ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE HACIENDA

MANUAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SECRETARÍA DISTRITAL DE HACIENDA

SUBSECRETARÍA GENERAL

Código: MN-05

Versión: 1.0

Vigente a partir de: 11 de Mayo de 2018

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Manual del Subsistema de Gestión de Seguridad de la Información

NOMBRE DEL DOCUMENTO:	Manual SGSI SDH.docx
VERSIÓN DEL DOCUMENTO:	1.0
FECHA:	27/11/2017
LECTORES:	Servidores públicos y contratistas de la SDH
CLASIFICACIÓN:	Uso interno de la SDH

RESUMEN

Este documento contiene las políticas específicas, normas particulares y estándares relacionados con Seguridad y Privacidad de la información, los cuales se agrupan en procedimientos y lineamientos. Este documento está alineado con las normas NTD SIG 001:2011, NTC ISO/IEC 27001:2013, con el componente de Seguridad y Privacidad de la Información de la estrategia GEL establecido en el decreto único reglamentario 1078 del 2015 del Min TIC, así como con la normativa sobre tratamiento de datos personales.

Documentos asociados (Este documento debe ser leído en conjunto con)

Nombre del Documento	Ver.	Fecha
Políticas de seguridad y privacidad de la información - POL-05	2.0	Febrero de 2017

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

TABLA DE CONTENIDO

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

1. INTRODUCCIÓN

La Secretaría Distrital de Hacienda ha reconocido la información como el activo más importante para su operación; su protección y seguridad tiene una importancia primordial en el desarrollo de su gestión. En tal sentido, para disminuir los riesgos y proteger este y otros activos de información (los cuales abarcan entre otros: a las personas y los elementos que interviene en el tratamiento de información y tienen valor para la entidad), es necesario implementar un conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad en el manejo, transformación y operación de la información y de igual forma administrar estos controles para mantener este nivel a lo largo del tiempo.

Para la determinación, implementación y mejoramiento de los controles y procedimientos necesarios se recurre a un Subsistema de Gestión de Seguridad de la Información de aquí en adelante (SGSI), el cual ayudará a centrar los esfuerzos y recursos en la mitigación de los riesgos que sean identificados como de mayor impacto y/o probabilidad conforme al análisis y evaluación de éstos.

La entidad publica este manual en la Intranet para conocimiento y como material de consulta por parte de servidores públicos y contratistas de la SDH, el cual será actualizado periódicamente por parte de las áreas encargadas de llevar a cabo la implementación del SGSI, o que tengan a su cargo la operación de alguno de los controles que hacen parte del subsistema. También podrá ser actualizado cuando se presenten novedades en aspectos como; indicadores, ajustes en la metodología de análisis de riesgos o cambios en los procedimientos que lo componen.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

El SGSI se basa en las políticas de seguridad y privacidad de la información, las cuales cuentan con el aval de la alta Dirección (Aprobadas en Feb 1 de 2017 por la Secretaria de Hacienda), adicionalmente son sustento de este subsistema: la normatividad legal vigente en Colombia consignada en el normograma, principalmente el código único disciplinario.

2. ALCANCE DEL MANUAL

Este manual establece el marco de referencia para el gobierno y los aspectos necesarios para la gestión, implementación, operación, seguimiento y mejora del Subsistema de Gestión de Seguridad de la Información en la Secretaría Distrital de Hacienda, conforme a lo estipulado en la norma NTD SIG 001:2011, en la ISO/IEC 27001:2013 y en la estrategia de Gobierno en Línea.

El Sistema de Gestión de Seguridad de la Información va dirigido e involucra a todos los servidores públicos (cualquiera que sea su: tipo de vinculación, funciones y nivel jerarquico), contratistas (personas naturales o jurídicas), entes gubernamentales y contribuyentes que utilizan los servicios provistos por la entidad. El cumplimiento de lo dispuesto en este manual, las políticas y demás elementos del SGSI en cuanto a la protección de la información y otros activos es responsabilidad de todo el personal, acorde con las funciones, roles y responsabilidades formalmente asignadas por la entidad.

Este manual aplica a todo el ámbito de la SDH, a sus recursos, procesos, activos de información, servidores públicos, contratistas y proveedores; la violación a lo establecido en este manual podrá ser motivo para adelantar acciones disciplinarias, administrativas y/o penales según aplique, en caso de que un servidor, contratista o proveedor haga uso indebido, altere, acceda o utilice en forma no autorizada alguno de los activos de información o divulgue información reservada.

3. GLOSARIO

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Activo de Información: Es todo aquello que tiene valor para la Entidad y que gestiona información (tomado del procedimiento 76-P-02). Hacen parte de los activos de información el hardware, el software, la información en cualquier medio en que se encuentre así como las personas y sus habilidades.

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en el daño a un activo de información a toda la organización.

Confidencialidad: Propiedad que indica que la información esté disponible y sea dada a conocer sólo a personas, entidades o procesos autorizados.

Criptografía: Técnica que se ocupa del cifrado o codificado de un mensaje, destinada a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Custodio del activo de información: Es una parte designada de la Entidad, un cargo, área o grupo de trabajo encargado de administrar y proteger los activos de información; además se encarga de hacer efectivos los controles de seguridad administrativos o técnicos que el propietario de la información (ver definición más adelante) haya definido, tales como el control de archivos, el uso de copias, la eliminación entre otros.

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

DIT: Dirección de Informática y Tecnología

Evento de Seguridad de la Información: Identificación de una condición en un sistema o servicio que indica una posible violación a la política de seguridad o la falla de un control o una situación desconocida que es relevante para la seguridad de la información.

Gestión de Riesgos: Aplicación sistemática de políticas de administración, procedimientos y prácticas a las actividades de comunicar, consultar, establecer el contexto e identificar, analizar, evaluar, tratar, monitorear y revisar un riesgo.

Hash: Es un algoritmo matemático que transforma cualquier bloque de datos en una nueva serie única de caracteres con una longitud fija, si al bloque de datos se le modifica un solo carácter la función hash arrojará un valor totalmente diferente. (Adaptado de: https://blog.kaspersky.com.mx/que-es-un-hash-y-como-funciona/2806/)

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Incidente de Seguridad: Evento o serie de eventos no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones del negocio, amenazando la seguridad de la información o de un activo de información.

Integridad: Propiedad de exactitud e integridad.

No repudio: capacidad de probar la ocurrencia o participación en un evento o acción digital y las entidades participantes.

Propietario de información / Propietario de activo de información: Corresponde a una parte designada de la Entidad, un cargo, área o grupo de trabajo que tiene la responsabilidad, aprobada por la Dirección, de definir:

a. Quiénes tienen acceso y qué pueden hacer con la información o con el activo de información (modificar, leer, procesar, entre otros)

b. Cuáles son los requisitos para que la información o el activo de información se proteja de pérdida de: confidencialidad, integridad o disponibilidad.

c. Cual es el destino o la disposición final del activo de información una vez ya no sea requerido (a).

Seguridad de la Información: Proceso que busca preservar la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una organización.

SETIC: Subdirección de Servicios de TIC

Sistema de Información: Se refiere a un conjunto de recursos y métodos organizados para: recopilar, procesar, mantener, transmitir y difundir la información según, determinados procedimientos, tanto automatizados como manuales.

SITIC: Subdirección de Infraestructura de TIC

SOTIC: Subdirección de Soluciones de TIC

Subsistema de Gestión de Seguridad de la Información (SGSI) : Componente del Sistema Integrado de Gestión, basado en un enfoque hacia los riesgos del negocio, cuyo objetivo es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Software Base: Componente lógico que tiene como función controlar e interactuar con el sistema operacional, además de controlar el hardware y soportar algunos programas, está conformado por sistema operativo, lenguajes de programación, ensambladores y compiladores.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Trazabilidad: Característica de los activos de información que permite establecer su ubicación y estado a través del tiempo y a lo largo de su gestión.

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de la entidad

VPN: en informática, acrónimo del inglés Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, por ejemplo Internet, manteniendo y garantizando la protección de la información. El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet. También permite en forma segura que los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, por ejemplo, un hotel. Todo esto utilizando la infraestructura de Internet.

4. PROCESOS Y PROCEDIMIENTOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En este capítulo se describen los procesos y procedimientos que hacen parte fundamental en la implementación de Subsistema de Gestión de Seguridad de la Información (SGSI), se encuentran agrupados en dos tipos, el primero está compuesto por los procesos y procedimientos que existen en el SGC y pueden requerir algún ajuste y por procedimientos proyectados, lo anterior debe ser realizado en un plazo máximo de un año; el segundo tipo son los procesos y procedimientos que deben estar formalizados e integrados al Sistema de Gestión de Calidad en un término de dos (2) años después de la entrada en vigencia de este documento y deberán contar con el visto bueno del líder del SGSI.

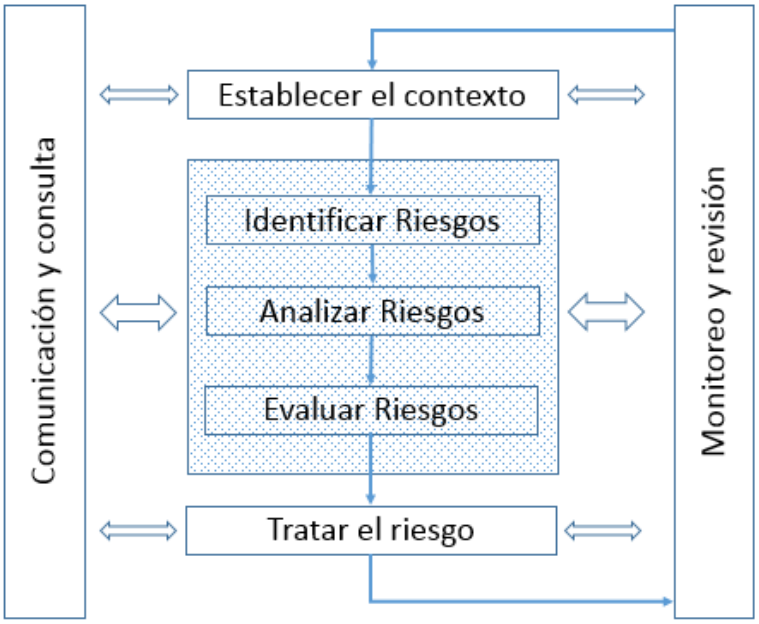
En esta sección del manual se utiliza la expresión de procedimiento para describir el documento que contenga el alcance, objetivos y descripción detallada de las actividades, pero podrá adoptar otro tipo de nombre, conforme a los estándares de manejo de documentos en el sistema de gestión de calidad. En forma similar algunos podrán fusionarse a efectos de simplificación y optimización en la gestión documental.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

4.1 TIPO I

4.1.1 PROCESO: GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN.

La gestión del riesgo hace parte de las buenas prácticas de gestión de una entidad, consiste en la realización iterativa de actividades de mejora continua cuyos elementos principales se ilustran en la gráfica Nro. 1



Gráfica Nro. 1 – Proceso de Gestión del Riesgo

La gestión de riesgos asociados a seguridad de la información, se realiza conforme al procedimiento del sistema de gestión de calidad 76-P-02 [1], liderado por el responsable de cada proceso y apoyado por el líder del SGSI con el acompañamiento de la Oficina de Análisis y Control de Riesgos.

[1] o el que lo sustituya, modifique o adicione conforme a las definiciones del área responsable.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

4.1.2 PROCEDIMIENTO: MONITOREO DE REGISTROS TRANSACCIONALES.

Su objetivo es prevenir e identificar el acceso no autorizado o abusivo a la información almacenada en los Sistemas de Información. Para cumplir este fin, los sistemas de información deben ser monitoreados de manera preventiva y de esta formar garantizar la confidencialidad e integridad de la información. Este control de carácter preventivo, genera alertas sobre cambios en los datos que no cumplan parámetros normales de operación, esta actividad se rige por el principio de transparencia que rige la función pública.

El alcance de este procedimiento incluye las novedades y consultas a los sistemas de información y abarca desde la detección del origen de la transacción, hasta la investigación y cierre de la revisión por parte de los entes de control que hacen parte del mismo. Este control hace parte del sistema de control interno, que se enmarca en el elemento de "*autorregulación*" establecido en el modelo estándar de control interno (MECI), y se adopta como estrategia para la gestión del riesgo, que es uno de los componentes del módulo de "*control de la planeación y gestión*" del modelo antes mencionado.

Las investigaciones que se derivan de este control están regidas por las competencias establecidas en el manual de funciones de la entidad (definidas en la resolución 101 del 15 de Abril de 2015 o la que a futuro la complemente o modifique) y las acciones que se deriven de las mismas siguen lo establecido en el código único disciplinario.

En este procedimiento juegan un importante papel los criterios o reglas de monitoreo, los cuales son de carácter confidencial y son definidos y ajustados periódicamente por el responsable del proceso, tomando como base la sensibilidad de algunos registros, así como el análisis histórico y estadístico de los registros en el sistema.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

4.1.3 PROCEDIMIENTO: GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Gestión de Incidentes de Seguridad de la información se encuentra descrita dentro del procedimiento 65-P-03[2] que es responsabilidad de la Subdirección de Servicios de TIC. El objetivo principal de la Gestión de Incidentes de Seguridad de la información es contar con un plan estructurado y ordenado que permita manejar adecuadamente los incidentes de seguridad de la información. En forma general la gestión de incidentes inicia con la identificación, análisis y evaluación del incidente y finaliza con la respuesta que se considera más eficiente y adecuada. En forma detallada dentro del procedimiento se llevan a cabo los siguientes pasos:

- Detectar e identificar si el incidente se clasifica como incidentes de seguridad de la información.
- Definir los roles y responsabilidades dentro de la SDH donde se definen quienes evalúan los riesgos y permiten mantener la operación y la disponibilidad del servicio. También
- Definir los reportes y escalamiento de los incidentes de seguridad de la información. Esto incluye reportes a autoridades o entes de control, cuando esto aplique, como por ejemplo lo establecido en la ley de tratamiento de datos personales en cuanto al reporte de incidentes a la superintendencia de industria y comercio (Ley 1581 de 2012 Articulo 18 literal k).
- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente.
- Definir mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información.
- Mantener actualizada la base de conocimiento y registro de incidentes de seguridad de la información.

[2] o el que lo sustituya, modifique o adicione conforme a las definiciones del área responsable.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

4.1.4 PROCEDIMIENTO: PLAN DE CONTINUIDAD DE NEGOCIO.

El plan de continuidad de negocio tiene por objetivo garantizar la continuidad del servicio y los procesos críticos de la entidad, por medio de la identificación de escenarios razonablemente posibles y la estructuración de actividades que permitan responder al evento conforme a los roles y responsabilidades previamente definidas. En el sistema de gestión de calidad se idéntifica como el procedimiento 76-P-03[3].

4.1.5 PROCEDIMIENTO: ADMINISTRACIÓN DE CUENTAS DE USUARIO.

Este procedimiento contempla lo relacionado con el control de acceso a los servicios tecnológicos provistos por la entidad para sus colaboradores, así como el acceso a los sistemas de información tanto para personal interno como de otras entidades que hacen uso de las aplicaciones de la SDH. Los pasos y controles establecidos en este documento dan cumplimiento a los controles establecidos por el dominio: Control de Acceso de la norma ISO27001:2013 identificado como A.9. En el sistema de gestión de calidad se idéntica como el procedimiento 65-P-06.

4.1.6 PROCEDIMIENTO: EJECUCIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN.

Este procedimiento contempla lo relacionado con la disponibilidad de una copia de los datos, así como de la configuración de los sistemas de información y el software base. Los pasos y controles establecidos en este documento dan cumplimiento a los controles establecidos por el dominio: Seguridad de las Operaciones de TICS, objetivo de control, Copias de Respaldo, referenciados en la norma ISO27001:2013 y que se identifica en ese estándar como A.12.3. En el sistema de gestión de calidad se identifica con el código 46-P-07[2].

4.1.7 PROCEDIMIENTO: CONTROL DE ACCESO FÍSICO

[3] o el que lo sustituya, modifique o adicione conforme a las definiciones del área responsable.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Son un conjunto de documentos, en los cuales se describe la manera en la cual se garantiza el control de acceso seguro a las instalaciones de la entidad tanto para servidores públicos, contratistas y personal vinculado a proveedores como visitantes autorizados. Dentro del sistema de gestión de calidad tenemos el Instructivo "Servicio de Vigilancia y Seguridad" perteneciente al procedimiento 42-P-01[4].

4.1.8 PROCEDIMIENTO: INGRESO Y DESVINCULACIÓN DEL PERSONAL

Dentro del Sistema de Gestión de Calidad existen dos procedimientos relacionados con el ingreso y desvinculación de personal que son: el 02-P-01 Provisión de Personal cuyo objetivo es "Proveer los cargos de libre nombramiento y remoción con oportunidad a fin de cubrir estos cargos con personal idóneo para contribuir al logro de los objetivos institucionales" y el 85-P-03 cuyo objetivo es "Desvincular de la Entidad a los servidores públicos que cesan el ejercicio de sus funciones, conforme con la normativa vigente y teniendo en cuenta la causal por la cual se origina el retiro". En estos procedimientos se deben incluír controles como: verificación de antecedentes, firma de acuerdos de confidencialidad y recepción de entregables de propiedad de la entidad. Estos mismos controles aplican al procedimiento de la Subdirección de Asuntos Contractuales para las vinculaciones a través de contratos de prestación de servicios profesionales y de apoyo a la gestión.

4.1.9 PROCEDIMIENTOS: CONSERVACION DE DOCUMENTOS

En cumplimiento de normatividad sobre la conservación de documentos en entidades públicas, la entidad ha adoptado procedimientos y lineamientos para la conservación de documentos físicos y digitales, los cuales hacen parte del proceso CPR-43 Gestión Documental, estos documentos hacen parte del sistema integrado de conservación que fue aprobado mediante la resolución SDH-00064 de Abril 7 de 2017.

[4] o el que lo sustituya, modifique o adicione conforme a las definiciones del área responsable.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

4.1.10 PROCEDIMIENTO: GESTIÓN DE VULNERABILIDADES.

Debido a que las vulnerabilidades pueden presentarse no solo en los componentes tecnológicos, sino que también pueden estar presente en la forma de actuar de las personas o estar asociadas a la estructuración de los procedimientos, por medio de actividades de revisión y evaluación es posible detectarlas y corregirlas. En el caso de las vulnerabilidades tecnológicas y debido a la amplia gama de productos que soportan los procesos de la entidad y a que permanentemente se descubren fallas o brechas en estos productos, la gestión de vulnerabilidades tecnológicas es un mecanismo constante y periódico que consiste en la identificación, análisis de fallas y aplicación de correctivos.

La identificación de vulnerabilidades se realiza por medio de revisiones técnicas especializadas (análisis de vulnerabilidades), análisis de código fuente, pruebas de penetración o la generación de alertas técnicas, estas últimas pueden provenir de los mismos fabricantes o de compañías de seguridad.

Resultado del análisis anteriormente expuesto, un grupo interdisciplinario de perfil técnico decide la(s) acción(es) que debe(n) ser tomada(s) y posteriormente se realiza el seguimiento a los resultados obtenidos. Las acciones que se definan y que son ejecutadas por parte del administrador de cada producto o plataforma, son priorizadas por el nivel de riesgo al que se encuentre expuesta la entidad y en su ejecución, se aplican los pasos establecidos en el procedimiento de gestión de cambios.

4.1.11 PROCEDIMIENTO: GESTIÓN DE CAMBIOS

En este procedimiento se deberá definir la manera como se realiza el control de cambios de manera segura en la SDH, tanto para los procesos y procedimientos del SGC como para los sistemas de información. Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, revisiones técnicas a las aplicaciones después de cambios en la plataforma, valoración de impacto, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa) entre otros.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

4.1.12 PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Este procedimiento debe definir cómo se realiza la protección contra códigos maliciosos teniendo en cuenta, que controles utiliza (hardware o software), cómo se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.

4.1.13 PROGRAMA DE GESTION DE DATOS PERSONALES

Este programa contendrá: las actividades, controles, roles y responsabilidades que le permitan a la entidad dar cumplimiento a la protección de datos personales y reserva de información, entre ellas se encuentran: identificación y gestión de riesgos relacionados con el tratamiento de datos personales, coordinación del programa en toda la entidad, promoción de la cultura de protección de datos, inventario y registro de las bases de datos que contienen información personal, reporte de novedades a la autoridad de protección de datos en Colombia.

4.2 TIPO II

4.2.1 PROCEDIMIENTO: GESTIÓN DE ACTIVOS DE INFORMACIÓN.

Este procedimiento establecerá la manera en que los activos de información serán identificados e inventariados, las responsabilidades a cargo de los propietarios de activos de información, especificará cómo son clasificados y rotulados de acuerdo con su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral o contractual con la entidad. Lo anteriormente descrito permitirá dar cumplimiento tanto a los controles establecidos en el dominio que lleva el mismo nombre en la ISO27001:2013, como a lo definido en los decretos que reglamentan la Ley de

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Transparencia y Acceso a la Información Pública, respecto a la publicación de información sobre éstos activos.

4.2.2 PROCEDIMIENTO: GESTIÓN DE CAPACIDAD

Se debe especificar la forma en como se realiza la gestión de la capacidad para los sistemas de información. Se deben definir condiciones para acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda, etc.

4.2.3 PROCEDIMIENTO DE TRANSFERENCIA DE INFORMACIÓN

En este procedimiento se debe describir cómo se realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción. Se deben definir las condiciones de protección de la información que se va a transferir, la duración del acuerdo, responsabilidades, propiedad de la información, acciones en caso de incumplimiento, entre otros. En especial este procedimiento establecerá las condiciones bajo las cuales se dará aplicabilidad a la reserva tributaria, establecida en el régimen tributario nacional con respecto a la reserva de las bases gravables y la determinación privada de los impuestos (artículo 583), así como la reserva de los expedientes (artículos 692 y 849-9).

5. LINEAMIENTOS.

Esta sección contiene las políticas y normas que la entidad establece para el tratamiento de la información, el uso de activos de información o de servicios tecnológicos, los cuales son presentados siguiendo el mismo orden que presenta la norma ISO 27001, específicamente el anexo de controles de la misma.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

5.1 TRATAMIENTO DE DATOS PERSONALES.

Conforme a la misión de la entidad la entidad aplica el principio de la reserva tributaria establecida en el Estatuto Tributario Decreto 624 de 1989 Art. 583: el cual establece la reserva de la declaración: “La información tributaria respecto a las bases gravables y la determinación privada de los impuestos que figuren en las declaraciones tributarias, tendrá el carácter de información reservada” , la reserva tiene un marco constitucional fundamentado en el Art. 15 de la constitución política: *"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.*

En cuanto a jurisprudencia tenemos que *"El derecho fundamental a la intimidad se proyecta en dos dimensiones: como secreto que impide la divulgación ilegítima de hechos o documentos privados, o como libertad, que se realiza en el derecho de toda persona a tomar las decisiones que conciernen a la esfera de su vida privada.” (Sentencia C-489 de 1995)*

Por otra parte la administración tributaria distrital ha definido su posición con respecto a la protección de la información en los siguientes términos: *“La reserva tributaria tiene su sustento en el secreto profesional, de acuerdo al cual los trabajadores de la Administración tributaria están impedidos en hacer públicos, los hechos que conocieran durante el desarrollo de sus actividades y la violación de la misma constituiría una violación al secreto profesional, pues el bien jurídico que se protege es la libertad de la persona en lo que respecta a su intimidad, ya que ningún tercero debe poder llegar a conocer sobre hechos que corresponden al ámbito personal, y que si llega a obtener dicha información, ya sea por su profesión, oficio, arte, estado o ministerio, debe guardar la absoluta reserva, porqué así se lo establece constitucionalmente y tan sólo deberá ser revelada cuando la ley se lo permita o el mismo contribuyente lo consienta o cuando exista un interés social superior al interés individual justificable.” (Concepto 932 de 11 de septiembre de 2001 DIB)*

Por todo lo anterior es compromiso y obligación de los servidores públicos vinculados a ala SDH, guardar la más estricta confidencialidad y reserva sobre la información tributaria independiente del medio en el que esta se encuentre.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

En la SDH el tratamiento de datos personales se realiza según lo establecido en la Ley Estatutaria 1581 de 2012, su decreto reglamentario 1377 de 2013 y se encuentra detallado en el documento POL-05 *"Políticas de Seguridad y Privacidad de la Información"* del Subsistema de Gestión de Seguridad de la Información de la entidad. Los datos personales puede ser requeridos por la SDH en cumplimiento de sus funciones legales o para la realización de procesos de soporte de tipo interno en los cuales hay interacción con servidores públicos o ciudadanía en general. En cualquier caso, a los datos se les aplica un tratamiento coherente con la protección irrestricta del derecho al Hábeas Data del titular de la información, teniendo en cuenta los siguientes aspectos:

DERECHOS DE LOS TITULARES. El Titular de los datos personales tiene los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado;
- Solicitar prueba de la autorización otorgada a la SDH para el tratamiento, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012;
- Ser informado por la SDH (específicamente por el responsable del tratamiento o por el encargado del tratamiento), previa solicitud, respecto del uso que le ha dado a sus datos personales;
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y demás normas que la modifiquen, adicionen o complementen;
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que la SDH o el encargado por ésta para el tratamiento, han incurrido en conductas contrarias a la ley, la Constitución o las políticas internas de tratamiento de información;
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento por cuenta de la SDH.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO. En los literales d) y e) del Artículo 3 de la Ley 1581 de 2012, se hace expresa mención al Encargado y al Responsable del tratamiento, respectivamente. Así, el responsable del tratamiento es la 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, mientras que el Encargado del tratamiento es la 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. Los deberes de los responsables y de los encargados del tratamiento de datos personales se rigen por lo establecido en los artículos 17 y 18 de la Ley de Tratamiento de datos Personales (Ley 1581 de 2012), así como lo establecido en el decreto 886 de 2014.
Acorde con lo anterior, los responsables de los procesos harán las veces de responsables del tratamiento de datos personales que se lleven a cabo dentro de la ejecución del proceso. Los encargados del tratamiento de datos personales son todos los usuarios y/o partes interesadas identificadas en la caracterización de procesos.

AUTORIZACIÓN DEL TITULAR. En lo que respecta al tratamiento de datos de ciudadanos y personas vinculadas a la SDH, en los procesos propios de la gestión hacendaria y la sostenibilidad financiera del distrito capital no se requiere autorización para el tratamiento de datos personales por tratarse de una entidad pública en ejercicio de sus funciones legales (artículo 10 de la ley 1581 de 2012).

En otros procesos en los que se requiere el tratamiento de datos personales y aplique la solicitud de la autorización, el responsable del tratamiento informará al titular los siguientes aspectos:

- El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
- Los derechos que le asisten como Titular;
- Los datos de contacto del Responsable del Tratamiento

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

SOLICITUD Y SUMINISTRO DE INFORMACIÓN. El titular de la información podrá hacer uso de los canales de atención dispuestos por la SDH para solicitar información sobre el tratamiento de sus datos personales y presentar solicitudes relacionadas con éstos. La entidad responderá por el mismo medio por el cual fue recibida la solicitud o por el que considere más adecuado, atendiendo el principio de confidencialidad, siempre y cuando esté a su alcance establecer que la solicitud proviene y será entregada al titular de los derechos sobre la información en cuestión, lo anterior sin perjuicio y aplicando lo establecido en el artículo 13 de la Ley 1581 de 2012 respecto de las personas a quienes se les puede suministrar la información.

La atención de peticiones, consultas o reclamos sobre el tratamiento de datos personales se gestiona por medio del procedimiento “Seguimiento y Control a Peticiones, Quejas, Reclamos y Sugerencias” del SGC, identificado como 89-P-01 en el SGC.

Los términos para la atención de consultas y reclamos de los titulares, se rigen por lo establecido en los artículos 14 y 15 de la ley 1581 de 2012.

5.2 CONTROL DE ACCESO Y USO DE LOS SISTEMAS DE INFORMACIÓN

- Cada servidor público o contratista firma la declaración de aceptación de la política de seguridad y privacidad de la información en el momento de su posesión o firma del contrato de servicios. Es prerrequisito para la autorización de acceso a los recursos informáticos
- A cada servidor público o contratista se le asigna un identificador de usuario para acceder a la red corporativa y a los diferentes sistemas de información. El identificador es único y personal, permitiendo la identificación de las acciones que realiza el usuario tanto en la red como en los sistemas de información
- La Dirección de Informática y Tecnología (DIT) diseña e implementa procedimientos que cancelan automáticamente los accesos a los recursos tecnológicos tales como sistemas de información y red corporativa, a los servidores públicos o contratistas que finalizan la relación laboral o contractual con la entidad. Para este fin se definió el formato Constancia de Entrega (85-F.10).

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La Dirección de Informática y Tecnología (DIT) diseña e implementa procedimientos para que ante una novedad administrativa, los derechos de acceso sean suspendidos durante el tiempo que se presente la novedad.
- Los acuerdos de confidencialidad y de cumplimiento de los lineamientos de Seguridad de la Información hacen parte de las obligaciones y deberes que deben cumplirse en el marco de la relación laboral o contractual establecida con la Entidad al momento de su vinculación a ella.
- Las contraseñas de usuario son personales e intransferibles, por lo tanto, bajo ninguna circunstancia se pueden compartir con ninguna persona.
- Los equipos que no pertenezcan a la SDH y por necesidades del servicio deban ser conectados a la red, deben cumplir con los estándares y políticas de seguridad como lo son: contar con un software antivirus, software debidamente licenciado, para el efecto y en caso de ser necesario, la SDH podrá instalar en forma temporal licencias de sus productos de seguridad, para proteger su infraestructura, sin que lo anterior implique la sesión de la licencia al tercero.
- El software comercial usado en la entidad cuenta con la respectiva licencia, la cual debe ser autorizada, adquirida e instalada por personal de la Dirección de Informática y Tecnología, por lo que no está permitido a ningún servidor público la copia, distribución e instalación de software comercial. La subdirección de servicios de TIC realiza monitoreo sobre el software instalado en los equipos de la entidad.
- El acceso a las plataformas informáticas a través del sistema operativo en servidores está restringido, a aquellos servidores públicos, contratistas o terceros que estén autorizados por la Subdirección de Infraestructura de las TIC en cumplimiento de sus funciones. Para equipos de escritorio y portátiles el acceso con permisos de administrador está restringido a servidores públicos, contratistas o terceros que estén autorizados por la subdirección de servicios de las TIC, ésto con el fin de realizar funciones de administración o gestión del sistema.
- Las actualizaciones al sistema operativo y productos base de cualquier sistema computacional de la SDH se realizan siguiendo el procedimiento de gestión de cambios, al igual que deben contar con la plena identificación de los riesgos asociados y aquellas

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

son planeadas cuidadosamente, así como también incorporan procedimientos de roll back o marcha atrás.

- El responsable del proceso autoriza y revisa periódicamente los accesos a sus sistemas de información o aplicaciones, de acuerdo con los roles establecidos y las necesidades de uso y también podrá revocar este acceso, acorde a las necesidades de seguridad o privacidad.
- Los desarrolladores evitarán almacenar contraseñas, cadenas de conexión u otra información sensible en texto claro en programas fuente o scripts e implementarán controles para asegurar la confidencialidad e integridad de dichas contraseñas.
- Los desarrolladores implementan un mensaje para que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso, ésto para las aplicaciones que no hacen uso de un inicio de sesión único (SSO por sus siglas en inglés).
- El sistema de acceso (centralizado o propio de cada aplicación) establece los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma controlada, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y en su lugar, generando mensajes generales de falla.
- El sistema de acceso (centralizado o propio de cada aplicación) garantiza que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a las aplicaciones, acorde con la definición del lineamiento de control de acceso.
- Las aplicaciones restringen el acceso a información sensible, tal como: archivos de configuración, direcciones URL o funciones protegidas, el acceso a este tipo de información solamente es permitido a usuarios autorizados (administradores).
- La Dirección de Informática y Tecnología implementa, opera y gestiona medidas de prevención en la infraestructura tecnológica de la entidad, con el fin de proteger contra software malicioso como por ejemplo virus.
- Los estándares de contraseñas para servidores públicos de la entidad aparecen en la siguiente tabla y aplican a nivel de directorio activo, herramientas de autenticación única (Single Sign On) y para las aplicaciones, cuando éstas resuelven en forma autónoma el proceso de autenticación:

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Característica	Valor	Observaciones
No reutilización de las últimas claves – historial de contraseñas	15	
Vigencia máxima de la clave - días	30	
Vigencia mínima de la clave - días	1	Este parámetro debe ser mayor que 0
Longitud mínima de la clave	8	
Requerimientos de complejidad	habilitado	Habilitar este lineamiento en AD exige cumplir por lo menos 3 de las siguientes 4 características: • Caracteres en mayúscula (desde la A hasta la Z, excluyendo la Ñ) • Caracteres en minúscula (desde la a hasta la z, excluyendo la ñ) • Dígitos base 10 (desde el 0 hasta el 9) • Caracteres no alfanuméricos (por ejemplo: !, $, #, o %) Notas: Para efectos de compatibilidad con OID, estas 4 características se convierten en requeridas en por lo menos un carácter de cada uno) (restricción a nivel de AD para que el primer carácter no sea carácter especial o numérico – requiere API y desarrollo)
Número de intentos de conexión.	4	
Duración del bloqueo de cuenta – minutos	30	
Restablecer contador de bloqueo después de: x minutos	30	Debe ser menor o igual a duración del bloqueo de cuenta.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Característica	Valor	Observaciones
Mensaje para los usuarios que intentan iniciar sesión	(Ver siguiente columna)	Bienvenido a la SDH La actividad en nuestros sistemas de información es auditada y su uso no autorizado, puede ocasionar sanciones disciplinarias y legales.
Solicitar al usuario cambio de clave antes de su vencimiento - días	5	

El estándar para claves de acceso para ciudadanos se describe en la siguiente tabla:

Estándar de Claves de Acceso Para Ciudadanos

Característica	Valor	Observaciones
No reutilización de las últimas claves – historial de contraseñas	1	Indica que el ciudadano, debe generar como nueva clave una diferente a la actual.
Vigencia máxima de la clave.	3 años	
Vigencia mínima de la clave - días	1	Este parámetro debe ser mayor que 0
Longitud mínima de la clave	8	
Requerimientos de complejidad	habilitado	Habilitar este lineamiento en AD exige cumplir por lo menos 3 de las siguientes 4 características: • Caracteres en mayúscula (desde la A hasta la Z, excluyendo la Ñ) • Caracteres en minúscula (desde la a hasta la z, excluyendo la ñ) • Dígitos base 10 (desde el 0 hasta el 9) • Caracteres no alfanuméricos (por ejemplo: !, $, #, o %) Notas: Para efectos de compatibilidad con OID, estas 4 características se convierten

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Característica	Valor	Observaciones
		en requeridas en por lo menos un carácter de cada uno) (restricción a nivel de AD para que el primer carácter no sea carácter especial o numérico – requiere API y desarrollo)
Número de intentos de conexión.	4	
Duración del bloqueo de cuenta – minutos	60	
Restablecer contador de bloqueo después de: x minutos	60	Debe ser menor o igual a duración del bloqueo de cuenta.
Mensaje para los usuarios que intentan iniciar sesión	(Ver siguiente columna)	Bienvenido a la SDH La actividad en nuestros sistemas de información es auditada y su uso no autorizado, puede ocasionar sanciones disciplinarias y legales.
Solicitar al usuario cambio de clave antes de su vencimiento.	3 meses	

Los parámetros y características de las claves en la SDH se pueden complementar por medio de funciones en la base de datos, las cuales se habilitan a nivel de perfil, mecanismo que permite mayor nivel de seguridad.

Los valores anteriormente descritos requieren revisión y actualización conforme a criterios de seguridad.

5.3 TRANSFERENCIA Y ACCESO A INFORMACIÓN.

Este conjunto de lineamientos tiene como fin mantener la seguridad de la información que se transfiere tanto dentro de la organización, como con cualquier entidad externa.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La Dirección de Informática y Tecnología habilita la transferencia de información empleando protocolos seguros entre la SDH y las entidades externas, cuando sea necesario.
- Las áreas de la SDH con responsabilidad sobre el manejo de personal de planta así como de contratistas hacen firmar el acuerdo de confidencialidad establecido por la entidad. Lo anterior aplica para el acceso y/o transferencia de información tanto por personal interno como externo y esta obligación se incluye en los términos del acuerdo (contrato) entre las partes.
- La Subdirección de Infraestructura de TIC (SITIC) define y habilita el uso de protocolos seguros (por ejemplo https) para la transferencia de información a través de redes públicas para las aplicaciones de la SDH que así lo requieran, con el fin de prevenir perdida de integridad y acceso no autorizado a la información.

5.4 DESARROLLO Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN

La entidad define los siguientes mecanismos con el fin de que permitan realizar una adecuada gestión (adquisición, mantenimiento, desarrollo) del software que es de propiedad de la entidad, buscando que las necesidades de la entidad tengan un adecuado cubrimiento y se apliquen las mejores prácticas de la industria.

- Todo componente de software (aplicación, sistema, código fuente) que sea desarrollado para la SDH, es propiedad intelectual de la entidad y se encuentra clasificada como activo importante, por lo que debe ser protegido con estrictos controles de seguridad.
- Todo el personal interno o externo que participe en el desarrollo de software durante las diferentes etapas: especificación, análisis, diseño, desarrollo, pruebas, capacitación, mantenimiento o cualquier otra actividad relacionada, firma un acuerdo de confidencialidad con la SDH, donde el individuo o tercero se compromete a guardar secreto profesional sobre el software y su proceso de desarrollo, y donde acepta que el código fuente y todos sus componentes son propiedad de la SDH, por lo que no copiará ni reutilizará el código parcial o totalmente para ningún otro fin.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- Toda aplicación adquirida o desarrollada, así como las mejoras realizadas a las mismas, deben considerar la seguridad como un aspecto a cubrir en todo el ciclo de vida del software: desde la especificación, hasta la puesta en producción, para esto la entidad cuenta con una guía de seguridad para el desarrollo de software identificada en el sistema de gestión de calidad como 44-G-08 la cual hace parte del procedimiento de construcción o mantenimiento de soluciones de software.
- Antes de adquirir o desarrollar una aplicación, el área usuaria debe especificar claramente los requerimientos mínimos de seguridad con los que debe contar la aplicación. Las diferentes alternativas deben ser revisadas con los desarrolladores o proveedores y el líder del SGSI, con el fin de obtener un balance adecuado entre los requerimientos de seguridad y funcionalidad (facilidad de uso, simplicidad operativa actualizaciones, costos, entre otros), buscando minimizar los riesgos de perdida de confidencialidad, integridad o disponibilidad de la información.
- La puesta en producción de nuevas soluciones tecnológicas, actualizaciones, reconfiguraciones o cambios al software existente, estará sujeta al cumplimiento del procedimiento de gestión de cambios, cumpliendo los requisitos de seguridad para la puesta en producción.
- Al adquirir sistemas de terceros se debe cumplir con los requisitos de seguridad establecidos y con el licenciamiento apropiado del software, cumpliendo con lo establecido en la normativa de derechos de autor, la Dirección de Informática y Tecnología, es la responsable de la instalación del software adquirido y autorizado y aplica controles para evitar infringir los lineamientos al respecto.
- Las herramientas de control de versiones del software, así como los repositorios de código fuente son accesibles sólo por personal autorizado y asociado a la función de desarrollo de sistemas, así como al personal de las áreas de control y auditoría. La Subdirección de Infraestructura de TIC (SITIC) gestiona y administra estos controles de acceso.
- Las herramientas para el desarrollo y utilitarios de software (como por ejemplo; IDE Integrated Development Environment, IDE SQL, Control de versiones) se eliminan de manera segura de cualquier equipo de cómputo en el que haya sido instalado.
- Las herramientas de desarrollo se instalan únicamente en los ambientes definidos para el desarrollo de software.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La Subdirección de Infraestructura de TIC (SITIC) instala actualizaciones de seguridad (parches) una vez se haya analizado el impacto, estimado los riesgos y definido un mecanismo de marcha atrás (o roll back).
- La Subdirección de Soluciones de TIC (SOTIC) es responsable por que el proceso que gestiona el ciclo de vida del software, siga los requisitos de seguridad, cómo mínimo los siguientes:
    - Interacción de la aplicación con la infraestructura: Hace referencia a que la aplicación no debe interferir o cambiar parámetros de seguridad del sistema operativo y otras herramientas de software base en el servidor y que la aplicación debe contemplar mecanismos propios de protección, complementando las medidas de protección de la infraestructura.
    - Identificación y autenticación: Hace referencia a que las aplicaciones siempre que sea técnicamente posible deben integrar este proceso a las herramientas de la SDH que cumplen este objetivo, buscando consolidar procesos de inicio de sesión único (SSO por sus siglas en Ingles) .
    - Autorización y control de sesión: Hace referencia al esquema que facilite el manejo de permisos y el control sobre la sesión del usuario en la aplicación.
    - Control de acceso: Hace referencia a los mecanismos de manejo de usuarios y claves, las cuales pueden ser consultadas en el ítem 6.2.1 de este manual.
    - Confidencialidad: Hace referencia a la protección de la información en redes públicas.
    - Integridad: Cubre los aspectos relacionados con la protección del código fuente y los registros a nivel de bases de datos, así como el cargue de archivos que requieren validaciones de estructura y calidad.
    - Disponibilidad: Hace referencia al manejo adecuado de excepciones y errores que eviten fallas por consumo de recursos.
    - Auditoría: Ver los aspectos de auditoría en el ítem 6.2.14
    - Repudio: El término se refiere al desconocimiento por parte de uno de los intervinientes en un mensaje, transacción o registro digital. Cuando un sistema de información por norma o reglamentación deba asegurar que esta situación no se presente, debe contemplar el uso de certificados digitales de firma, así como los

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

demás aspectos establecidos en la Ley 527 de 1999 de comercio electrónico y sus decretos reglamentarios.

- La Subdirección de Soluciones de TIC (SOTIC) realiza pruebas al software, incluyendo, pero no limitadas a pruebas: unitarias, de estrés y carga, de volumen, de regresión, antes de liberar una versión de software, acorde con las características del proceso que apoyará el sistema en ambiente de producción.
- La Subdirección de Soluciones de TIC (SOTIC) realiza pruebas de seguridad a los controles de acceso a los sistemas y de trazabilidad de los registros, incluyendo; identificación, autenticación y autorización, controles de cifrado y almacenamiento seguro, así como cualquier otro control que se haya implementado.
- La Subdirección de Infraestructura de TIC (SITIC) en conjunto con la Subdirección de Soluciones de TIC (SOTIC) realizan pruebas a las configuraciones del sistema incluyendo: sistema operativo, bases de datos, middleware y cualquier componente que interactúe como parte del sistema a liberar.
- Los datos de producción no se utilizan en el ambiente de pruebas ni desarrollo sin la aplicación de una técnica de enmascaramiento (mezcla aleatoria de datos, que impida por ejemplo, la individualización de información de un contribuyente), el uso de información para este propósito debe estar autorizado por los dueños de los activos de información, quienes también son responsables de solicitar su eliminación una vez cumplido el objetivo.
- Se eliminan todos los datos de prueba como: cuentas creadas, contraseñas y cualquier otra información utilizada en pruebas antes de liberar una versión a producción.
- Cualquier tipo de modificación a la versión vigente de una aplicación cuenta con una ventana de mantenimiento, previo acuerdo con el líder funcional de la aplicación y previo aviso a los usuarios involucrados de manera que la misma no estaría disponible en producción al momento de realizar el cambio; de la misma manera, cuando la Subdirección de Infraestructura de TIC (SITIC) vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
- La Subdirección de Soluciones de TIC (SOTIC) aplica, sin excepción, herramientas que permiten el control de versiones del código fuente y la trazabilidad de las modificaciones.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- El software de control de versiones registra las operaciones de forma detallada (fecha, hora, autor) en logs, incluyendo accesos, modificaciones y actualizaciones de versiones; al igual que el servidor de aplicaciones registra las operaciones de despliegue de las aplicaciones.
- La Subdirección de Infraestructura de TIC (SITIC) activa los registros de errores, los cuales se revisan periódicamente para valorar riesgos en el funcionamiento.
- La Subdirección de Infraestructura de TIC (SITIC) protege los logs para evitar su uso inadecuado, incluyendo borrado o modificación.
- La Subdirección de Infraestructura de TIC (SITIC) establece ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, para aquellos sistemas de información de misión crítica, contando cada uno con capas independientes de presentación, capa media y datos, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- En el código fuente se evita a toda costa la inclusión y manejo de códigos y claves de autenticación.

5.5 ACCESO A ACTIVOS DE INFORMACIÓN

Mediante estos lineamiento se establecen los mecanismos de protección de los activos de información, cuando terceros tienen acceso a éstos.

- Cada uno de los cargos que es responable de procesos, actúa como propietario de la información que los soporta (sea que se encuentre en medio físico o digital), y es su responsabilidad custodiarla y protegerla asegurando el cumplimiento de las directrices y normativa que regula el uso y acceso adecuado a ésta. La protección antes mencionada se extiende a otros activos de información que estén a su cargo (ej. áreas de archivo, computadores a su cargo, etc.)
- La Dirección de Informática y Tecnología es la responsable de los activos de información correspondientes a la plataforma tecnológica de la SDH (esto es hardware o software) y en consecuencia, realiza su operación y administración con el fin de preservar la seguridad de la información.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La conexión entre sistemas internos de la SDH y otros de terceros debe ser aprobada por la Dirección de Informática y Tecnología o por la Subdirección de Infraestructura de TIC (SITIC) con el fin de no comprometer la seguridad de la información de la SDH.

5.6 DISPOSITIVOS MÓVILES Y MEDIOS REMOVIBLES.

La SDH provee las condiciones para el manejo de los dispositivos móviles como teléfonos inteligentes, tabletas y computadores portátiles, (referente al servicio de telefonía celular, acorde con lo establecido en la resolución SDH-0053 del 16 de febrero del 2009). Los aspectos aquí contenidos pueden abarcar dispositivos de propiedad de los colaboradores, cuando éstos hacen uso de servicios suministrados por la entidad.

- La SDH habilita un método de bloqueo para los dispositivos móviles y portátiles institucionales que serán entregados a los usuarios. Se configuran estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado. En el caso de los dispositivos móviles el tiempo establecido es de 2 minutos; para los portátiles es de 15 minutos. Cuando el método de acceso al dispositivo es por medio de contraseña, se deben seguir las recomendaciones de los lineamientos dados en la sección de control de acceso tales como claves robustas, cambiarla con frecuencia y no compartirlas.
- La SDH activa el cifrado del medio de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo, esta configuración no debe ser modificada por el usuario.
- La SDH configura la opción de borrado remoto de información en los dispositivos móviles institucionales, evitando así pérdida de confidencialidad de información en caso de pérdida o robo.
- La SDH cuenta con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales, acogiéndose al lineamiento de respaldo de información, establecido por la entidad.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La Subdirección de Servicios de TIC (SETIC) instala un software de antivirus en los portátiles institucionales y vela por que se mantenga actualizada esta protección en cada equipo.
- La Subdirección de Infraestructura de TIC (SITIC), activa los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y mantiene estos códigos bajo su custodia.
- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares públicos donde sea evidente el riesgo de robo.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la descarga e instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones o actualizaciones del sistema operativo únicamente desde las tiendas oficiales de los dispositivos móviles institucionales.
- La Subdirección de Infraestructura de TIC (SITIC), es la encargada de actualizar el sistema operativo de los dispositivos móviles institucionales cada vez que éstos notifiquen de una actualización disponible.
- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar la opción de compartir recursos como: WiFi, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los funcionarios pueden conectar los dispositivos móviles institucionales asignados, a un computador ajeno a la entidad, siempre que este cuente con medidas apropiadas de protección como por ejemplo: producto antivirus actualizado y sistema operativo actualizado y que su uso esté bajo su tutela.
- La información contenida en los dispositivos móviles institucionales es considerada propiedad de la Secretaría Distrital de Hacienda.
- Los servidores públicos son responsables por la custodia de los medios de almacenamiento institucionales asignados.
- La utilización de medios de almacenamiento removibles como: CD/DVD RW, memorias USB, está autorizado sólo al personal encargado de instalar y configurar el software de la SDH. Este podrá utilizar medios removibles para transferir datos. Cualquier otro cargo

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

requiere autorización específica por parte del Director o Jefe de Oficina Asesora a la cual pertenece el funcionario.

- Los usuarios deben ser cautelosos acerca de la fusión de las cuentas de correo electrónico personales y de trabajo en sus dispositivos móviles. Deben tener especial cuidado para asegurar que los datos de la entidad sólo se envíen a través del sistema de correo electrónico corporativo.
- El soporte de primer nivel para los usuarios de dispositivos móviles es la mesa de servicios, por medio de sus diferentes canales, y en caso de ser necesario un segundo nivel, este es provisto directamente por los proveedores de los equipos, por conducto de la subdirección administrativa.

5.7 TELETRABAJO.

La SDH establece las circunstancias y condiciones bajo las cuales se realiza el teletrabajo, lo cual implica el acceso remoto a la plataforma tecnológica de la entidad. Así mismo, pondrá en práctica controles para que las conexiones se realicen de manera segura, a saber:

- Los usuarios que realizan teletrabajo deben contar con las aprobaciones requeridas y acatar las políticas de seguridad y privacidad, las condiciones de uso y en general las demás normas y políticas establecidas en la entidad así como la normatividad vigente sobre el teletrabajo (Ley 1221 de 2008)
- El teletrabajador facilitará y permitirá el acceso a los recursos suministrados por la entidad para fines de mantenimiento, reemplazo o actualización, los cuales tienen como finalidad mantener niveles adecuados de desempeño y seguridad.
- Las herramientas y medios suministrados no podrán ser usados por persona distinta al teletrabajador, quien al final de la vinculación laboral o cuando cese su condición de teletrabajador deberá restituir los objetos y herramientas entregadas para la ejecución del mismo, en buen estado, salvo el deterioro causado por el uso normal.
- El teletrabajador deberá contemplar mecanismos alternos y de contingencia, de tal manera que con un grado de confianza razonable, pueda desempeñar sus labores y cumplir sus obligaciones aunque su sitio de trabajo se vea afectado por cortes de energía

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

o suspensión de servicio de conectividad (acceso a internet).

- Los mecanismos y técnicas de seguridad y control mínimos que se aplican en el teletrabajo son los siguientes:
    - Autenticación por medio de usuario y contraseña.
    - Procedimiento seguro de generación y entrega de claves.
    - Uso de protocolos que cifren la información que fluye entre el teletrabajador y la entidad, por medio de esquemas como por ejemplo VPN.
    - El dispositivo del usuario que se utilice en el teletrabajo contará con herramientas de seguridad como antivirus y firewall, provistas y/o configuradas bajo las políticas de seguridad de la entidad. También contará con herramienta de gestión remota para soporte y mantenimiento.
    - Generación de registros de auditoría de la actividad del teletrabajador.
    - La entidad se reserva el derecho a realizar visitas de auditoría y control al sitio y personal que trabaja bajo la modalidad de teletrabajo, aplicando el mismo procedimiento y técnicas que aplica en las visitas de auditoría a dependencias y procesos al interior de sus instalaciones.
- Dependiendo del tipo de actividad que será desarrollada por el teletrabajador y a los riesgos que se deriven de ésta, podrán ser adoptadas medidas más robustas o complementarias, las cuales deberán ser avaladas por el líder del subsistema de seguridad de la información.
- La Subdirección de Infraestructura de TIC (SITIC) analiza y gestiona los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la SDH.
- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas por el director o jefe de oficina para establecer dicha conexión a los equipos de la plataforma tecnológica de la SDH y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Los usuarios deben establecer conexiones remotas únicamente en computadores previamente identificados y sólo en condiciones de contingencia, en computadores públicos de hoteles, cafés internet u otros.
- El acceso remoto a la red de la SDH y a sus recursos solamente se facilitará a los usuarios

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

autorizados por cada una de las direcciones de la SDH. La Subdirección de Infraestructura de TIC (SITIC), gestiona y controla dicho acceso. Las aplicaciones sensibles hacen uso de protocolos seguros; los privilegios de acceso a los recursos (aplicaciones) son restringidos, de acuerdo con los roles de los usuarios (permisos de acceso).

- El personal de las Subdirecciones de Servicios de TIC (SETIC) e Infraestructura (SITIC) es el único autorizado para hacer uso de la herramienta de control remoto en los equipos usados en la gestión de la SDH.

5.8 USO DE CRIPTOGRAFÍA

A continuación los lineamientos para asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información

- La Subdirección de Soluciones de TIC (SOTIC) y la Subdirección de Infraestructura de TIC (SITIC) almacenan y transmiten la información sensible (reservada o restringida) bajo técnicas de cifrado, con el propósito de proteger su confidencialidad e integridad, siempre que el análisis de riesgo determine que es requerido.
- La Dirección de Informática y Tecnología (DIT), vela por el cumplimiento de los siguientes aspectos en relación con las actividades asociadas al ciframiento, como son:
    - Vela por que todo sistema de información o aplicación que requiera realizar transmisión o almacenamiento de contraseñas cuente con mecanismos de hash.
    - Define y aplica un procedimiento para el uso, protección y la administración de claves de cifrado.
    - Vela por la adopción de mecanismos de activación, recepción y distribución de las claves públicas de cifrado a usuarios autorizados (en el caso de ciframiento asincrónico) y velará por que la clave tenga un periodo de validez de 2 años.
    - Define procedimientos de custodia de claves de cifrado, manteniéndolas en caja fuerte, tanto para ambientes de la operación en el día a día como bajo operación en contingencia.
    - El cambio periódico de las claves de cifrado.
    - Las claves de cifrado son cambiadas cuando se considere que han perdido su

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

confidencialidad o cuando el custodio culmine su relación laboral con la SDH.

- Los procesos de cifrado y descifrado de información, se realizan utilizando infraestructura (servidores o computadores de escritorio) que no estén conectados a redes públicas o externas o que tengan acceso directo a Internet; adicionalmente el acceso a dichos procesos es controlado mediante autenticación.
- Para todas y cada una de las actividades que hacen parte de la gestión de las claves criptográficas se mantiene un registro de las actividades realizadas.
- Los acuerdos o contratos de servicio con los proveedores de servicios de criptografía o entidades certificadoras: establecen responsabilidades, confiabilidad de los servicios, tiempos de respuesta y esquemas de contingencia.
- La Subdirección de Soluciones de TIC (SOTIC) adopta los estándares criptográficos acorde con los niveles de riesgo, los cuales pueden ser del tipo sincrónico o asincrónico, ésto hace referencia a las llaves (claves) que cada uno de ellos usa, los primeros usan la misma clave para cifrar y descifrar mensajes, los segundos utilizan dos llaves: una pública y otra privada (conocido por el acrónimo en inglés de PKI). Debido al crecimiento exponencial de la capacidad de procesamiento, los estándares de ciframiento aquí descritos son reevaluados periódicamente, por lo que éstos deben ser considerados como un mínimo.
    - Ciframiento sincrónico: Se hace uso del algoritmo AES con una llave de 128 bits.
    - Ciframiento asincrónico: Se hace uso del algoritmo RSA con llave de mínimo 1024 bits.
- Para aquellos procesos que requieren la validación de integridad, la Subdirección de Soluciones de TIC (SOTIC) adopta el algoritmo de hash SHA-2- (de 256 bits), el cual está implementado en una gran variedad de aplicaciones y protocolos de seguridad, como por ejemplo: TLS y SSL, PGP, SSH, S/MIME, PPCoin e IPsec.

5.9 RESPALDO DE INFORMACIÓN (BACK UP)

El respaldo de los archivos de datos de la SDH y la capacidad de recuperar tales datos es un elemento primordial del plan de recuperación de servicios de información (conocido por sus siglas en inglés DRP). La Dirección de Informática y Tecnología (DIT) es la responsable de la definición

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

y la ejecución de la estrategia de back up y recuperación, asegurando la restauración de los datos que hacen parte de los procesos misionales y que han sido definidos como críticos , así como el cumplimiento de los tiempos definidos en las tablas de retención documental.

El procedimiento 46-P-07 del Sistema de Gestión de Calidad establece los pasos y responsabilidades para el respaldo, recuperación y custodia externa de los medios que contienen copia de respaldo de la información de servidores y bases de datos. En forma similar la Subdirección de infraestructura de TICS (SITIC), define y opera políticas y lineamientos de back up para las plataformas de procesamiento central actuales y futuras. Una copia de estas definiciones , puede ser consultada en la plataforma SharePoint o haciendo clic aquí (su acceso requiere permisos otorgados por el administrador del sitio)

Con respecto a las copias de respaldo de la información en equipos de trabajo (PCs) y computadores portátiles, cada usuario es responsable de su almacenamiento haciendo uso de la unidad identificada con la letra “X”, configurada en su equipo.

Servidores e infraestructura de almacenamiento central:

- La Subdirección de Infraestructura de TIC (SITIC) aplica procedimientos de respaldo de información (código, configuraciones y datos) de los ambientes de desarrollo, pruebas y producción, así como de la configuración de los equipos de comunicaciones.
- La Subdirección de Infraestructura de TIC (SITIC) define características como: prioridad (alta, media, baja), día de la semana y hora, tipo de backup (incremental, diferencial, full) para la realización de los backups de sistemas de información alojados en servidores.
- Periódicamente la Subdirección de Infraestructura de TIC (SITIC), verifica la correcta ejecución de los procesos de backup, suministra las cintas requeridas para cada trabajo y controla la vida útil de cada cinta o medio empleado.
- Los medios de almacenamiento utilizados para respaldar la información deben ser adecuados, de acuerdo con su vida útil esperada. Debe considerarse cuidadosamente la compatibilidad del formato en el cual estén almacenados los datos y realizar migraciones, especialmente ante cambios de plataforma y cuando estén involucrados formatos de una plataforma específica.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La Subdirección de Infraestructura de TIC (SITIC) garantiza que se implementan las medidas para salvaguardar y proteger la integridad de los archivos de datos durante la recuperación y restauración; especialmente donde éstos puedan reemplazar archivos más recientes.
- Las copias de respaldo deben guardarse en un lugar de acceso restringido bajo condiciones medio ambientales específicas para medios magnéticos. Se debe mantener copia en un sitio diferente al data center, donde se encuentren protegidas contra posibles amenazas que pueden producir perdida de información.
- La Subdirección de Infraestructura de TIC (SITIC) mantiene un inventario actualizado de las copias de respaldo de la SDH, en el cual se incluye información sobre el contenido como por ejemplo: ubicación física, fecha de generación, fecha de disposición, nombre, tipo de backup, hostname(s), librería(s), tipo de máquina, función, prioridad, tamaño backup, nombre de pool.
- Los medios de almacenamiento que vayan a ser dispuestos para eliminación se destruyen en forma adecuada utilizando un método como: desmagnetización, trituración, pulverización o incineración. Por el contrario aquellos medios que vayan a ser reutilizados surten un proceso de borrado seguro, el borrado seguro también aplica para unidades de almacenamiento de equipos de cómputo que finalizan su ciclo de vida en la entidad, procedimiento que es realizado por la subdirección de servicios de TIC (SETIC). Como criterio para definir el método a aplicar, se debe tener en cuenta el impacto en el medio ambiente.
- La Subdirección de Infraestructura de TIC (SITIC) vela y controla por que los medios que se entregan a un tercero para su custodia sean protegidos contra perdida de confidencialidad, integridad y no disponibilidad, durante su transporte o durante la custodia misma, mediante el uso de elementos como bolsas selladas o contenedores con llave.
- La Subdirección de Infraestructura de TIC (SITIC) dispone de recursos (hardware y software) que tienen por objeto respaldar la información de las áreas, producto del desarrollo de sus funciones y se realizan copias de seguridad de forma periódica.
- Los backup que se transportan a custodia externa se movilizan en vehículos que cuenten con mecanismos de protección contra hurto, así como mecanismos de control y seguimiento como por ejemplo GPS.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- Los medios de almacenamiento que se custodian en instalaciones externas a la SDH deben contar con un alto nivel de seguridad, cumpliendo con medidas como por ejemplo: ubicadas en zonas de bajo riesgo, medidas medio ambientales, temperatura y humedad, control de acceso mediante: tarjeta o sistemas biométricos, vigilancia con circuito cerrado de televisión y personal especializado en seguridad.
- La rotación de medios se hace cuando dichos medios han cumplido los tiempos estipulados por las tablas de retención documental de la entidad.

Equipos de escritorio y portátiles.

- Los usuarios son responsables de copiar la información resultante del ejercicio de sus funciones, en los recursos que ha dispuesto la Subdirección de Infraestructura SITIC, para que se realice la respectiva copia de seguridad. Los cuales se identifican como unidad X en el PC del usuario.
- Solo en circunstancias excepcionales se realizará copia de seguridad de los equipos de los usuarios o portátiles. Cuando sea éste el caso, la Subdirección de Servicios de TIC (SETIC) realiza copia de respaldo de la información.
- Es responsabilidad de cada área mantener depurada y actualizada la información en los recursos de almacenamiento dispuestos por la Subdirección de Infraestructura de TIC (SITIC).

5.10 SEGURIDAD FÍSICA Y DEL ENTORNO.

Las medidas de seguridad física de la sedes de la entidad, se rigen por los procedimientos y guías del SGC como son: 42-I-11, 76-I-09, 78-I-03, 78-P-02 y POL-06 [5] entre otros.

Este grupo de lineamientos tiene como objetivo complementar los documentos antes referenciados y detallar algunos aspectos de seguridad para áreas de acceso restringido, para lo cual se centran en la minimización de los riesgos de seguridad física, que puedan afectar los

[5] o los que los sustituyan, modifiquen o adicionen conforme a las definiciones del área responsable.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

activos de información, así como las instalaciones donde éstos se encuentren. Aplican para todas las instalaciones que resguarden los activos de información de la SDH y es de obligatorio cumplimiento para funcionarios, contratistas y visitantes.

- El acceso físico a las áreas restringidas está controlado mediante técnicas robustas de control de acceso, identificación y autenticación, las cuales contemplan cerraduras, identificación con tarjeta de proximidad y hueella dactilar. El personal autorizado para acceder a éstas debe contar con información de los riesgos propios del área.
- Las solicitudes de acceso al centro de cómputo o a los centros de cableado son registradas en una bitácora y aprobadas por funcionarios de la Subdirección de Infraestructura de TIC (SITIC) autorizados para ésto y los visitantes siempre deberán estar acompañados de un funcionario de dicha subdirección durante su visita.
- La Dirección de Gestión Corporativa deshabilita o modifica los privilegios de acceso físico al centro de cómputo, archivos y los centros de cableado, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- La Subdirección de Infraestructura de TIC (SITIC) provee las condiciones físicas y medioambientales necesarias para la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo: mediante sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de video vigilancia; algunos de éstos generan alarmas en caso de detectar condiciones inapropiadas y son monitoreados de manera permanente.
- La Subdirección de Infraestructura de TIC (SITIC) vela porque los recursos de la plataforma tecnológica de la SDH ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas: mediante el uso de UPS y plantas eléctricas que son responsabilidad de la Dirección de Gestión Corporativa.
- La Dirección de Gestión Corporativa garantizará que las instalaciones del data center y los centros de cableado se encuentran separadas de áreas que tengan líquidos inflamables y que aquellas cuentan con medidas de protección y detección contra riesgos como; inundación e incendio.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La Dirección de Informática y Tecnología asegura que las labores de mantenimiento de redes eléctricas, de voz y de datos, son realizadas por personal debidamente autorizado e identificado, manteniendo un registro de control de las visitas.
- Los Directores, Subdirectores y Jefes de Oficina velan porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas sólo sean utilizados por funcionarios autorizados y que éstos no sean conocidos por otros funcionarios, salvo en situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran; en este último caso, los mecanismos de acceso deben ser inicializados por parte del personal autorizado una vez superada la emergencia.
- La Subdirección Administrativa y Financiera:
    - Proporciona los recursos necesarios para proteger, regular y velar por el buen estado de los controles de acceso físico implantados en la entidad.
    - Basada en el análisis de riesgos, identifica mejoras o nuevos mecanismos de protección requeridos con el fin de proveer la seguridad física de las instalaciones de la entidad.
    - Gestiona los registros del sistema de control de acceso a la entidad y la Dirección de Informática y Tecnología brinda el soporte técnico, así como realiza el almacenamiento y custodia de las copias de respaldo.
    - Vela por la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.
- La Dirección de Informática y Tecnología realiza revisiones periódicas al cableado estructurado con el fin de evitar interceptación de tráfico o daños.
- Los ingresos y egresos de personal a las instalaciones de la SDH son registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir con los controles de acceso implantados.
- Los funcionarios portan el carné que los identifica como tales en un lugar visible mientras se encuentren en la entidad; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.
- A los servidores públicos y personal provisto por terceras partes no les es permitido ingresar a áreas a las cuales no tengan autorización.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- Todo equipo informático ingresado al Centro de Cómputo deberá ser registrado en una bitácora para su monitoreo y control.

5.11 CORREO ELECTRÓNICO.

Los siguientes son los lineamientos para el uso del servicio de correo electrónico corporativo.

- La Dirección de Informática y Tecnología garantiza el óptimo funcionamiento de la plataforma de correo electrónico.
- La Subdirección de Infraestructura de TIC (SITIC) establece procedimientos e implanta controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- Los funcionarios de la SDH cuentan con un correo electrónico institucional que es personal y es de uso exclusivo para temas institucionales. ´
- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, es considerado uso indebido utilizar el correo de otra persona.
- Los mensajes y la información contenida en los buzones de correo institucional son considerados propiedad de la SDH y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los correos electrónicos institucionales son mecanismos oficiales de comunicación, es responsabilidad de los usuarios leer y responder oportunamente.
- Cada usuario del correo electrónico tiene asignado de un espacio de almacenamiento para su buzón, el tamaño es definido por la Dirección de Informática y Tecnología. Es responsabilidad del funcionario administrar dicho espacio.

- La Dirección de Informática y Tecnología procura que todos los archivos adjuntos recibidos en los correos electrónicos, sean revisados con el fin de constatar que no contengan virus o código malicioso.
- Los buzones institucionales (por ejemplo, contactenos@shd.gov.co) deben estar asociados al menos a un funcionario, quien es el responsable de la información recibida y enviada desde ese correo electrónico.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

5.12 INTERNET Y REDES SOCIALES.

Los siguientes lineamientos se aplican para estos servicios:

- La Dirección de Informática y Tecnología proporciona los recursos necesarios para la prestación del servicio de acceso a Internet. Debido a que se debe garantizar la calidad del servicio y gestionar el riesgo derivado del acceso a los diferentes sitios web, los usuarios, según las necesidades de su cargo, se encuentran agrupados en categorías, las cuales se detallan a continuación:

Nivel de Acceso (*)	Cargos	Tipo de Páginas de Internet Permitidas
3	Funcionarios de la mesa de dinero de la tesorería.	Financieras, económicas, gobierno, educativas y buscadores. (Se excluyen los servicios de correo electrónico público y de mensajería instantanea).
2	Servidores públicos de la SDH que no hagan parte del grupo 3 (nivel por defecto).	Adicionales a las del nivel 3, las siguientes: comerciales y noticias.
1	Directivos, Asesores y Personal de la Oficina Asesora de Comunicaciones.	Adicionales a las del nivel 2, las siguientes: redes sociales, video y audio.

* Ordenadas de mayor a menor restricción.

Tabla de niveles de acceso para el uso de Internet.

Cuando un funcionario requiere un nivel de acceso diferente al aquí establecido, debe contar con la autorización de su jefe inmediato y tramitar la solicitud de cambio de categoría por medio del formato 65-F-14.

- La Subdirección de Infraestructura de TIC (SITIC) implementa controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como de alto riesgo.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- La Subdirección de Infraestructura de TIC (SITIC) genera registros de la navegación y los accesos de los usuarios a Internet y se reserva el derecho a auditarlos y monitorear el uso de los recursos.
- Los usuarios del servicio de Internet de la SDH pueden hacer uso del mismo,siempre que esté relacionado con las funciones del cargo que así lo requieran; el uso con fines diferentes es facilitado por la entidad, sin que ésto se entienda como permiso para realizar actividades al margen de la ley, que atenten contra el bienestar y buen nombre de terceros o que afecten la imagen de la entidad.
- Los usuarios del servicio de Internet deben evitar la descarga de software, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores, salvo el personal expresamente autorizado para esto.
- No está permitido el acceso a páginas relacionadas con: pornografía, drogas, alcohol, racismo, terrorismo, insurgencia, violencia, web proxys, hacking y/o cualquier otra página que vaya en contra de la ética, las buenas costumbres, las leyes vigentes o normas establecidas en este documento o cualquier actividad que discrimine o afecte el buen nombre de una persona o entidad.
- No está permitida: la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores, fondos de pantalla, información u obras, así como cualquier otra acción que atente contra los derechos de propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad, confidencialidad de la infraestructura tecnológica, entre otros.
- No está permitido el intercambio o publicación no autorizada de información de uso interno de la SDH.
- No está permitido el acceso y uso de páginas para realizar, en nombre propio o de terceros, transacciones o negocios de especulación privada tales como pirámides, comercio multinivel, acceso a sistemas transaccionales de bolsas de valores, de divisas o de mercancías, así como la promoción o uso de criptomonedas.
- Los funcionarios son responsables del acceso a Internet, a sus contenidos así como al uso racional del servicio.
- La Dirección de Informática y Tecnología ofrece el servicio de internet, garantizando su disponibilidad, tiempos de respuestas adecuados, navegación segura y protección de la

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

red de datos de posibles ataques y delincuentes digitales, mediante la implementación y puesta en producción de estrategias de seguridad digital.

- La Dirección de Informática y Tecnología utiliza filtros de software y otras técnicas posibles para restringir el acceso a información inapropiada en Internet por parte de los funcionarios.
- Se generan reportes de intentos de acceso, los cuales son revisados por entes de control de manera periódica.
- Los navegadores de Internet se configuran, maximizando las características de seguridad propias del mismo. La Subdirección de Servicios Tecnológicos asegura la configuración apropiada para los navegadores en los equipos.
- La información obtenida de las fuentes de Internet debe ser verificada antes de su utilización para propósitos institucionales.

5.13 AUDITORÍA.

El proceso de auditoría debe realizarse privilegiando el uso de herramientas de propósito específico, como son: auditoría propia de la base de datos o software de capa media (o middleware). Cuando la auditoría sea resuelta en forma autónoma por la aplicación, han de considerarse los siguientes aspectos:

- Mecanismo de registro de eventos: Se debe permitir que la aplicación y todos sus componentes (Bases de datos, servidor web, etc.) generen registros de auditoria a través de syslog y archivos locales.
- Configuración de eventos a auditar. La aplicación debe implementar un módulo que permita seleccionar los eventos que deban ser registrados en el archivo de auditoria; algunos de los eventos a considerar incluyen los siguientes:
    - Inicio y detención de servicios.
    - Autenticación.
    - Gestión del control de acceso (otorgamiento de permisos).
    - Acciones de usuarios privilegiados.
    - Invocación de procesos sensibles.
    - Intentos de acceso no autorizado a información.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

- Borrado o actualización de información sensible (ej. claves de acceso).
- Modificación de configuración sensible.

- Asociación usuario con registro de auditoria. Todos los registros de auditoría deben estar asociados por el identificador de usuario y/o el proceso que los origina.
- Visualización y notificación de registros de auditoria. Se debe proveer con la aplicación un módulo de visualización de los eventos generados. También se debe permitir configurar los eventos que deben ser reportados inmediatamente a través de correo electrónico o mensajería instantánea (notificaciones).
- Falla en el registro de eventos. Se debe notificar al administrador cuando el registro de eventos sea fallido y debe intentar automáticamente el reinicio del proceso de registro de auditoría.
- Integridad y disponibilidad de los registros de auditoria. Se deben implementar mecanismos de protección de integridad y disponibilidad de los registros de auditoría. Para garantizar la integridad los registros deben ser firmados y para garantizar la disponibilidad, los registros deben ser ingresados en los esquemas de backup.
- Control de acceso sobre los registros de auditoria. Los registros de auditoría deben estar protegidos mediante esquemas de control de acceso (roles), en el sistema de archivos o en la base de datos, según sea el caso. Los usuarios autorizados sólo podrán acceder en modo consulta a los registros de auditoría.
- El estándar de configuración de auditoría para el directorio activo es el que se muestra a continuación; algunas de estas características, por equivalencia también aplican para otras plataformas (por tratarse de aspecto técnicos se presentan en inglés, ya que los mismos están dirigidos a personal de ingeniería y administradores de plataformas de TI).

Configuración de Auditoria para el Directorio Activo

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Característica	Tipo de evento	Observaciones / Fuente
Sincronización de hora		Los servidores que soportan los procesos de misión crítica y todo componente que hace parte de la plataforma de seguridad se mantienen sincronizados con el servidor NTP.
Audit Policy – Audit account logon events	éxito o falla	Se audita cada instancia de inicio o cierre de sesión de usuario en otro equipo distinto del que se utiliza para validar la cuenta.
Audit logon events	éxito o falla	Se audita cada instancia de un inicio o cierre de sesión de usuario en un equipo.
Audit policy change	éxito o falla	Se auditan todas las incidencias de los cambios en las directivas de asignación de derechos de usuario, las directivas de auditoría o las directivas de confianza.
Audit Policy – Audit account management	éxito o falla	Se audita cada suceso de la administración de cuentas en un equipo. Algunos ejemplos de eventos de la administración de cuentas son: se crea, cambia o elimina una cuenta de usuario o un grupo; se cambia el nombre; se deshabilita o se habilita una cuenta de usuario; se establece o se cambia una contraseña.
Audit system events	éxito o falla	Se audita cuándo un usuario reinicia o apaga el equipo, o si se produce un suceso que afecte la seguridad del sistema o el registro de seguridad.
Advanced Security Audit policy / Audit Logoff	éxito	Determina si el sistema operativo genera eventos de auditoría cuando finalizan las sesiones de inicio de sesión. Estos eventos se producen en el equipo en el que se obtuvo acceso. En el caso de un inicio de sesión interactivo, estos eventos se generan en el equipo que se ha iniciado la sesión
Advanced Security Audit policy / Audit logon	éxito o falla	Determina si el sistema operativo genera eventos de auditoría cuando un usuario intenta iniciar sesión en un equipo. Estos eventos están relacionados con la creación de inicios de sesión y se producen en el equipo en el que se obtuvo acceso.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Característica	Tipo de evento	Observaciones / Fuente
Audit Other Account Management Events		Se genera registro de auditoría si se llama a la comprobación de directivas de contraseña aplicación interfaz de programación (API) o si se realizan cambios en la directiva de dominio
Audit User Account Management	éxito	Determina si el sistema operativo genera eventos de auditoría cuando se realizan las tareas de administración de cuenta de usuario: • Una cuenta de usuario es creada, cambiada, elimina, cambia el nombre, deshabilitada, habilitada, bloqueada o desbloqueada. • Configurar o cambiar la contraseña de una cuenta de usuario. • Historial de seguridad (SID) de identificador se agrega a una cuenta de usuario. • Se establece la contraseña del modo de restauración de servicios de directorio. • Se cambian los permisos en las cuentas que son miembros de grupos de administrador. • Credenciales de administrador de credenciales son una copia de seguridad o restauración.
Audit Account Lockout	falla	Genera evento de auditoría si se intenta acceder con una cuenta que se encuentra bloqueada.
Audit Special Logon	éxito	Determina si el sistema operativo genera eventos de auditoría cuando: • Inicio de sesión con privilegios equivalentes a administrador.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

Característica	Tipo de evento	Observaciones / Fuente
Audit Policy Change	éxito	Se genera eventos de auditoría cuando se realizan cambios en la directiva de auditoría, como: • Cambiar los permisos y la configuración de auditoría en el objeto de directiva de auditoría (mediante el uso deauditpol /set /sd). • Cambiar la directiva de auditoría del sistema. • Registrar y anular el registro de los orígenes de eventos de seguridad. • Cambiar la configuración de auditoría por usuario. • Cambiar el valor deCrashOnAuditFail. • Cambiar la configuración de auditoría en un objeto (por ejemplo, modificar la lista de control de acceso de sistema (SACL) para un archivo o clave del registro).
Audit Authentication Policy Change	éxito	Genera eventos de auditoría cuando se realizan cambios en la directiva de autenticación, como: • Creación, modificación y eliminación de las confianzas de dominio. • Cambios en la directiva de Kerberos en Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas Cuenta\directiva

Esta configuración se debe utilizar como referencia, debido a la dinámica y evolución de esta plataforma en el tiempo y se debe adaptar según las nuevas funcionalidades y características de seguridad de las nuevas versiones.

6. CONTROL DE CAMBIOS

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia

VERSIÓN	FECHA	DESCRIPCIÓN DE CAMBIOS
1	21/06/2018	N.A.

7. APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Oscar Ramirez Cárdenas * Profesional Universitario	Elda Francy Vargas Bernal * Directora de Gestión Corporativa Leonardo Arturo Pazos Galindo * Director Jurídico Hector Felipe Ángel Carvajal * Tesorero Distrital Lisandro M Junco Riveira Director de Impuestos de Bogotá Luis Felipe Rivera García * Director Informática y Tecnología. Nelson Andrés Pardo Figueroa * Jefe Oficina Asesora de Planeación Oscar Javier Cruz Martinez * Subdirector de Talento Humano John jairo Vargas Supelano * Subdirector de Gestión Documental Alfonso Javier Segura Melo * Subdirector Administrativo y Financiero	Beatriz Elena Arbeláez Martínez * Secretaria de Hacienda Hector Mauricio Escobar Hurtado * Subsecretario General

* Firmó documento original aprobado en Comité del Sistema Integrado de Gestión el 7 de diciembre de 2017.

Sede Administrativa: Carrera 30 Nº 25-90
Código Postal 111311
Teléfono (571) 338 5000 • Línea 195
contactenos@shd.gov.c
Nit. 899.999.061-9
Bogotá, Distrito Capital - Colombia