POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NOVIEMBRE 2018

VEEDURÍA DISTRITAL Prevención • Transparencia • Incidencia	**POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

CONTENIDO

VEEDURÍA DISTRITAL Prevención • Transparencia • Incidencia	**POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

INTRODUCCION

La Entidad, consciente de la importancia de definir controles para preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona en los procesos y a través de los procedimientos, debe aplicar políticas de seguridad que minimicen los riesgos que amenacen y vulneren la información, con el fin de dar continuidad a sus servicios.

En este documento se plantean políticas que alineada con los objetivos institucionales y la misionalidad de la Entidad permitirán dar lineamientos que protejan y resguarden la información que tiene la Veeduría Distrital, donde funcionarios y contratistas juegan un papel importante y vital en la conservación.

AUDIENCIA

De uso interno de la Veeduría Distrital.

DERECHOS DE AUTOR

GLOSARIO

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Amenaza informática: la aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).

Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

Autenticidad: propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Veeduría Distrital, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

Datos abiertos: son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).
Datos personales sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

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

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Impacto: el coste para la empresa de un incidente -de la escala que sea- , que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

Parte interesada (*Stakeholder*): persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto 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.

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

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

Segregación de tareas: reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Titular de la información: es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociada de modo inequívoco a un individuo o entidad.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

MARCO LEGAL

Ley 1273 de 2009 del Congreso de la República. 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 1581 de 2012 del Congreso de la República. Por el cual se dictan disposiciones generales para la protección de datos personales. HABEAS DATA.

Ley 1712 de 2014 del Congreso de la República. 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 619 de 2007 de la Alcaldía Mayor de Bogotá D.C. Se establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y se dictan otras disposiciones.

Decreto 316 de 2008 de la Alcaldía Mayor de Bogotá D.C. Por medio del cual se modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.

Decreto 2609 de 2012 de la Presidencia de la República. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 1377 de 2013 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

Decreto 2573 de 2014 de la Presidencia de la República. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 103 de 2015 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto Único Reglamentario 1078 de 2015, Título 9 capítulo 1, Estrategia del Gobierno en Línea. Sección 2, Artículo 2.2.9.1.2.1 numeral 4 define el componente de Seguridad y Privacidad de la Información.

Decreto 415 de 2016 de la Presidencia de la República. Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

Norma Técnica ISO/IEC 27001 de 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

Resolución 305 del 20 de octubre de 2008 de la Comisión Distrital de Sistemas CDS de Bogotá D.C. Las entidades, organismos y órganos de control del Distrito Capital dispondrá lo necesario para la Creación del Comité de Seguridad de la Información CSI o una instancia semejante, que debe validar las Políticas de Seguridad de la Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores de cada ente público.

Resolución 151 de 2016 de la Veeduría Distrital. Por medio del cual se designa al Líder TIC en la Veeduría Distrital.

Resolución 118 de 2016 de la Veeduría Distrital. Por la cual se conforma el Comité de Seguridad de la Información de la Entidad.

Resolución 283 del 2016 de la Veeduría Distrital. Por medio de la cual se designa el Líder del Gobierno en Línea de la Veeduría Distrital.

Resolución 318 de 2016 de la Veeduría Distrital. Por medio de la cual se adopta la Política de Tratamiento y Protección de Datos Personales de la Veeduría Distrital.

Circular 27 de 2014 de la Alta Consejería Distrital TIC. Estrategia Líderes de Gobierno en Línea del Distrito Capital.

Programa de Gestión Documental –PGD-. Veeduría Distrital. GD-PL-2.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Veeduría Distrital, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un modelo de seguridad y privacidad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para la Veeduría Distrital, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a los funcionarios, contratistas y terceros, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Modelo de Seguridad y Privacidad de la Información MSPI estarán determinadas por las siguientes premisas:

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

La Veeduría Distrital considerará como información aquella que se maneje en virtud de los procesos de la Entidad y de los proyectos de inversión.

1.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

• La Veeduría Distrital ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.

• La Veeduría Distrital protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio y proyectos de inversión, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la misma. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• La Veeduría Distrital protegerá su información institucional de las amenazas originadas por factores internos y externos que afecten cualquiera de sus principios.

• La Veeduría Distrital protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• La Veeduría Distrital controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• La Veeduría Distrital implementará control de acceso a la información, sistemas y recursos de red.

• La Veeduría Distrital garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• La Veeduría Distrital garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• La Veeduría Distrital garantizará la confiabilidad y el nivel de sensibilidad de la información que provenga de terceros y de sistemas de información con los cuales se tenga interoperabilidad.

• La Veeduría Distrital garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

• La Veeduría Distrital actualizará la política teniendo en cuenta la valoración de riesgos de procesos y de seguridad de la información.

En caso de incumplimiento de las Políticas de Seguridad y Privacidad de la información, la Veeduría Distrital, iniciará las investigaciones disciplinarias correspondientes, conforme a lo dispuesto en la Ley 734 del 2002.

2. POLITICAS ESPECÍFICAS

2.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Veeduría Distrital definió en el documento “Roles y Responsabilidades de Seguridad de la Información”, los diferentes actores con sus funciones en materia de Seguridad de la Información en la Entidad.

Se crea el Comité de Seguridad de la Información, encargado entre otras funciones, de proponer las políticas en materia de seguridad de la información y proponer estrategias para la divulgación de la política a todos los funcionarios y contratistas de la entidad.

2.2 GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Veeduría Distrital con el liderazgo de los procesos de Direccionamiento estratégico, Gestión TIC y Gestión Documental, identificará, clasificará y etiquetará los activos de información de la Veeduría Distrital mediante metodología que estos procesos establezcan.

Los funcionarios y/o contratistas deberán evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

Todo funcionario o contratista que se desvincule temporal o definitivamente de la Veeduría Distrital, deberá realizar la devolución de activos de información que tenga asignada y en custodia, físico o virtual, al supervisor o jefe inmediato, requisito para firmar el formato de retiro de funcionario o contratista TH-FO-12 y GAB-FO-29.

La información que se grabe en los portátiles destinados para las presentaciones es de responsabilidad de quien use el equipo, Gestión TIC hará mantenimiento a dichos equipos y eliminará cada quince días los archivos utilizados.

Es de exclusiva responsabilidad de cada funcionario tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio.

La información que reposa en los dispositivos móviles asignados por la Entidad (Directivos) es responsabilidad de quien tiene en uso el dispositivo móvil. Cuando se entreguen estos dispositivos, el proceso de bienes y servicios deberá eliminar los datos contenidos en el dispositivo.

La Veeduría Distrital tendrá fragmentada la red, en mínimo, 3 unidades:

Y:\ para guardar información que pueden ver todos los usuarios de la Veeduría Distrital de manera temporal, la cual se depurará por el proceso de Gestión TIC cada 15 días.
G:\ para guardar información por cada centro de gestión de la Entidad, la cual deberá estar organizada de acuerdo con las Tablas de Retención Documental.
U:\ para que el usuario logueado guarde su información.

El proceso de Gestión TIC será el encargado de realizar backup de la información guardada en las unidades Y, G y U. El backup de la unidad C (disco duro del equipo) será responsabilidad del usuario.

2.3 CONTROL DE ACCESO

La creación, reactivación o desactivación de usuarios de la red o sistemas de información; al igual que los roles y permisos otorgados, los realizará Gestión TIC a través de solicitud enviada por correo electrónico del jefe inmediato y/o supervisor.

El proceso de Gestión TIC de la Veeduría Distrital es quien gestionará el control de acceso a través de usuario y contraseña, a la red de la Entidad, correo electrónico y a los sistemas de información que administre, para ello, diligenciará por cada usuario el formato de Administración de Usuarios, TIC-FO-01 y seguirá Procedimiento Administración de Usuarios para Herramientas Tecnológicas y Control de Accesos TIC-PR-04.

En caso de retiro temporal o definitivo de cualquier servidor público o contratista, se deberá deshabilitar o actualizar los privilegios en los sistemas a los que el usuario estaba autorizado en caso de encargos o suplencia temporal, previa solicitud por correo electrónico, enviada por el jefe inmediato y/o supervisor al responsable del proceso Gestión TIC.

Gestión TIC debe mantener actualizada la documentación relacionada con la administración de usuarios. Formato TIC-FO-01 y monitoreará la asignación de permisos y roles otorgados a los usuarios.

Las contraseñas serán de uso personal e intransferible, deberán ser cambiadas con frecuencia. Evitar que las contraseñas sean fáciles de recordar; no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios); estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos; si son temporales, cambiarlos la primera vez que se ingrese.

Es responsabilidad del funcionario o contratista el uso o tratamiento dado a su usuario y contraseña.

El administrador de la red, configurará los servidores para que semestralmente el sistema solicite al usuario cambio de contraseña.

No es recomendable la utilización de la opción 'recordar contraseña'.

La instalación de software en los equipos de cómputo de la Entidad, será realizada a través del usuario del administrador de la red. Toda solicitud al respecto, debe gestionarse a través de Gestión TIC quien aprobará su instalación.

2.4 NO REPUDIO

Para ingresar a los sistemas de información que administra la Veeduría Distrital, los funcionarios y contratistas deben tener su propio usuario y contraseña, se entenderá que las transacciones que se generen con este, son avaladas por el servidor que tiene a su cargo dicho usuario.

2.5 PRIVACIDAD Y CONFIDENCIALIDAD

La Veeduría Distrital aplicará la Política de Seguridad de Datos Personales, adoptada mediante Resolución 318 de 2016.

La Veeduría Distrital consignará como obligación general en todos los contratos el siguiente texto: "*Mantener reserva sobre la información que tenga acceso con ocasión del cumplimiento de las obligaciones contractuales. En este sentido* ***EL CONTRATISTA*** *deberá abstenerse de publicitar o utilizar información que se le entregue, como resultado del desarrollo del contrato.*"

Todo funcionarios y/o contratista que ingrese a la Entidad, debe leer y firmar el compromiso de manejo de la información pública clasificada y/o reservada y tratamiento de datos personales, anexo a esta política.

2.6 SEGURIDAD FISICA Y DEL ENTORNO

Los equipos de cómputo y servidores de la Veeduría Distrital, ubicados en el centro de cómputo, deberán ser mantenidos en un ambiente seguro y protegido por: controles de acceso y seguridad física, detección de incendio y sistemas de extinción de conflagraciones y sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

El acceso al centro de cómputo deberá ser restringido y sólo a personal autorizado a través de sistema biométrico.

No se permitirá ingerir alimentos o bebidas en las instalaciones del Centro de Cómputo ni en los puestos de trabajo donde se encuentren equipos de cómputo.

La Veeduría Distrital contará con equipos de protección (firewall) desde y hacia internet para proteger la integridad y confidencialidad de la información.

Ningún usuario de la Veeduría Distrital podrá instalar software sin licencia, solo podrá ser autorizado por el Líder Gestión TIC, quien revisará en los mantenimientos preventivos este tema, de acuerdo con lo establecido en el Procedimiento Mantenimiento Correctivo y Preventivo TIC-PR-03.

Ningún equipo podrá ser retirado de su sitio sin autorización del responsable del proceso de Gestión TIC y haber diligenciado el formato de Traslado de Elementos ABS-FO-03.

Todo computador, servidor, dispositivo de comunicaciones como switches, enrutadores o cualquier otro hardware que requiera ser conectado a la red, debe tener la autorización y supervisión del Líder de Gestión TIC.

Todo personal que ingrese o salga de la Veeduría Distrital tendrá que hacer uso de la tarjeta de aproximación que permita tener un control de acceso del personal, ésta tarjeta debe estar previamente configurada por los funcionarios de Gestión TIC, con los datos básicos personales de identificación. Al retirarse de la Entidad, esta tarjeta debe ser devuelta para su nueva configuración. En caso de pérdida, se debe seguir las instrucciones de la administración del edificio.

Los funcionarios y contratistas de la Veeduría Distrital evitarán colocar encima o cerca de los computadores ganchos, clips u otros elementos o comida que puedan caer accidentalmente dentro del equipo y afectar su buen funcionamiento.

Con el fin de ahorrar energía, los funcionarios y contratistas apagarán las pantallas si se retiran temporalmente de su puesto y apagarán totalmente el equipo al finalizar la jornada laboral.

La Veeduría Distrital a través del proceso de Gestión TIC, realizará mantenimiento preventivo dos veces al año a los equipos de cómputo de propiedad de la Entidad, atendiendo el procedimiento establecido para ello, TIC-PR-03.

Ningún funcionario o contratista está autorizado para efectuar algún tipo de intervención, reparación y/o modificación en un equipo a su cargo. El mantenimiento preventivo y correctivo debe ser realizado por personal del proceso de Gestión TIC.

Todos los equipos de cómputo propios serán incluidos en la póliza colectiva de la Veeduría Distrital y se debe garantizar que el proveedor de los equipos arrendados asuma los riesgos por pérdida de los mismos.

La Veeduría Distrital revisará las condiciones de seguridad física y del entorno de los equipos y puestos de trabajo de los teletrabajables, se les garantizará la accesibilidad a los aplicativos y sistemas que requieran para su trabajo.

Cuando se requiera sacar un equipo de cómputo de la Entidad, se deberá diligenciar el Formato de Autorización de Salida de Elementos ABS-FO-01

La información que reposa en medios físicos como el papel, en lo posible debería permanecer guardada en sitios bajo llave o archivadores mientras no se esté haciendo uso de ella o se termine la jornada laboral. El manejo de esta información es responsabilidad de quien la tenga en custodia.

Los escritorios deberán permanecer libres de papeles una vez culmine la jornada laboral.

2.7 SEGURIDAD DE LAS OPERACIONES

El proceso de Gestión TIC de la Veeduría Distrital realizará seguimiento al tráfico de la red especialmente cuando se tenga evidencia de actividad inusual o detrimentos en el desempeño.

Todos los equipos de cómputo de la Entidad deberán tener instalado software de antivirus licenciado y actualizado.

El proceso Gestión TIC, mantendrá actualizado el procedimiento de Administración de la red y comunicaciones de la Veeduría Distrital.

El proceso de Gestión TIC registrará en el formato de Bitácora Centro de Cómputo TIC-FO-06, todo evento que ocurra en el centro de cómputo.

La Veeduría Distrital a través del proceso de Gestión TIC establecerá los siguientes procedimientos y/o guías: Mantenimiento Preventivo, Administración de Usuarios, Copias de Seguridad y Restauración de Información, Administración de la red y comunicaciones.

La Veeduría Distrital a través del proceso de Gestión TIC establecerá e implementará controles para evitar la descarga de software no autorizado, la infección con código malicioso proveniente de internet y el acceso a sitios catalogados como restringidos y de alta peligrosidad.

Los funcionarios y contratistas de la Entidad deben evitar la descarga de software, archivos, música, juegos o videos desde internet que puedan saturar el canal dedicado de internet, disminuir la velocidad de transmisión o llegar a ocasionar algún daño en el equipo.

Los funcionarios y contratistas usarán los recursos y servicios de internet para asuntos institucionales. El uso personal no debe interferir con la operación eficiente de los sistemas de la Entidad, ni con los deberes y obligaciones de funcionarios y/o contratistas.

La Veeduría Distrital establecerá un procedimiento para la publicación y actualización de la información en la Página Web, basada en la Ley 1712 de Transparencia y acceso a la información.

El acceso a internet a través del WIFI de la Veeduría Distrital sólo será autorizado para computadores portátiles y la clave solo puede ser ingresada por personal autorizado de Gestión TIC.

Todos aquellos dispositivos de interconexión y servidores que conforman la plataforma tecnológica de la entidad y que lo ameriten, deben tener direcciones IP fijas. La asignación de estas direcciones debe estar documentada al detalle y mantenida por el administrador de la red de la entidad.

La Veeduría Distrital debe contar con un Plan de Contingencias tecnológico debidamente probado y actualizado que garantice la continuidad de los sistemas de misión crítica en la plataforma de la entidad, que cubra desde aplicativos y máquinas hasta sitio de operaciones.

2.8 COPIAS DE SEGURIDAD Y RESPALDO

Se deberán realizar y mantener copias de seguridad de la información de la Veeduría Distrital, bases de datos e información de las unidades de red, dentro y fuera de la Entidad.

La Veeduría Distrital a través del proceso de Gestión TIC, establecerá un procedimiento o guía para realizar copias de seguridad, restauración y migración de la información.

Todos los sistemas de información que componen la plataforma de la entidad, deberán incluir la documentación necesaria para garantizar la ejecución de tareas de recuperación de la información.

El proveedor del Hosting deberá tener mínimo 2 copias de seguridad de la información contenida en las páginas web de la Entidad.

Cuando haya rotación de equipos de cómputo, se eliminará la información, pero antes el usuario realizará backup del disco duro y el proceso de Gestión TIC a la información contenida en las unidades de red.

2.9 DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Los desarrolladores de software deberán garantizar ambientes seguros de desarrollo, pruebas y producción, materializado en obligaciones específicas de los contratos.

Los desarrolladores de software deberán conocer e implementar la guía de estilo e imagen institucional en aspectos en los que aplique e implementar la metodología propuesta para el desarrollo de sistemas de información.

Los desarrolladores de software deberán especificar las carpetas y archivos a los cuales se les debe sacar copias de seguridad.

Cada sistema de información o aplicativo debe mantener actualizado su documentación.

En los contratos de los proveedores, se debe establecer como obligación específica la entrega de la documentación necesaria para la administración y funcionamiento del sistema o aplicativo.

Los proveedores de software deberán realizar transferencia de conocimiento, obligación específica que debe estar consignada en el contrato.

2.10 REGISTRO Y AUDITORIA

Todos los sistemas y/o aplicativos deben generar logs o trazas de auditoría, para los desarrollos de software que se generen a partir de la divulgación de esta política, se debe establecer este punto como obligación contractual.

Todos los log del sistema y de las aplicaciones deben mantenerse en forma segura, de tal forma que evite el acceso no autorizado esta información y deberán analizarse para determinar si existen intentos de vulneración del sistema.

La Veeduría Distrital realizará seguimiento a la implementación de la Política de Seguridad de la Información.

2.11 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Veeduría establecerá un mecanismo para el reporte, registro y tratamiento de los incidentes de seguridad de la información que se presenten en la Entidad.

2.12 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Todos los funcionarios y contratistas de la Veeduría Distrital deben recibir sensibilización para tomar conciencia de la seguridad de la información y sus responsabilidades.

Se debe fortalecer la cultura del manejo de contraseñas para los diferentes sistemas, aplicativos o herramientas que tiene la Entidad.