



**ALCALDÍA MAYOR
DE BOGOTÁ D.C.**

SECRETARÍA DE DESARROLLO ECONÓMICO

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

**Bogotá Distrito Capital
SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO**

Abril de 2019




MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

Tabla de contenido

1.	INTRODUCCION	4
2.	OBJETIVO	4
3.	ALCANCE.....	4
4.	MARCO LEGAL	5
5.	DOCUMENTOS DE REFERENCIA.....	6
6.	TERMINOS Y DEFINICIONES.....	7
7.	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION	11
8.	POLITICAS SEGURIDAD DE LA INFORMACIÓN.....	11
8.1.	Políticas Generales	11
8.2.	Políticas de Firewall.....	13
8.3.	Políticas de Internet.	14
8.4.	Políticas de Áreas Seguras.....	15
8.5.	Políticas Base de Datos.....	15
8.6.	Políticas de BACKUP.	16
8.7.	Política Acceso Físico.....	17
8.8.	Política Transferencia de información.	17
8.9.	Política Acceso remoto.....	18
8.10.	Política Acceso inalámbrico.....	18
8.11.	Política Acceso múltiple factor de autenticación.....	19
8.12.	Política Dispositivos móviles.	19
8.13.	Política Transición de IPv4 a IPv6.	20

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

8.14.	Política Funcionarios	21
8.15.	Política de Mejora Continua.....	21
8.16.	Política de Evaluación del Desempeño	22
8.17.	Política Uso Compartidos en la Red (Carpetas).....	22
8.18.	Política Escritorio Limpio	23
8.19.	Política de Seguridad en la Nube.....	24
8.20.	Política Gestión del Incidente.....	24
8.21.	Política Gestión del Riesgo	25
8.22.	Política Controles Criptográficos	26
9.	SANCIONES A LAS VIOLACIONES DE LA POLITICA DE SEGUIRADA DE LA INFORMACION.....	27
10.	ACUERDO DE CONFIDENCIALIDAD	30
11.	CONTROL DE CAMBIOS	30

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

1. INTRODUCCION

El manual de Políticas de Seguridad de la Información establece los lineamientos y políticas administrativas, técnicas y legales, las cuales deben ser adoptadas todos los funcionarios, contratistas, proveedores, y todo personal externo que utilice los servicios de tecnologías de la información que ofrece la Entidad.

Las políticas de seguridad descritas, se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia

2. OBJETIVO


El objetivo del presente documento es establecer las políticas en seguridad de la información de la Secretaria Distrital de Desarrollo Económico, con el fin de regular la gestión de la seguridad de la información, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información

3. ALCANCE

Comprende el cumplimiento de los estándares de seguridad bajo las normas de sistema de gestión seguridad informática SGSI ISO 27001, los requerimientos establecidos de seguridad por MINTIC y legislación vigente.


Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y proveedores que presten sus servicios o tengan algún tipo de vinculación con la Secretaria Distrital de Desarrollo Económico, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de seguridad y protección de los activos de información.

Debe ser conocida y de obligatorio cumplimiento por parte de funcionarios, contratistas y terceros que acceden al uso al uso de las plataformas y servicios tecnológicos que preste la Entidad.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

4. MARCO LEGAL


TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Ley	1273	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".	2009	X		
Decreto	235, Art.1-4	Por el cual se regula el intercambio de información entre Entidades para el cumplimiento de funciones pública	2010	X		
Ley	1581	Por el cual se dictan disposiciones generales para la protección de datos personales.	2012	X		
Decreto	1377	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.	2013	X		
Ley	1712	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.	2014	X		
Decreto	2573	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	2014	X		
Decreto	1074	Por el cual Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.	2015	X		
Decreto	415	Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.	2016	X		

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
DECRETO	1008	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones	2018	X		
LEY	1928	"por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest.	2018	X		

5. DOCUMENTOS DE REFERENCIA

Tipo Documento	Descripción del documento
Modelo de Seguridad y Privacidad de la Información	Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información del El Ministerio de Tecnologías de la Información y las Comunicaciones
Conpes 3854	Lineamientos de seguridad digital del Consejo Nacional de Política Económica y Social República de Colombia, Departamento Nacional de Planeación
Norma Técnica Internacional ISO 27001, 27002, 27005	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

6. TERMINOS Y DEFINICIONES

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

Amenaza: situaciones que desencadenan en un incidente en la Entidad, realizando un daño material o pérdidas inmateriales de sus activos de información

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Áreas seguras: Lugares donde se encuentra localizada la información crítica para la organización, éstas estarán protegidas por un perímetro de seguridad y por los controles de acceso pertinentes.

Back-up (copia de respaldo): Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CDs), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

Base de datos: Conjunto de archivos de datos recopilados, definidos, estructurados y organizados con el objeto de brindar información.


Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Cortafuegos: (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Contraseña: Cadena de caracteres que permite validar la autenticidad de una cuenta de usuario.

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

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Cuenta de Usuario: Credencial que identifica a un usuario para autenticarse sobre una plataforma tecnológica.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

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


Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

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

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

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

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.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

Logs: Registro oficial de eventos, durante un rango de tiempo en particular, en donde se almacena toda actividad que se hace en el equipo monitoreado.

Niveles de respaldo de información: Hace referencia a los diferentes ambientes en los cuales la copia de seguridad se guarda de manera oportuna con el fin de tener varios niveles de recuperación de la información en caso de desastre.

No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Parche: Actualizaciones que se aplican a un programa de software para corregir o mejorar su funcionalidad.

Plan de Contingencia: Procedimientos alternativos de una Entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.

Plan de Pruebas de Recuperación: Pruebas de recuperación de copias de respaldo programadas con el fin de verificar la consistencia e integridad de las copias de respaldo.


Plataforma Tecnológica: Una plataforma tecnológica es una agrupación de equipamientos técnicos y humanos destinados a ofrecer unos recursos tecnológicos para la realización de las tareas de los usuarios

Política: Instrucciones mandatorias que indican la intención y la directriz de la alta gerencia respecto a la operación de la Entidad.

Política de escritorio despejado: La política de la entidad que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

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 consecuencias.

Riesgo residual: nivel restante de riesgo después del tratamiento del riesgo.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

Servicios de Servidores: son todas aquellas herramientas o aplicaciones de software que están disponibles para apoyar la gestión de la Entidad, algunos servicios disponibles son: Servicios de dominio de Active Directory, Servidor de aplicaciones, Servidor DHCP, Servidor DNS, Servicios de archivos, Hyper-V, Servicios de acceso y directivas de redes.

Servidor: En redes locales se entiende como el software que configura un PC u otro computador como servidor para facilitar el acceso a la red y sus recursos.

Sistema de gestión de la 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, basándose en un enfoque de gestión del riesgo y de mejora continua.

Sistema Operativo (SO): Es el software básico de un computador que provee una interface entre el resto de programas, los dispositivos de hardware y el usuario.

Software Antivirus: Herramienta cuyo objetivo es detectar y eliminar virus informáticos.


TI: se refiere a tecnologías de la información

TIC: se refiere a tecnologías de la información y comunicaciones

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

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

Valoración del riesgo: proceso global de análisis y evaluación del riesgo.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

Virus: Son programas creados para infectar sistemas y otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente.

Vulnerabilidad: debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas. Potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información.

7. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION


La información de la entidad se considera como uno de los principales activos de la Entidad, y como tal, debe ser protegida adecuadamente con controles administrativos, técnicos y legales de forma que se evite que persona o medio físico no autorizado pueda acceder, operar, distribuir la información, atento contra la integridad, confidencialidad y disponibilidad de los activos de información.

La Secretaria Distrital de Desarrollo Económico orienta sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los servicios de tecnologías de la información y de los activos de información de la Entidad, tomando como base que la efectividad de esta política depende finalmente del comportamiento de los usuarios y del cumplimiento de los controles establecidos en las políticas de seguridad descritas en el presente documento, fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 y el modelo de seguridad y privacidad de la información de MINTIC.


8. POLITICAS SEGURIDAD DE LA INFORMACIÓN

8.1. Políticas Generales

- ✓ El comité de seguridad está encargado de aprobar las modificaciones que se realicen al manual de seguridad de la información y aquellos documentos de alto impacto relacionados con la seguridad de la información, además, se revisara una vez al año o cuando existan cambios en el objetivo del negocio o en el entorno del riesgo.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019


- ✓ El área de IT es la única facultada para administrar y configurar el acceso a los recursos de la plataforma tecnológica en la entidad de acuerdo a la descripción de cargo.
- ✓ Todo aquel elemento o equipo de hardware retirado de las instalaciones de la entidad debe tener su respectiva orden de salida con la firma del líder de proceso o administrador de infraestructura y gerencia administrativa y financiera.
- ✓ Se monitorea constantemente el tráfico entrante a la plataforma de la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO a través de una herramienta para detectar posibles intrusos.
- ✓ El manejo de la información y los servicios en la nube están autorizados siempre y cuando se cumpla con los acuerdos de confidencialidad, integridad y disponibilidad, además, que exista un contrato de servicio y el proveedor cumpla con los requerimientos de las normas y legislaciones vigentes.
- ✓ Los datos que se extraiga de las bases de datos y que corresponda a información de los clientes a través de diferentes medios removibles deben quedar cifrada y bajo custodia en condiciones de seguridad.
- ✓ Para el formato de Perfil de seguridad se identifica por cargos los controles de acceso, el software autorizado, los permisos de los productos corporativos y no corporativos, el nivel de acceso a internet, los permisos sobre medios removibles, acceso a los tipos de información y acceso múltiple factor de autenticación.
- ✓ Se retira y se da de baja aquellos equipos (servidores, desktop o portátiles) que, por sus características técnicas, software base, soporte han cumplido su vida útil y son punto vulnerable de seguridad.
- ✓ Se realiza al año dos análisis de vulnerabilidades internas / externas y una prueba de Ethical hacking a todos los servicios y servidores del ambiente de producción de lo cual las vulnerabilidades detectadas se atenderán aquellas que son críticas, altas y medias.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

- ✓ Para la asignación de privilegios de personal nuevo, su acceso estará sujeto a la aprobación y solicitud del jefe inmediato.
- ✓ Se posee implementado el documento “Seguridad y privacidad de la información” que contiene las políticas y procedimientos que dan cumplimiento a las leyes 1581 del 2012 y 1266 del 2008 para tratamiento de datos.
- ✓ Para los accesos de carpeta compartida como el file server, este se diligencia el formato de “permisos de acceso al File Server” a través de la herramienta de gestión dirigido al oficial de seguridad para su aprobación.
- ✓ Se posee implementado por el directorio activo una política de escritorio que aplica para todos los servidores, computadores y portátiles de la entidad.
- ✓ Por parte del área de seguridad de la información se realizará auditorias en los activos de criticidad alta cada 6 meses.

8.2. Políticas de Firewall


- ✓ La SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO tiene dispositivos de seguridad perimetral (Firewall) en todas las sedes donde tiene infraestructura y controla el tráfico y seguridad de la información.
- ✓ Al realizar cambios o actualizaciones en el firewall se realiza un backup en un medio externo con el fin de garantizar la integridad e inmediato retorno a un escenario funcional.
- ✓ Se registra en la bitácora de firewall todo cambio realizado en la consola de control perimetral.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

- ✓ El intercambio de información con entidades se hace a través de una conexión VPN punto a punto cumpliendo con los requerimientos de cifrado y seguridad que exige la norma y legislación vigente.
- ✓ Para todos los equipos de escritorio de la entidad se tiene habilitado el servicio de firewall local de acuerdo con las políticas de la herramienta de antimalware.
- ✓ Para todo firewall nuevo que se conecte a la plataforma tecnológica se incluye en los diagramas de red, guías de hardening y configuración. La última versión liberada de firmware esta aplicada.
- ✓ Por parte del área de seguridad de la información se realizará auditorias en los activos de criticidad alta cada 6 meses.

8.3. Políticas de Internet.

- ✓ El uso de internet es únicamente para actividades relacionadas con las funciones del negocio, manteniéndose las restricciones de seguridad establecidas por la entidad.
- ✓ El uso de servicios de mensajería instantánea solo se utilizará para actividades de la entidad y el acceso a las redes sociales estará autorizado solo a un grupo restringido de usuarios teniendo en cuenta su perfil.
- ✓ Solo se permite el acceso a la red de internet corporativa a los equipos que están en el inventario de activos.
- ✓ Para clientes, visitantes como aliados estratégicos, consultores, freelance y proveedores, se le habilitará el acceso a la red pública de internet mediante una solicitud vía correo electrónico o herramientas de gestión del funcionario responsable al oficial de seguridad para su respectiva aprobación.
- ✓ No se permite el uso de los recursos de internet corporativo para la descarga, distribución y/o reproducción de música, videos y similares.


MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

8.4. Políticas de Áreas Seguras

- ✓ Se establece como áreas seguras aquellas ubicaciones sobre las cuales existen mecanismos de control que garanticen la seguridad de la información solo a personal autorizado. Estas son:
 - Sede Sta Helenita.
 - Plataforma los luceros
 - Data Center.
 - Área de oficina.
- ✓ Para el Data Center2 (Ubicación remota) se tiene establecido contractualmente las condiciones que contemplan las políticas y procedimientos de seguridad.
- ✓ Para los ingresos a los data center, se tiene establecido un formato de ingreso permanente en el horario 7 * 24 y la autorización se confirma mensualmente por el oficial de seguridad.
- ✓ Para el caso de ingreso por parte de proveedores, clientes o visitantes se tramita por el responsable de la actividad mediante una solicitud al oficial de seguridad para la autorización de ingreso, donde se especifica el nombre de la persona, número de cédula, fecha, hora, duración y actividad a realizar por parte del responsable de la actividad.

8.5. Políticas Base de Datos.


- ✓ La información de los clientes que se maneja en la plataforma tecnológica se tiene en línea los 2 últimos años con corte al 01 de enero de cada año.
- ✓ La información correspondiente a los años anteriores deberá ser entregada al cliente mediante carta y posteriormente eliminada a excepción que exista una cláusula contractual donde se tenga la responsabilidad de custodia o almacenamiento por más tiempo.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

- ✓ Se realizan planes de mantenimiento de la información de tal modo que las bases de datos de producción tienen un tamaño menor a 500 GB.
- ✓ Una vez cumplido este tiempo se deberá hacer entrega al cliente mediante acta y posteriormente eliminación dejando acta firmada.

8.6. Políticas de BACKUP.

- ✓ Los funcionarios son responsables de realizar y actualizar los respaldos de la información que tiene en el equipo asignado mínimo cada 30 días.
- ✓ Para los cargos de la alta dirección, se realizará los backup de manera automática.
- ✓ Una vez al mes se realiza la restauración del backup full de las bases de datos de producción y de los servidores definidos como críticos.
- ✓ Bajo ninguna eventualidad ni solicitud se entregará copia de las bases de datos y servidores en dispositivos como discos duros externos, USB, CD, DVD. Salvo por la solicitud escrita del cliente y por la aprobación del oficial de seguridad.
- ✓ El área de TI garantiza los respaldos de información que reposa en los ambientes productivos de la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO y de recuperación de desastres bajo los RTO y RPO definidos en los acuerdos contractuales.
- ✓ Se realiza un backup diario full de las base de datos en la herramienta de backup de la entidad.
- ✓ Se realiza un backup de los logs, cada 2 horas de las bases de datos clasificadas como críticas.
- ✓ El backup generado de las bases de datos críticas, se almacena en una unidad externa de almacenamiento debidamente cifrado.


MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

- ✓ Para el retiro de un funcionario de la entidad se realiza un backup de la información por parte del área de TI tan pronto se reciba el portátil o equipo asignado por la entidad. Además, se realiza la cancelación de la cuenta en el directorio activo

8.7. Política Acceso Físico.

- ✓ El acceso al data center está restringido únicamente al personal autorizado y bajo la supervisión del área de TI con previa aprobación del oficial de seguridad.
- ✓ Para la autorización de acceso al data center se diligencia el formato de ingreso y este debe estar autorizada y tramitada por el oficial de seguridad quien mediante comunicación escrita notificará la autorización con fecha y hora de ingreso.
- ✓ Para el acceso al data center se tiene dos copias, las cuales están a cargo del área de TI y la otra en custodia por el subdirector de informática y sistemas en un lugar seguro.
- ✓ Para el monitoreo de las instalaciones, se cuenta con un circuito cerrado de televisión, con un periodo de conservación de la información de mínimo 2 meses.
- ✓ Todo personal que transite dentro de las instalaciones de la entidad portaran de manera visible el carnet que lo identifica como funcionario, visitante o consultor.
- ✓ Para los visitantes, el funcionario que autoriza su ingreso lo acompaña de manera permanente mientras permanezca dentro de las instalaciones de la entidad.
- ✓ Para acceso a las áreas seguras se cuenta con un dispositivo de control de acceso con huella donde quedan registrado el ingreso de los funcionarios de la entidad.

8.8. Política Transferencia de información.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019


- ✓ Para la transferencia de información se utiliza sitio seguro SFTP asignando un usuario y contraseña.
- ✓ Para la entrega de información, se establece mecanismos de protección de la información como puertos seguros, cifrado y la contraseña se entrega por otro medio.

8.9. Política Acceso remoto

- ✓ El acceso remoto a los servidores críticos y bases de datos, se realizan por el líder, administrador de TI.
- ✓ Se debe tener implementado como múltiple factor de autenticación aplicaciones del dispositivo Mobile o de terceros mediante la cual se accederá a la plataforma tecnológica de la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO.
- ✓ Se establece el tiempo de desconexión por inactividad de la sesión es de 10 minutos.
- ✓ El oficial de seguridad autoriza los accesos remotos de los empleados y proveedores.
- ✓ Está prohibido copiar, mover o almacenar información de las base de datos de los servidores cuando se acceda mediante tecnologías de acceso remoto.

8.10. Política Acceso inalámbrico.

- ✓ Los puntos de acceso inalámbrico autorizados por la entidad son la red identificada como Plaza Artesanos SDDE para los funcionarios de la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO y la red identificada como Invitados para los usuarios externos.
- ✓ No está permitido la utilización y conexión de la red inalámbrica de la entidad para a actividad diferente a la labor del empleado (se aplica la Políticas de Internet).


MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

8.11. Política Acceso múltiple factor de autenticación.

- ✓ El acceso a los servidores y base de datos, se realizará a través múltiple factor de autenticación, por previa autorización del oficial de seguridad.
- ✓ Está prohibido copiar, mover o almacenar datos en discos duros locales, dispositivos electrónicos extraíbles al acceder con tecnologías de acceso remoto.

8.12. Política Dispositivos móviles.


- ✓ Los dispositivos móviles autorizados a conectarse a la red inalámbrica corporativa (WLAN) son los portátiles que hacen parte del inventario de activos o equipos propios de la alta dirección.
- ✓ Los dispositivos móviles autorizados para contener, administrar o manejar información privada y/o confidencial de la entidad son de propiedad de la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO.
- ✓ El funcionario al cual se le asigna el equipo móvil es responsable por su seguridad y correcta operación dentro de la red interna y en lugares públicos.
- ✓ Los portátiles están permanentemente asegurados dentro de las oficinas con una guaya que no permita su movilidad sin previa autorización.
- ✓ Todo equipo móvil como portátil, Tablet, disco duro externo que ingrese a las instalaciones de la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO, se debe registrar.
- ✓ La entidad ha establecido un procedimiento para el transporte de los equipos portátiles, servidores u otro medio de transporte de información.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

- ✓ Los dispositivos móviles personales de los visitantes o funcionarios que requieran tener acceso a una red inalámbrica para el acceso a la red pública de internet deben solicitar al oficial de seguridad mediante un correo electrónico el acceso.

8.13. Política Transición de IPv4 a IPv6.

- ✓ Debe ser estructurado con esquemas de seguridad y privacidad de la información, de las cuales debe cumplir con las políticas de confidencialidad, disponibilidad e integridad.
- ✓ Debe prepararse un rollback, para los casos de indisponibilidad en los servicios.
- ✓ Se debe revisar los procesos de transición hacia el nuevo protocolo, analizando los niveles de impacto en los servicios como:
 - Directorio Activo
 - DNS
 - Correo Electrónico
 - Host – DHCP
 - Proxy
 - Aplicaciones
 - Web
 - Gestión y Monitoreo
- ✓ Mantener los mismos nombres de servicios utilizados sobre la red tanto para IPv4 como para IPv6.
- ✓ No usar direcciones IPv6 literales en el desarrollo del software y en el uso de librerías de software.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019


- ✓ Analizar y documentar los riesgos asociados a la transición de IPv4 a IPv6.

8.14. Política Funcionarios

- ✓ En los puestos de trabajo de los funcionarios no se tiene documentos clasificados como privado, confidencial o secreto.
- ✓ Se debe retirar inmediatamente cualquier documento enviado a las impresoras que contenga información sensible, secreta o confidencial.
- ✓ Los documentos electrónicos o físicos que contienen información sensible, secreta, privada o confidencial se guarda en condiciones de seguridad y con acceso de lectura por personal autorizado.
- ✓ Los funcionarios de la entidad son responsables del cumplimiento de las políticas de seguridad de acuerdo con el alcance que se define en este documento.

8.15. Política de Mejora Continua

- ✓ De acuerdo con las auditorías realizadas, la entidad deberá realizar actividades para controlar y corregir los hallazgos o no conformidades presentadas.
- ✓ Se debe evaluar y revisar los hallazgos o no conformidades desde la causa del problema con el fin de mitigarlo
- ✓ Se debe revisar las lecciones aprendidas con el fin de que no se repita las no conformidades encontradas.
- ✓ Generar e implementar tareas o actividades, relacionadas con un ticket para llevar el seguimiento en las siguientes auditorias.


MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

8.16. Política de Evaluación del Desempeño

- ✓ Programar, revisar y ejecutar auditorias para validar la eficacia del MSPI.
- ✓ Generar medición de la efectividad de Controles.
- ✓ Controlar y revisar las valoraciones de los riesgos en la entidad.
- ✓ Realizar seguimiento de los indicadores de gestión del MSPI.
- ✓ Actualizar los planes de seguridad.
- ✓ Llevar Registros de las actividades del MSPI.
- ✓ Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).


8.17. Política Uso Compartidos en la Red (Carpetas)


- ✓ Se prohíbe almacenar o intercambiar archivos de audio en cualquier formato (WAV, Mp3, etc.) para fines personales.
- ✓ Se prohíbe almacenar o intercambiar archivos de videos y/o fotografías personales en cualquier formato.
- ✓ Se prohíbe guardar archivos que no sean de uso laboral.
- ✓ Antes de eliminar cualquier información del recurso compartido, verifique con el administrador o propietario de la información que esta va hacer borrada.

<p>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO</p>			 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small></p>
<p>DOCUMENTO CONFIDENCIAL</p>			
<p>Código:</p>	<p>Versión:</p>	<p>Fecha creación:</p>	<p>Fecha actualización: 01/04/2019</p>

- ✓ Se debe guardar únicamente información que se está trabajando.
- ✓ El usuario de la unidad del recurso compartido debe reportar al jefe inmediato si encuentra información que no es de su área.
- ✓ Si en las carpetas se encuentran archivos de música, fotos, videos, etc. de carácter personal, estos serán borrados inmediatamente sin notificarle al usuario.
- ✓ El tiempo de retención de la información es de 8 meses, una vez transcurrido este tiempo se realiza depuración de la información.
- ✓ El no cumplimiento de esta política atenta contra la seguridad de la información y es sancionado de acuerdo con el procedimiento definido.

8.18. Política Escritorio Limpio

- ✓ Ejecutar el bloqueo de pantalla siempre que el responsable o usuario del equipo se ausente de la terminal, ejecutando la combinación de teclas Windows () + L.
- ✓ Cerrar sesiones de usuario cuando no se requiera los servicios del equipo durante tiempos superiores a 3 minutos.
- ✓ En caso de usar medios físicos de autenticación tipo tokens o tarjetas inteligentes se deberá definir en las políticas de la maquina o de dominio el bloqueo de la estación al retirar el medio físico.
- ✓ Ejecutar el procedimiento de clasificación, etiquetado y manejo de la información de forma segura y ordenada en rutas de acceso recordables.
- ✓ En la pantalla no debe permanecer ningún icono, acceso directo o archivo, esta debe estar completamente despejada.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019


- ✓ Para el personal operativo en la pantalla solo deben permanecer los iconos de acceso directo a las diferentes herramientas de gestión de la solución, no deben permanecer archivos digitales de ningún tipo.

8.19. Política de Seguridad en la Nube

- ✓ Realizar monitoreo a los log de transferencia de datos hacia la nube.
- ✓ Implementar controles de criptografía para la transferencia de información.
- ✓ Proteger los volúmenes de su exposición a un clonado mediante snapshot.
- ✓ Realizar backup de la información que se envía hacia la nube.

8.20. Política Gestión del Incidente

- ✓ Se define roles y responsabilidades dentro de la entidad para evaluar los riesgos y así mantener la operación, la continuidad y la disponibilidad del servicio.
- ✓ Gestionar los eventos de seguridad de la información para detectar e identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- ✓ Definir de manera oportuna los eventos de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
- ✓ Asegurar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Con el fin de mejorar el esquema global de la gestión de incidentes de seguridad de la información.
- ✓ Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y


MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.

- ✓ Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
- ✓ Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información
- ✓ Informar de forma completa e inmediata al ColCert (Grupo de respuesta a emergencias cibernéticas de Colombia), la existencia de un potencial incidente de seguridad informática que afecte a activos de información críticos del Estado.


8.21. Política Gestión del Riesgo

- ✓ Se deben identificar riesgos para todos los procesos y activos que conforman la Secretaría Distrital de Desarrollo Económico.
- ✓ Se debe realizar la verificación y actualización de los riesgos identificados, por lo menos una vez al año, cada vez que se identifique un nuevo riesgo o al presentarse un accidente fatal o grave.
- ✓ Es responsabilidad de los directores de procesos, así como de su personal a cargo realizar la identificación y verificación de riesgos con el apoyo de las áreas de seguridad y de aseguramiento de la información.
- ✓ Teniendo en cuenta la identificación y priorización de riesgos realizada, se debe gestionar primero los riesgos en nivel alto, seguidos del nivel medio y Nivel bajo.
- ✓ Para los riesgos identificados con nivel alto, seguidos del nivel medio la decisión de mitigar, aceptar o transferir el riesgo estará a cargo del comité directivo de la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

8.22. Política Controles Criptográficos

- ✓ Todos los equipos de cómputo portátiles asignados por la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO a los empleados, clientes, proveedores, o terceras partes deberán contar con la herramienta de cifrado debidamente instalada y parámetros definidos por la entidad.
- ✓ Todos los equipos MAC de la entidad deberán contar con la implementación de la herramienta de cifrado o la suministrada por el fabricante del dispositivo.
- ✓ Para los dispositivos móviles (teléfono celular, tabletas, iPad, discos duros extraíbles, dispositivos de almacenamiento masivo USB, etc.) asignados por la entidad de ser posible deberán estar debidamente cifrados por la herramienta suministrada por la entidad o fabricante, de no ser posible deberán estar habilitados los controles de aseguramiento y criptografía suministrados por el fabricante del dispositivo.
- ✓ Se deben implementar controles criptográficos de acuerdo con la herramienta definida por la SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO para:
 - La protección de claves de acceso a sistemas, datos y servicios.
 - La transmisión de información clasificada.
 - El almacenamiento de la información contenida en las unidades compartidas.
 - El almacenamiento y transmisión de información contenida en dispositivos móviles, correos electrónicos y en la nube (discos duros externos, dispositivos de almacenamiento masivo USB, CD/DVD, teléfonos celulares (Smartphone) OneDrive, SFTP).
- ✓ Sera responsabilidad de cada dueño de información garantizar la que información que tengan a su cargo se encuentre debidamente cifrada con la herramienta suministrada por la entidad donde quiera que se almacene dicha información (computadores portátiles, computadores de escritorio, discos duros extraíbles, dispositivos de almacenamiento masivo USB, celulares, tabletas, OneDrive para la Empresa, SFTP y en general almacenamiento en la nube) y a través de los diferentes medios de transmisión que se utilicen.


MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

9. SANCIONES A LAS VIOLACIONES DE LA POLITICA DE SEGUIRADA DE LA INFORMACION


El Comité de Seguridad de la Información solicitará la publicación en la Intranet el documento Políticas de Seguridad de la Información, socializará su contenido y hará cumplir su alcance. El desconocimiento de la política de seguridad de la información de la Secretaria Distrital de Desarrollo Económico, por parte de funcionarios, contratistas y terceros puede generar acciones disciplinarias. Las investigaciones disciplinarias y las respectivas sanciones le corresponden a la Dirección de Gestión Corporativa y Control Interno Disciplinario.

Actuaciones que conllevan a la violación de la seguridad de la información establecida por la Secretaria Distrital de Desarrollo Económico:


- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada).
- No guardar la información digital, producto del procesamiento de la información perteneciente a la Entidad.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a la Entidad, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Almacenar la información de la Entidad en los computadores personales de los usuarios,.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la Entidad, para obtener, mantener o difundir material pornográfico u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnologías de la Información de la Entidad.
- Enviar sin autorización información de la Entidad a través de correos electrónicos personales.
- Enviar información pública reservada o información pública clasificada por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Usar dispositivos de almacenamiento externo en los computadores sin la autorización previa.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización previa.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Entidad.
- No cumplir con las actividades designadas para la protección de los activos de información de la Entidad.
- Descuidar documentación con información crítica, reservada o clasificada de la Entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Almacenar información crítica reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca a Entidad o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la Entidad sin la debida autorización.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de la Entidad para beneficio personal.
- El que sin autorización acceda en todo o parte de la infraestructura informática o se mantenga dentro del mismo en contra de la voluntad de la Entidad.
- El que impida u obstaculice el funcionamiento o el acceso normal a la infraestructura informática, los datos informáticos o las redes de telecomunicaciones de la Entidad, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la Entidad.
- El que distribuya, envíe, introduzca software malicioso u otros programas de software con efectos dañinos en la plataforma tecnológica de la Entidad.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

- El que modifique, altere datos personales de las bases de datos de la Entidad sin la debida autorización.
- El que superando las medidas de seguridad de la información suplante un usuario ante los sistemas de autenticación y autorización establecidos por la Entidad.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la Entidad o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la Entidad a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a la infraestructura de tecnologías de las Información de la Entidad.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por la Entidad.
- Retirar de las instalaciones de la Entidad equipos de cómputo que contengan información institucional sin la debida autorización.
- Sustraer de las instalaciones de la Entidad, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o Entidades no autorizadas.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la Entidad, funcionarios o contratistas.
- Realizar cambios no autorizados en la plataforma tecnológica de la Entidad.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en los equipos de cómputo, cuyo uso no esté autorizado por la Subdirección de Tecnología y Sistemas la Entidad.
- Copiar sin autorización las aplicaciones de software de la Entidad, o violar los derechos de autor o acuerdos de licenciamiento.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO			 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE DESARROLLO ECONÓMICO</small>
DOCUMENTO CONFIDENCIAL			
Código:	Versión:	Fecha creación:	Fecha actualización: 01/04/2019

10. ACUERDO DE CONFIDENCIALIDAD

Todos los funcionarios y contratistas deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos laborales y de prestación de servicios utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación temporal o cuando se permita el acceso a información y/o a los recursos a personas o Entidades externas.

11. CONTROL DE CAMBIOS

Fecha	Numeral	Responsable	Versión	Descripción del cambio