se debe tomar las acciones adecuadas para minimizar o evitar la dependencia de elementos o personas claves para la prestación de un servicio. Dentro de las acciones se deben contemplar: redundancia de elementos, arquitecturas de contingencia o de alta disponibilidad, técnicas de gestión de conocimiento sobre la operatividad de la infraestructura, etc.

Los umbrales de óptimos de capacidad se pueden obtener incrementando la capacidad o reduciendo la demanda, lo cual incluye las siguientes posibles acciones que deberán ser llevadas a cabo por la Oficina de Tecnologías de la Información y las Comunicaciones que son:

1. Eliminación obsoleta
2. Supresión de aplicaciones
3. Bases de datos o ambientes en de uso
4. Optimización de procesos o tareas automáticas
5. Afinamiento de consulta de bases de datos o lógica de aplicaciones
6. Restricción de ancho de banda para servicios con alto consumo de capacidad que no sean misionales.

12.1.3. Separación de los Ambientes de Desarrollo, Prueba y Producción

La Secretaría Jurídica Distrital debe reducir riesgos asociados a modificaciones, cambios o accesos no autorizados en sistemas en producción.

Se deben establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información de la Secretaría Jurídica Distrital. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario de activos de información.

El ambiente de desarrollo se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código. Por su parte, el ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas hacia el software teniendo como base los criterios de aceptación y los requerimientos de desarrollo.

Finalmente, el ambiente de producción debe utilizarse para la prestación de un servicio que involucra la manipulación de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la entidad.

Se debe seguir un procedimiento formal para el paso de software y aplicaciones de un ambiente a otro (desarrollo, pruebas y producción), que establezca las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a

uno existente. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario de activos de información.

No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.

Se debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

Se deben 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.

Cada uno de los ambientes debe estar claramente identificados, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada ambiente.

Los cambios a sistemas en producción que involucren aspectos funcionales deben ser informados y consultados con el(los) proceso (s) propietario(s) de la información.

12.2. Protección Contra Código Malicioso

La Secretaría Jurídica Distrital debe establecer medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos.

La infraestructura de procesamiento de información debe contar con un sistema de detección/prevención de intrusos, sistema anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores de la Secretaría Jurídica Distrital.

Se restringirá la ejecución de código móvil aplicando políticas en el sistema operacional, en el software de navegación de cada máquina y en el sistema de control de navegación.

Los usuarios de los servicios TIC de la Secretaría Jurídica Distrital son responsables de la utilización de programas antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos y/o removibles y/o los archivos y/o el correo electrónico que esté autorizado a emplear.

La Secretaría Jurídica Distrital contará permanentemente con los programas antivirus de protección a nivel de red y de estaciones de trabajo, contra virus y/o código malicioso, el servicio será administrado por la Oficina de Tecnologías de la Información y las Comunicaciones.

Los programas antivirus deben ser instalados por la Oficina de Tecnologías de la Información y las Comunicaciones en los equipos centralizados de procesamiento y en las estaciones de trabajo de modo residente, para que estén activados durante su uso.

La Oficina de Tecnología implementará los siguientes controles:

1. Prohibir el uso de software no autorizado
2. Instalar y actualizar periódicamente software de detección y reparación de virus examinando computadores y medios informáticos, como medida precautoria y rutinaria.
3. Mantener los sistemas de información al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
4. Revisar periódicamente el contenido del software y datos de los equipos de procesamiento que sustentan procesos críticos, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
5. 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.
6. Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

12.3. Copias de Respaldo (Backup)

La Secretaría Jurídica Distrital debe proporcionar medios de respaldo adecuados para asegurar que la información esencial y el software asociado se puedan recuperar después de una falla.

La información de cada sistema de información debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, CD, DVD, Disco Externo, de acuerdo a su nivel de criticidad identificada en el inventario de activos de información.

La información con criticidad mayor debe estar sujeta a una mayor frecuencia de tareas de respaldo. Los medios se almacenarán en una custodia externa que cuente con los mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico (Ver Procedimiento de Administración de Backups y Restore).

Se deben realizar pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad. Estos aspectos técnicos se deben registrar en el formato de Control de Restauración de Información. (Ver Procedimiento de Administración de Backups y Restore).

El custodio de cada activo de información es el responsable de verificar que los backups se ejecuten correctamente y de acuerdo al tipo y frecuencia acordados.

El administrador de las Bases de Datos y el Oficial de Seguridad de la Información son los responsables de definir la frecuencia de respaldo, el tipo, el medio de almacenamiento y los requerimientos de seguridad de la información, de acuerdo a las disposiciones definidas en el Manual de Política de Copias de Seguridad y Recuperación.

Estos aspectos de configuración se deben registrar en el formato de Control Backup.

Todas las copias de información con criticidad alta deben ser almacenadas en un área adecuada y con control de acceso.

Las copias de respaldo se deben guardar con el objetivo de restaurar el sistema luego de una infección de virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, contaminación de los datos y por requerimientos legales.

Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

Es responsabilidad de cada funcionario ubicar la información más crítica asociada con su labor encomendada en el servidor de archivos definido para cada usuario. El servidor de archivos estará protegido con un sistema de respaldo de la información.

12.4. Registro y Seguimiento

Todos los eventos que se presenten se registran en el Sistema de Medición Análisis y Reporte para la toma de decisiones SMART allí se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

1. Identificador del usuario
2. Fecha y hora DE INICIO Y TERMINACIÓN
3. Registros de intentos exitosos y fallidos de acceso al sistema
4. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

12.4.1. Sincronización de Relojes

Los relojes de todos los sistemas de procesamiento de información de la entidad deberán ser sincronizados con una única fuente de referencia de tiempo.

Para garantizar la integridad de la información debe existir un registro de cualquier modificación realizada al sistema de procesamiento de la información, por tal razón se debe tener en cuenta lo siguiente:

1. Llevar un registro documentado en el que se consignen las solicitudes de modificación o de cambios que se hayan realizado a los sistemas de procesamiento de información.

2. Documentar de manera clara y explícita cuando hayan ocurrido fallas, la forma como fueron corregidas y el porcentaje de avance de la acción de mejora.

12.5. Gestión de Vulnerabilidades Técnicas

Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de esta en el sistema de información, se debe evaluar la exposición de la entidad a estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.

Para ello la gestión de vulnerabilidades técnicas debe estar basado en:

1. Monitoreo sobre la plataforma tecnológica
2. Reportes de fabricantes y proveedores
3. Servicios de seguridad informática contratados
4. Reporte de usuarios internos y externos.

12.5.1. Restricciones sobre la Instalación de Software

Los funcionarios de la entidad, no podrán instalar ningún software, programa o aplicativo en los equipos designados para su labor en la entidad o bajo la modalidad de teletrabajo.

13. SEGURIDAD DE LAS COMUNICACIONES

13.1. Gestión de la Seguridad de Redes

El acceso a las redes de la entidad, debe estar limitado a los funcionarios de la entidad y demás personas autorizadas por la misma por medio de claves de acceso a los sistemas de información.

Se establecerá un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad establecidos.

La entidad proporciona a los funcionarios todos los recursos tecnológicos de conectividad necesarios, para que puedan desempeñar las funciones/actividades para las cuales fueron contratados, por tal motivo no se permite conectar a las estaciones de trabajo o a los puntos

de acceso corporativos, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones.

13.2. Separación de las Redes

Se debe establecer un esquema de segregación de redes con el fin de controlar el acceso a los diferentes segmentos de red. El tráfico entre estos segmentos de red estará controlado mediante un elemento de red que permita una autorización a un nivel de detalle específico (Dirección IP, puerto).

13.3. Transferencia de Información

La entidad asegura la protección de la información y el software en el momento de ser transferida o intercambiada internamente y externamente con cualquier otra organización, por lo cual establece procedimientos y controles mínimos requeridos para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información.

La información de la entidad puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, descarga de archivos desde internet, transferencia de datos por medio de los sistemas de información misionales (SIPROJ. SIPEJ) o administrativos y financieros, teléfonos, equipos fax, mensajes de texto por teléfonos móviles.

Se prohíbe el envío de información confidencial o sensible de la entidad a personal externo de la entidad sin autorización previa.

Está prohibido el uso del correo electrónico personal (Hotmail, Gmail, entre otros) para el envío o recepción de cualquier tipo de información relacionada con la entidad.

No está permitido el intercambio de información pública clasificada y reservada de la entidad, por medio telefónico o por correo electrónico, sin las debidas protecciones y controles necesarios que la ameritan por su nivel de clasificación.

Para tal fin, se pueden apoyar en soluciones tecnológicas de cifrado para la información en medio digital.

La información física, no se debe dejar abandonada en impresoras, en el puesto de trabajo o un área de circulación alta de personas.

13.3.1. Acuerdos sobre Transferencia de Información

Se debe contar con procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones, en concordancia con la normatividad vigente.

Las alianzas y convenios con los proveedores estarán regidos bajo los siguientes criterios:

1. Cualquier alianza o convenio del procesamiento de información con proveedores o con personal externo de la SJD, debe contar con mecanismos de confidencialidad, integridad y auditabilidad de tal forma que cumplan con los estándares definidos por la seguridad de la información.
2. La información referente a servicios, trámites e información entre la SJD y los usuarios de la página WEB, debe contar con la seguridad necesaria para el uso de registro de usuarios, gestión de sesiones seguras, generación de registros de auditoría y validez jurídica para dar valor probatorio a los mensajes de datos.
3. Para todo intercambio de información confidencial o restringida se deben establecer acuerdos de confidencialidad.

13.3.2. Mensajes Electrónicos

Con el fin de garantizar la confidencialidad de la información, se deben establecer parámetros para el envío de la información a terceros por medio del correo electrónico de la entidad para proteger adecuadamente la información incluida en la mensajería electrónica, para tal fin:

Los funcionarios de la entidad, serán responsables de todas las actividades realizadas con su cuenta de correo institucional.

En el caso de recibir un correo electrónico de un destinatario desconocido, esté no debe ser abierto y el empleado debe notificar de forma inmediata, para evitar que en caso de que este contenga algún virus, infecte el sistema.

El servicio de correo electrónico debe ser usado únicamente para el ejercicio de las funciones de competencia de cada usuario.

13.3.3. Acuerdos de Confidencialidad o No Divulgación

Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la entidad para la protección de la información.

En todo convenio o contrato que la entidad firme con sus funcionarios, contratistas, y demás personal será necesario:

1. Establecer una cláusula de confidencialidad de la información.

2. En el caso de los contratistas se debe incluir dentro de los contratos la cláusula de confidencialidad y reserva de la información a la cual tengan acceso mientras permanezcan en la entidad.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

14.1. Requisitos de Seguridad en la Adquisición de los Sistemas de Información

La Secretaría Jurídica Distrital, debe asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, incluyendo los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

14.1.1. Análisis y Especificaciones de Requisitos de Seguridad de la Información

La Secretaría Jurídica Distrital, establecerá los requisitos relacionados con seguridad de la información, los cuales deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

14.1.2. Seguridad de Servicios de las Aplicaciones en Redes Públicas

La Secretaría Jurídica Distrital, debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas, mediante un proceso de gestión de tecnología de información y comunicación.

14.1.3. Protección de Transacciones de Servicios de Aplicaciones

La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la trasmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada por medio de controles que establecerá el Proceso de gestión de tecnología de información y comunicación de la Secretaría Jurídica Distrital.

14.2. POLÍTICA DE DESARROLLO SEGURO

La Secretaría Jurídica Distrital debe establecer las condiciones y vigilar que el desarrollo y mantenimiento llevado a cabo, tanto internamente como por proveedores externos, para que cumplan con buenas prácticas para el desarrollo seguro, además de establecer criterios de seguridad que deben ser considerados en todas las etapas de desarrollo.

14.2.1. Requisitos de Seguridad en el Desarrollo de los Sistemas de Información

La construcción y modificación de sistemas de información o la implementación de nuevos módulos a los sistemas de información misionales o de apoyo, desarrollados al interior de la entidad o contratados con terceras partes, deben contemplar un completo análisis de requerimientos en cuanto a seguridad de la información, análisis de riesgos y posibles escenarios de riesgos asociando los controles respectivos para la mitigación de los mismos.

14.2.2. Procedimiento de Control de Cambios

Cualquier tipo de cambio sobre los sistemas de información deberá seguir lo establecido en el Procedimiento de Análisis, Diseño, Desarrollo e Implementación de Soluciones de la Secretaría Jurídica Distrital y debe tener en cuenta la aceptación de las pruebas técnicas y funcionales dictaminadas por cada uno de los responsables a quienes afectaran los cambios que se realicen.

Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.

14.2.3. Revisión Técnica de Aplicaciones después de Cambios en la Plataforma.

Cuando se cambian las plataformas de operación, La Oficina de Tecnologías de la Información y las Comunicaciones, designara un Ingeniero el cual debe revisar las aplicaciones Misionales y Administrativa de la Secretaría Jurídica distrital y someterlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la entidad provocado por los cambios previa.

14.2.4. Restricciones sobre los Paquetes de Software

Los cambios a los paquetes de software son autorizados, supervisados y realizados por funcionarios de la oficina de Tecnologías de la Información y las Comunicaciones de la entidad. Si es necesario que un proveedor o contratista realice los cambios al paquete de Software, estos cambios serán realizados bajo el permiso y supervisión de la misma área, con la finalidad de garantizar la confidencialidad e integridad de la información contenida en los computadores, dispositivos móviles, sistemas de información y procesamiento a los que sea necesario realizarle cambios.

14.2.5. Desarrollo de Software Contratado Externamente

El desarrollo de software contratado con terceras partes, deberá contemplar todos los requisitos en cuanto a seguridad de la información fijados en este documento, solo se darán por recibidos desarrollos realizados sobre los estándares de la entidad en cuanto a herramienta de desarrollo, y pruebas técnicas y funcionales.

Los contratos de desarrollo de software con terceros deberán tener claramente definidos los alcances de las licencias, los derechos de propiedad del código desarrollado y los derechos de propiedad intelectual, junto con los requerimientos contractuales relacionados con la calidad y seguridad del código desarrollado.

Se debe realizar un análisis de vulnerabilidades técnicas a los sistemas de información desarrollados y que estén en proceso de paso a producción, para garantizar que los nuevos desarrollos no exponen la seguridad de la información de la Secretaría Jurídica Distrital ni su infraestructura. Esta actividad está a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.

14.2.6. Prueba de Seguridad en los Sistemas de Información

Se deberá estandarizar el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software.

Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.

Para propósitos de desarrollo y pruebas de software, se deberán generar datos de prueba distintos a los que se encuentran en el ambiente de producción.

Los desarrolladores y terceros, no deberán tener acceso a información de producción que contenga datos sensibles.

Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto.

Existen normas de seguridad para la documentación del software que se deben llevar a cabo en la SJD, que son:

1. El diccionario de datos, o repositorio de metadatos, deberá mantener una descripción actualizada de las definiciones de los datos.

2. Si el desarrollador incluye comentarios en el programa fuente, estos no deben divulgar información de configuración innecesaria.

3. La documentación de los desarrollos deberá:

   a. Generarse durante el ciclo de vida de desarrollo y no postergarla hasta el final.
   b. Ser revisada por los usuarios finales del Sistema en desarrollo
   c. Actualizarse si el programa cambia alguna de sus funcionalidades
   d. Almacenarse en un sitio centralizado (servidor) administrado por el funcionario encargado de desarrollo.

Existen normas para la codificación y pruebas que la SJD debe llevar y son:

1. No está permitido modificar programas sin que quede registrado o documentado
2. No está permitido escribir o modificar código auto-copiante
3. En lo posible, las pruebas del Sistema deberán incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación de errores.
4. Se deberán tener las siguientes consideraciones con relación a los datos de entada y salida de los sistemas de información:

   a. Realizar las validaciones de datos de entrada y salida en un Sistema confiable
   b. Utilizar rutinas de validación centralizadas y estandarizadas
   c. Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud entre otros.

d. Limpiar las salidas de datos no confiables hacia consultas SQL,XMLo hacia comandos de sistemas operativo

Existen normas para la implementación de los sistemas que la SJD debe llevar y son:

1. Se deberá velar por los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.

2. Se deberá efectuar sintonía o ajuste (tunning) de los controles establecidos en la fase de diseño.

3. Las aplicaciones deberán contar con un sistema de autenticación de usuario, que mínimo exija nombre de usuario y contraseña. Además, en los casos que la aplicación esté expuesta a internet, debe implementarse la validación de captcha.

4. Las aplicaciones deberán contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.

Con la finalidad de garantizar la disponibilidad de la información se deben realizar las siguientes pruebas:

- **Pruebas de compatibilidad**: Se debe garantizar el funcionamiento adecuado y continúo del software desarrollado en diferentes plataformas: hardware, sistemas operativos, redes.
- **Pruebas de integración**: Se debe comprobar las conexiones y comunicaciones entre los diferentes módulos del software desarrollado y los demás sistemas de información de la entidad que tengan relación con el desarrollo.
- **Pruebas de función**: Esta prueba permite asegurar que el sistema cumple con la funcionalidad para el cual fue hecho, con las especificaciones técnicas esperadas y es útil para los funcionarios de la entidad.
- **Pruebas de desempeño**: La finalidad de esta prueba está orientada a establecer la eficiencia del sistema de información cuando es utilizado por parte de los funcionarios de la entidad, estableciendo posibles fallas antes de su puesta en marcha.
- **Pruebas de instalación**: Esta prueba consiste en instalar el sistema de información en el servidor que alojará la base de datos o los archivos fuente del sistema de información.

15. RELACIÓN CON LOS PROVEEDORES

15.1. Política de Seguridad en Relación con los Proveedores

La Secretaría Jurídica Distrital debe proteger en términos de seguridad la información accedida por los proveedores.

15.2. Tratamiento de Seguridad en los Acuerdos con Terceras Partes

En los Contratos o Acuerdos con terceras partes y que implique un intercambio, uso o procesamiento de información de la entidad, se debe ***contemplar*** la posibilidad de celebrar Acuerdos de Confidencialidad en el manejo de la información. Estos acuerdos deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio. El contrato o acuerdo debe definir claramente el tipo de información que intercambiaran las partes.

El Oficial de Seguridad de la información, realizará una visita anual al proveedor, para revisar en sitio el cumplimiento de la seguridad de la información del objeto contratado, el tratamiento de los riesgos que se encuentren dentro del acuerdo de servicios y adicionalmente, realizará el respectivo seguimiento a los planes de acción y remediación en tiempos prudentes definidos en conjunto con el proveedor.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1. Gestión de Incidentes y Mejoras en la Seguridad de la Información

La Secretaría Jurídica Distrital debe gestionar adecuadamente los incidentes de seguridad de la información presentados en el contexto de la entidad, en el Sistema de Medición Análisis y Reporte para la toma de decisiones **SMART.**

Es responsabilidad de cada uno de los funcionarios de la entidad y terceras partes, reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información; esto con el fin de proceder con el tratamiento respectivo.

A todos los incidentes de seguridad reportados, se les debe dar el tratamiento y seguimiento respectivo, realizando el respectivo trámite ante las instancias correspondientes. (Ver Guía Gestión de Incidentes de Seguridad de la Información 2310200-GS-004).

16.2. Responsabilidades y Procedimientos

La Secretaría Jurídica Distrital, debe establecer acciones que mitiguen el impacto asociado a los incidentes que se presentan, por tal razón se establecerán los procedimientos para la gestión de los incidentes de seguridad de la información.

El procedimiento para la gestión de los incidentes reportados por colaboradores y usuarios debe ser revisado periódicamente por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones con el fin de identificar cambios o ajustes pertinentes que garanticen la eficiencia y eficacia de las respuestas.

Se asigna como responsable para la entidad de la gestión de los incidentes de seguridad al Oficial de Seguridad de la información quien debe documentar y conservar trazabilidad de los eventos y debilidades reportadas por los colaboradores y usuarios. Los registros deben ser conservados garantizando que se reciben notificación de los resultados después de tratado y solucionado el problema, en el Sistema de Medición análisis y Reporte para la toma de decisiones **SMART.**

16.3. Reporte de Eventos de Seguridad de la Información

El reporte de eventos, debilidades o incidentes que comprometan la gestión de datos personales, seguridad de la información o continuidad del negocio es una actividad obligatoria para todos los colaboradores y usuarios asociados a los activos y servicios de la Secretaria Jurídica.

La Oficina de Tecnología de la Información y Comunicaciones debe velar por que los colaboradores y usuarios reciban capacitación para registro y/o reporte de eventos y debilidades de gestión de la privacidad, seguridad de la información y continuidad del negocio.

16.4. Evaluación de Eventos de Seguridad de la Información

Los responsables de gestionar los incidentes deben mantener indicadores de gestión y reportes de los tipos de incidentes, cantidad de los mismos e impacto generado sobre servicios y activos de la entidad.

Los propietarios y custodios de servicios, recursos y activos de información, debe actualizar la valoración de riesgos y los análisis de impactos asociados a sus procesos, tomando como referencias incidentes presentados.

Cuando se detecte un evento o incidente en la seguridad de la información que puede culminar en una acción legal, se debe iniciar el tratamiento del incidente acorde al procedimiento Gestión de Incidentes de la entidad.

16.5. Respuesta a Incidentes de Seguridad

La Oficina de Tecnologías de la Información y Comunicaciones, debe probar periódicamente (por lo menos una vez al año), la capacidad de respuesta a incidentes del sistema de información para determinar la efectividad de la respuesta al incidente y documenta los resultados. El análisis forense de seguridad de la información.

Las respuestas de los incidentes de seguridad de la información deben contener por los menos:

1. La evidencia lo más pronto posible después de que ocurra el incidente
2. Llevar el asunto a una instancia superior, según se requiera
3. Registrar todas las actividades de respuesta involucradas para análisis posterior.
4. Comunicar la existencia del incidente a quien necesite saberlo
5. Tratar las debilidades de seguridad de la información que se encontraron que causen o contribuyan al incidente
6. Una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.

16.6. Aprendizaje Obtenido de los Incidentes de Seguridad de la Información

La Oficina de Tecnologías de la Información y Comunicaciones definirá 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 será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

16.7. Recolección de Evidencias

Se definirá 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 será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

Las Mesas de Trabajo de Seguridad de la Información y Continuidad del negocio junto con la Oficina de Tecnologías de Información y las Comunicaciones debe mantener un repositorio centralizado sobre el manejo de los incidentes para poder analizarlos, prevenirlos y divulgar los conocimientos obtenidos, de modo que las direcciones o dependencias de la Secretaría Jurídica Distrital, estén preparadas y protegidas a futuro de una mejor forma.

Las evidencias de los incidentes de seguridad deben demostrar la calidad e integridad de los controles utilizados demostrando protección y consistencia durante todo el período de almacenamiento y procesamiento de la información (cadena de custodia).

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La Secretaría Jurídica Distrital debe garantizar que los planes de continuidad de Negocios se ejecuten de forma segura sin exponer la información de la entidad.

17.1. Continuidad De La Seguridad De La Información

Ante la ocurrencia de eventos no previstos en cuanto a la indisponibilidad del centro de datos principal, de la Secretaría Jurídica Distrital debe contar y asegurar la implementación de un Plan de Recuperación de Desastres que asegure la continuidad de las operaciones tecnológicas de sus procesos críticos.

Para la Secretaría Jurídica Distrital su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier situación.

17.2. Planificación de la Continuidad del Negocio

La Secretaría Jurídica, debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, deben estar incorporados y definidos en un “Plan de contingencias”.

17.3. Disponibilidad de Instalaciones de Procesamiento de Información

La Secretaría Jurídica Distrital dispondrá de las instalaciones de procesamiento de información las cuales se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad de la información y se deberían poner a prueba para asegurar que la conexión automática de emergencia después de una falla de un componente a otro funcione de la forma prevista, de acuerdo a lo definido en la Mesas de Trabajo que realice la oficina de TIC.

18. CUMPLIMIENTO

18.1. Cumplimiento de Requisitos Legales y Contractuales

La Secretaría Jurídica Distrital debe garantizar el cumplimiento de los requisitos legales a los cuales está sometida en función de la información que custodia.

18.1.1. Identificación de los Requisitos de Legislación y Contractuales Aplicables

La Secretaria Jurídica, debe atender a todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como los requerimientos para cumplirlos.

De igual manera se deben identificar y documentar explícitamente los requisitos de la legislación aplicable, y mantenerlos actualizados para el Sistema de Gestión de Seguridad de la Información:

La entidad debe atender la siguiente normatividad: Norma ISO/IEC 27001:2013: Establece las directrices del Sistema de Gestión de la seguridad de la información.

Adicionalmente establece el rol y responsabilidad de los funcionarios y grupos de interés de la entidad y así mismo establece la metodología de identificación de los activos de información, la valoración de los riesgos, la calificación de los controles, el plan de tratamiento para la mitigación de los riesgos asociados a los activos de información, las revisiones y auditorías que se le hacen al SGSI.

Adicionalmente, de manera continua se deben realizar:

1. Revisiones permanentes sobre la expedición de nuevas leyes y normatividad que afecten de manera directa la Seguridad de la Información
2. La interpretación de las implicaciones en la Seguridad de la Información de estas leyes o decretos
3. La identificación de la posibilidad de incumplimiento legal y reglamentario por parte de la Secretaría Jurídica Distrital

18.2. Derechos de Propiedad Intelectual

La entidad debe cumplir con la reglamentación de propiedad intelectual para lo cual implementa los controles necesarios que garanticen el respeto de dicha reglamentación.

No se permite el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías,

gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

Definición de normas y procedimientos para el cumplimiento de la normatividad vigente.

Divulgación de las políticas de adquisición de software y las disposiciones de la normatividad vigente.

Se debe mantener un adecuado registro de activos.

Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, entre otros.

Implementar controles para evitar el exceso del número máximo permitido de usuarios.

Verificar que sólo se instalen productos con licencia y software autorizado.

Elaboración y divulgación de un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

Utilización de herramientas de auditoría adecuadas.

Cumplimiento con los términos y condiciones establecidos para obtener software e información en redes públicas.

Se debe realizar un inventario de licencias de software mínimo dos veces al año, en particular de herramientas de oficina y productividad, licencia de usuario de sistemas operativos de red, base de datos y otros.

Se debe tener control sobre el uso de software libre que hacen los usuarios, y su relación con la función que realizan.

18.3. Protección de los Registros de la Información

Los registros críticos de la entidad, se protegerán 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 Jurídica Distrital.

Los registros se clasificarán 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, papel, microfichas, medios magnéticos u ópticos entre otros.

CONTROL DE CAMBIOS.

ACTIVIDADES O NUMERALES QUE CAMBIARON	CAMBIOS EFECTUADOS	FECHA DEL CAMBIO	VERSIÓN
Creación del Documento	N.A.	25/10/2017	01
Ajustes al documento	Ajustes en objetivos específicos, estructura del documento, glosario, principios, y adiciones a la declaración de política, requeridos para fortalecer aspectos relacionados con protección de datos personales	28/11/2017	01
Ajustes al documento	Se ajustó el nombre del documento, los objetivos, se agregaron definiciones, se actualizó el marco legal y normativo, se ajustaron algunas políticas y se agregó la política de Teletrabajo y documentos electrónicos.	10/12/2019	02