MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

11 de Febrero de 2022

BOGOTÁ D.C. - COLOMBIA

TABLA DE CONTENIDO

CONTROL DE CAMBIOS			
FECHA	**VERSIÓN**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**
11/1/2022	0.1	Versión Inicial	Gerardo Moreno
10/02/2022	0.2	Ajuste al documento con nueva información	Gerardo Moreno
15/02/2022	0.3	Ajustes solicitados por la SDDE	Gerardo Moreno
08/03/2022	0.4	Ajustes solicitados por la SDDE	Gerardo Moreno

REFERENCIAS CONTRACTUALES DEL ENTREGABLE:
Contrato 530-2021. Objeto: Servicio de consultoría para dar cumplimiento a la Política de Gobierno Digital con la definición y diseño del modelo de referencia de arquitectura empresarial.

ACCIÓN	NOMBRE	ROL	FECHA
Elaboró	Gerardo Moreno	Arquitecto Empresarial	02/2022
Revisó	Hilda Jiménez	Gerente de Proyecto	02/2022
Aprobó	Armando Calderón	Supervisor contrato 530-2021	02/2022

1 INTRODUCCIÓN

La Secretaria Distrital de Desarrollo Económico tiene como misión liderar la formulación, gestión y ejecución de políticas de desarrollo económico, orientadas a fortalecer la competitividad, el desarrollo empresarial, el empleo, la economía rural y el abastecimiento alimentario, a través del diseño e implementación de estrategias efectivas que conlleven a la generación y mejora de ingresos de las personas, las empresas y el mejoramiento de la calidad de vida de los habitantes de la ciudad en general, fuente página www.desarrolloeconomico.gov.co, para esto la Secretaría Distrital de Desarrollo Económico cumple con las funciones estipuladas en el Artículo 3 del Decreto 552 de 2006 y el Artículo 1 del Decreto 91 de 2007.

En el desarrollo de sus actividades genera, preserva, compila, distribuye información, datos, documentos, etc. Esta información, al igual que la plataforma tecnológica son consideradas por la SDDE como activos valiosos para su funcionamiento y consecución de objetivos, por tal razón se hace necesario implementar un Sistema de Gestión de Seguridad de la Información – SGSI – el cual se enfoca en la gestión de riesgos y en el seguimiento de procedimientos y activación de controles para alcanzar el nivel óptimo de la seguridad de la información.

El Manual de Seguridad del Sistema de Gestión de Seguridad de la Información (MSGSI) suministra lineamientos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información. El Manual considera las necesidades y objetivos, los requisitos de seguridad, los procesos en donde se maneja información y el tamaño y estructura de la Secretaría Distrital de Desarrollo Económico, además promueve la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información, a través de la aplicación de procesos de gestión del riesgo, brindando confianza a las partes interesadas y disminuyendo su afectación en caso de posibles incidentes.

Este manual describe los lineamientos a alto nivel del SGSI tales como: su alcance, contexto, objetivos, organización, políticas, procesos y procedimientos.

2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La formulación e implementación del Sistema de Gestión de Seguridad de la Información aporta al uso estratégico de las tecnologías de la información a través de un enfoque en la preservación de la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información apoya el tratamiento de la información utilizada en los trámites y servicios que ofrece la SDDE, cumpliendo en todo momento con las normas sobre protección de datos personales, de Transparencia y acceso a la información pública, y alineándose con el marco de Referencia de Arquitectura TI.

El SGSI contribuye en la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

2.1 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información y Seguridad Digital aplica a todo el recurso humano interno y externo (funcionarios, contratistas, proveedores y pasantes) de la SDDE, y a terceros o externos que por el cumplimiento de sus funciones y las de la SDDE compartan, utilicen, recolecten, procesen, intercambien, transformen o consulten información, así como los entes de control, entidades relacionadas que accedan, ya sea interna o externamente, a cualquier tipo de información física o digital, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por la SDDE, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

2.2 CONTEXTO

En la búsqueda de mejorar la gestión de la SDDE se adoptó el Sistema Integrado de Gestión mediante la Resolución 111 de 2007, el cual genera beneficios como el cumplimiento de normatividad legal, mejora permanente de la capacidad institucional, diseño y aplicación de documentos de apoyo dentro de cada proceso, y ejecución de controles.

A través del mapa de procesos, se puede visualizar los procesos (Misionales, Estratégicos, de Apoyo y de Evaluación) sus interrelaciones, dentro de las cuales está contenida la base documental (procedimientos, manuales, formatos, guías e instructivos) para el desarrollo, mejora y logro de los objetivos institucionales.

Los procesos incluidos para el Sistema de Gestión de Seguridad de la Información corresponden a todos los procesos definidos por la Secretaría Distrital de Desarrollo Económico que hacen uso de la información y de las herramientas tecnológicas como se observa en el mapa de procesos de la Entidad.

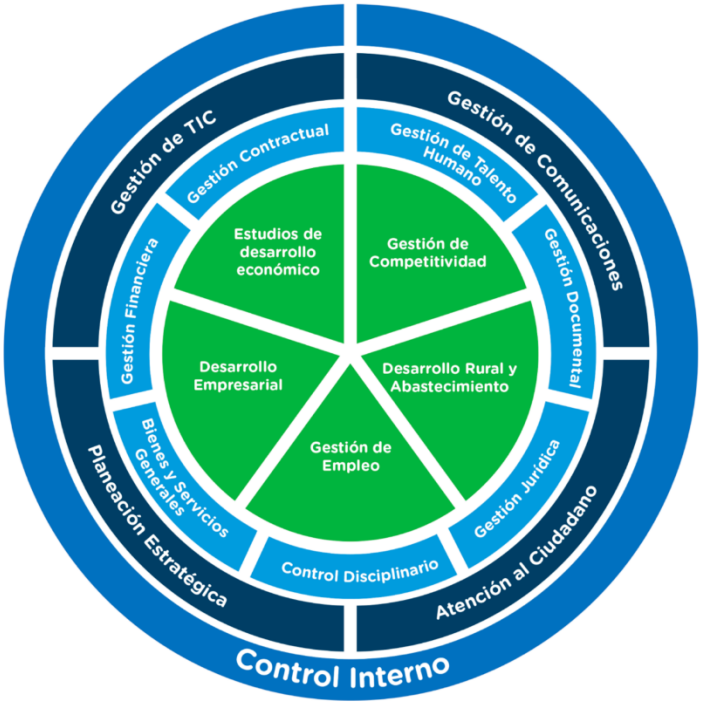

Imagen 1 – Mapa de Procesos de la Secretaría Distrital de Desarrollo Económico.

2.3 OBJETIVO DEL SGSI

Asegurar que se implementen y cumplan todos los controles adecuados sobre confidencialidad, integridad y disponibilidad de la información en la SDDE.

2.3.1 Objetivos Específicos

i. Definir, formular y formalizar los elementos normativos sobre la protección de la información.
ii. Gestionar los riesgos de Seguridad y Privacidad de la Información y de Seguridad Digital de manera integral.
iii. Mitigar el impacto de los incidentes de Seguridad y Privacidad de la Información y Seguridad Digital que se presenten en la Entidad.

iv. Establecer los mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información de la SDDE.
v. Definir los lineamientos necesarios para la gestión de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
vi. Generar conciencia y cultura de Seguridad y Privacidad de la Información como eje transversal de la SDDE.
vii. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, Seguridad Digital y protección de la información personal.

2.4 ORGANIZACIÓN DE SEGURIDAD

A nivel interno, mediante Resolución 084 de 2020 se adoptó el Plan de Seguridad y Privacidad de la Información, dicho plan determina la existencia de un Comité de Gestión de Seguridad de la Información, así mismo menciona un Oficial de Seguridad de la Información y su equipo de apoyo junto con sus funciones y responsabilidades.

2.5 RESPONSABILIDADES Y ROLES

A continuación, se definen las responsabilidades de los colaboradores de la SDDE frente al SGSI

2.5.1 Comité Directivo

Aprobar los siguientes planes:

Plan Estratégico de Seguridad de la Información (PESI)

- Plan de Implementación del Sistema General de Seguridad de la Información.

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2.5.2 Comité de Seguridad

El Comité de Seguridad es el responsable del mantenimiento y mejora continua del SGSI de la SDDE y de su ejecución y reporte de las acciones requeridas para mantener la seguridad en los niveles requeridos de la Entidad.

Está conformado por el Oficial de la Seguridad de la Información, el Subdirector de Informática y Sistemas y un representante de las áreas de misionales de la Entidad.

Su principal función es la de asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

Respecto a la Seguridad de la Información sus responsabilidades son:

- Aprobar el Manual de Seguridad de la Información y aquellos documentos de alto impacto relacionados con la seguridad de la Información.
- Revisar el Manual de Seguridad de la Información una vez al año o cuando sucedan cambios en el objetivo del negocio o en el entorno de riesgo.
- Aprobar el proceso de Seguridad y Privacidad de la Información, sus ajustes y modificaciones.
- Realizar seguimiento periódico a los riesgos de seguridad y privacidad de la información.
- Con base en las directrices para la gestión de la seguridad y la privacidad de la información y el modelo integral de gestión, revisar y aprobar, el Plan Estratégico de Tecnologías de la Información PETI de la entidad y demás normatividad aplicable.
- Aprobar las políticas específicas de seguridad de la información.
- Aprobar los controles a implementar para dar cumplimiento a estas políticas.
- Realizar seguimiento detallado a los informes de seguridad generados por la Subdirección de Informática y Sistemas y aprobar sus planes o acciones a tomar medidas sobre ellos.

- Prevenir pérdidas patrimoniales o que arriesguen los activos de información de la Entidad.
- Tomar decisiones frente a los incidentes de seguridad.
- Asesorar técnicamente a la Entidad para asegurar la protección de los Activos de Información de conformidad con los principios de seguridad de la Información.
- El Comité se reunirá periódicamente, previa convocatoria del Oficial de Seguridad de la Información. También puede ser convocado de manera extraordinaria cuando se sucedan circunstancias que lo ameriten.

2.5.3 Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información de la Entidad hace parte de la Subdirección de Informática y Sistemas y es responsable del diseño, desarrollo, implantación, mantenimiento y verificación del correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en línea con los requerimientos de la SDDE, el cual tendrá las siguientes responsabilidades:

- Apoyar a las diferentes dependencias de la Entidad en el análisis de riesgos de la información.
- Diseñar, desarrollar, instituir y controlar el proceso de Seguridad de la Información.
- Establecer los lineamientos de Seguridad de la Información.
- Definir la Arquitectura de Seguridad de Información en línea con la arquitectura de tecnología de la Entidad.
- Determinar la estrategia de uso y apropiación de la Seguridad de la Información.
- Especificar los lineamientos y las directrices de Seguridad de la Información a ser incluidas en el Plan de Contingencias.
- Establecer indicadores de gestión de calidad del Proceso de Seguridad de la Información en la Entidad.
- Asesorar en materia de Seguridad de la Información a la entidad.
- Promover el mejoramiento continuo de los Procesos de Seguridad de la Información en la Entidad.
- Gestionar los incidentes de Seguridad de la Información reportados por los funcionarios/contratistas o terceros e informar al Comité de Seguridad.

2.5.4 Líder de Seguridad Informática

El Líder de Seguridad informática de la Entidad hace parte de la Subdirección de Informática y Sistemas y es responsable del diseño, desarrollo, implantación, mantenimiento y verificación del correcto funcionamiento de la seguridad informática de la SDDE, con las siguientes responsabilidades:

- Diseñar, con el apoyo del Oficial Seguridad de la Información, la estrategia de ciberseguridad para la SDDE.
- Identificar riesgos que afecten la seguridad en la infraestructura tecnológica de la SDDE y proponer medidas preventivas.
- Gestionar los recursos de seguridad informática en la SDDE.
- Establecer controles asociados a los recursos tecnológicos de la Entidad.
- Determinar la Arquitectura de Seguridad Informática de acuerdo con la arquitectura TI de la Entidad.
- Gestionar los Incidentes /ciberincidentes en la infraestructura tecnológica.
- Participar en controles de seguridad informática en el Plan de Recuperación de Tecnología.
- Asesorar y comunicar a las partes interesadas en materia de ciberseguridad.

2.5.5 Subdirección de Informática y Sistemas

La Subdirección de Informática y Sistemas es responsable de administrar y controlar el acceso a los recursos de la plataforma tecnológica en la SDDE de acuerdo con la descripción del cargo. Sus responsabilidades frente al SGSI son:

- Monitorear a través de las herramientas tecnológicas de la Entidad el comportamiento del uso del servicio de Internet.
- Verificar qué usuarios y/o contratistas tienen acceso remoto a los recursos de la Entidad.
- Asegurar el correcto funcionamiento y la disponibilidad que la Entidad requiere del servicio de Internet, sobre el cual se deben aplicar los controles que se definan.
- Generar informes del uso del servicio, como medida preventiva de seguridad que permita tomar decisiones y realizar ajustes de configuración.

- Los terceros que requieran un acceso puntual a Internet se dará exclusivamente por medio de una red inalámbrica específica para tal fin, la cual contará con los mismos controles que la red institucional.
- Gestionar los accesos a los servicios o sistemas de información que dependan de la SDDE, y solicitar aquellos que deban ser tramitados ante externos, de acuerdo con lo indicado por los responsables o dueños de los sistemas de información.

2.5.6 Gestión Corporativa – Talento Humano

Responsable de facilitar los mecanismos necesarios para la creación de una cultura organizacional en Seguridad de la Información, así como de la implantación, mantenimiento y desarrollo de la organización de Seguridad de la Información. Entre sus responsabilidades de seguridad de la información, están:

- Apoyar al Oficial de Seguridad de la Información en la implementación, medición y fomento del Programa de Concientización en Seguridad de la Información.
- Participar en la investigación de las personas que tengan acceso a información crítica.
- Fomentar el cumplimiento de las Políticas y procedimientos de Seguridad de la Información en la Entidad a través de eventos de reconocimiento, incentivos, metas anuales, etc.
- Incluir responsabilidades tanto directas como indirectas en cuanto a Seguridad de la Información en el manual de funciones y en los contratos de prestación de servicios.

2.5.7 Oficina Asesoría Jurídica

La Oficina de Asesoría Jurídica es responsable de apoyar y asesorar, jurídicamente y contractualmente, en los aspectos relacionados con Seguridad y Privacidad de la Información, para que el SGSI se encuentre dentro del marco legal correspondiente y cuente con el sustento legal que formalice y haga viable su aplicación, entre sus responsabilidades de seguridad de la información, están:

- Verificar que el Sistema de Gestión de Seguridad de la Información emitido por la Entidad cuente con el sustento legal que permita su formalización, aplicación y obligatorio cumplimiento previa publicación y difusión
- Asesorar a la SDDE en el cumplimiento de las normas legales locales y/o internacionales que afecten a la Entidad en términos de Seguridad y Privacidad de la Información.
- Alertar al Oficial de Seguridad de la Información de la Entidad cuando se presenten cambios en las normas que afecten el Sistema de Gestión de Seguridad de la Información de la Entidad.
- Asesorar a la Entidad, en materia de Seguridad de la Información cuando se presenten pleitos o investigaciones.
- Analizar y orientar a la Entidad sobre los datos que son susceptibles de poner a disposición del público, sin que esto implique la vulneración de los derechos fundamentales de los individuos y el incumplimiento de la normatividad, en cuanto a la reserva legal que tienen algunos datos.
- Aplicar la normatividad jurídica para responder las solicitudes de información reservada y clasificada por parte de externos.
- Asesorar a la Entidad en la modificación de los contratos de prestación de servicios y el manual de funciones de los funcionarios y del reglamento interno de trabajo para que se incluyan responsabilidades de Seguridad de la Información y cláusulas de confidencialidad de la información.

2.5.8 Oficina de Control Interno

La Oficina de Control Interno es responsable de efectuar la verificación y seguimiento a la formulación, ejecución y resultados de los planes, programas, procedimientos y metodologías en los aspectos relacionados con Seguridad y Privacidad de la Información.

2.5.9 Oficina Asesora de Planeación

La Oficina Asesora de Planeación es responsable de incorporar la formulación, seguimiento y evaluación de los aspectos relacionados con Seguridad y Privacidad de la Información de conformidad con los lineamientos del plan estratégico de la entidad. También es responsable de determinar políticas de

protección de datos y privacidad de información sensible de acuerdo a los requerimientos legales.

2.5.10 Oficina de Atención al Ciudadano

La Oficina de Atención al Ciudadano es responsable de informar al ciudadano en los aspectos relacionados con Seguridad y Privacidad de la Información que se desarrollan en la SDDE.

2.5.11 Oficina de Gestión Documental

La Oficina de Gestión Documental es responsable de:

- Controlar y custodiar los documentos relacionados con Seguridad y Privacidad de la Información.
- Establecer controles de seguridad de la información que permitan prevenir riesgos asociados a los principios de confidencialidad, disponibilidad e integridad de la información almacenada por la Entidad.
- Generar el inventario y archivo de la diversidad documental asociada con la Seguridad de la Información.

2.5.12 Directores, Subdirectores y Jefes de Dependencia

Asegurar que todos los procedimientos de seguridad de la información se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información.

2.5.13 Líder de procesos y su información

Los Responsables de la Información en la Entidad deben valorar su información, reconocer los riesgos a que se expone y cuidar de que se provean los mecanismos necesarios para mitigar los riesgos a niveles aceptables. Frente a las responsabilidades de seguridad de la información, están:

- Identificar los activos, riesgos y controles para el manejo de la información.
- Sugerir posibles ajustes para la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Apoyar al Equipo de Seguridad de la Información en la identificación de los requerimientos de Seguridad de la Información.

- Participar en las Auditorías del Sistema de Gestión de Seguridad de la Información.
- Solicitar los accesos a los sistemas de información sobre los cuales sean responsables de acuerdo con los lineamientos definidos por la Subdirección de Informática y Sistemas.

Informar de manera oportuna a la Subdirección de Informática y Sistemas cuando el funcionario ha dejado de pertenecer a la Entidad, inicie su periodo de vacaciones o licencia, o cuando algún usuario tenga novedades en sus roles o funciones, para revocar o modificar las credenciales asignadas para las aplicaciones y servicios a los cuales tiene acceso.

2.5.14 Recurso Humano Interno

Responsables de llevar a cabo las Políticas, procedimientos y programas del área de Seguridad de la Información para garantizar la protección de la información, entre sus responsabilidades con el SGSI se encuentran:

- Conocer, adoptar y acatar los lineamientos del presente manual.
- Velar por el cumplimiento de los presentes lineamientos, notificando a sus superiores o a la Subdirección de Informática y Sistemas cualquier situación que infrinja o ponga en riesgo al SGSI.
- Los funcionarios y contratistas que sean designados como supervisores deben informar a sus contratistas acerca de las políticas de seguridad de la Información definidas por la Entidad y dejar constancia de este hecho.
- Cumplir con las políticas de Seguridad de la Información.
- Identificar los activos que sean críticos para la Entidad dentro de las actividades que desarrollan.
- Clasificar y manejar la información generada de acuerdo con las instrucciones de elaboración de Matriz de Activos de Información (GT-P5-F1).
- Colaborar e informar en las investigaciones de incidentes de seguridad de información.
- Contribuir en el proceso de concientización de la Entidad sobre la importancia de la Seguridad de la Información.
- Reportar las debilidades de seguridad de la información observadas o sospechas en los sistemas de información o servicios que presta la SDDE,

que afecten la confidencialidad, integridad o disponibilidad de la información.

- Reportar eventos o incidentes que afecten la seguridad de la información.
- Toda actividad realizada con el servicio de navegación de Internet es de responsabilidad exclusiva del usuario.
- Es responsabilidad del usuario proteger la identidad de las credenciales (usuarios y contraseñas) que use en los diferentes servicios y en Internet.
- Alojar la información en el repositorio designado para que sea ejecutado el respaldo de la información, para lo cual deberá tener presente el "procedimiento Copia Respaldo".
- Ningún usuario - cliente está autorizado para interferir o denegar cualquier servicio informático, utilizando programas, scripts comandos o cualquier otro método.
- El acceso no autorizado a la infraestructura tecnológica (Software, Hardware y servicios), se considera una violación de acceso.
- El funcionario y contratista de la SDDE debe bloquear su sesión cuando por cualquier motivo se ausente del puesto de trabajo.

2.5.15 Supervisores

- Mantener informado a los contratistas de los cuales es supervisor, de las políticas de seguridad de la Información que defina la Entidad y que le apliquen de acuerdo con el objeto de su contrato, dejando formalizado por escrito la obligación de los contratistas de conocer, entender y cumplir con dichas políticas.
- Informar de manera oportuna a la Subdirección de Informática y Sistemas cuando un contratista bajo su supervisión se desvincule de la Entidad.

2.6 POLÍTICA DEL SGSI

El Manual de Política de Seguridad de la Información de la SDDE (2019) define la Política de Seguridad como:

"La información se considera como uno de los principales activos de la Entidad, y como tal, debe ser protegida adecuadamente con controles administrativos,

técnicos y legales de forma que se evite que persona o medio físico no autorizado pueda acceder, operar, distribuir la información, atente contra la integridad, confidencialidad y disponibilidad de los activos de información.

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

2.7 LINEAMIENTOS Y NORMAS DEL SGSI

La Secretaría Distrital de Desarrollo Económico define la Seguridad de la información a través de los siguientes lineamientos y normas de Seguridad de la Información:

2.7.1 Control de Acceso

Lineamientos:

Todo usuario de la información de la Entidad, ya sea colaborador o tercero, deberá contar con una credencial o medio de identificación a través del cual se controle el acceso al uso de la información que está autorizado.

El acceso a las áreas seguras identificadas por la Entidad debe ser protegido y restringido.

Normas de Seguridad de la Información para el Control de Acceso:

2.7.1.1 Control de Acceso Lógico

i. La Subdirección de Informática y Sistemas suministrará a los usuarios las credenciales (usuario/contraseña) respectivas para el acceso a la información, los servicios de red y sistemas de información a los que hayan sido autorizados de acuerdo con el procedimiento GT-P7.

ii. En caso de ausencia por vacaciones o licencia, no se deben utilizar las credenciales del funcionario que estará ausente, ya que son intransferibles y en el momento en que se inicie la ausencia, las cuentas pasarán a modo “Inactiva”. La Subdirección de Informática y Sistemas, previa notificación de la Dirección Corporativa - Talento Humano, asignará nuevas credenciales de acceso al par designado del usuario, hasta la finalización del periodo de ausencia. El funcionario que va a estar ausente debe asignar los permisos de lectura al repositorio o entrega de la información necesaria para el trabajo temporal al par designado.

iii. Para los sistemas externos a la SDDE, el jefe de Dependencia deberá realizar la solicitud de los usuarios de acceso a la Subdirección de Informática y Sistemas, con el fin de gestionar ante los dueños de los sistemas de información los respectivos accesos. El custodio y responsable de cada usuario y contraseña será el funcionario al que se le otorga el permiso. Se le informarán éstos datos confidenciales a través de canales seguros de comunicación.

iv. El Jefe de Dependencia o quien haga sus veces será el responsable de informar a la Subdirección de Informática y Sistemas, a través de la herramienta de Mesa de Ayuda los cambios que se deban realizar sobre los usuarios (creación, modificación, eliminación, bloqueo y activación) de manera oportuna y completa. En caso de que la herramienta no se encuentre disponible se podrá realizar por correo institucional. La solicitud debe contener:
   - Nombre y apellidos completos del funcionario o contratista a quien se le asigna/modifica/suspende/elimina la cuenta.
   - Tipo de vinculación con la Entidad.
   - Nombre de la dependencia en donde realiza las funciones.
   - Acto administrativo o número de contrato

- Fecha de iniciación y terminación del contrato o fecha de vinculación del funcionario.
- Sistema de información o aplicaciones a las que accederá el funcionario o contratista.

v. La Subdirección de Informática y Sistemas realizará la revisión periódica de los derechos de acceso de los usuarios y a partir de las novedades que surjan realizará los ajustes que correspondan.

vi. Los cambios a las cuentas privilegiadas se deben controlar, registrar, conservar y realizar revisiones periódicas.

vii. Los sistemas de información de la Entidad deben contar con una bitácora de registro de eventos o acciones por usuario, la Subdirección de Informática y Sistemas podrá verificarlas cuando lo considere necesario.

viii. La Subdirección de Informática y Sistemas debe autorizar, previa solicitud la realización de actividades remotas que utilicen los servidores e infraestructura tecnológica, sistemas, datos, información y procesos de la SDDE informando:

- Fecha de realización de las actividades.
- Dependencia y funcionario que lo solicita.
- Servicio, servidor y/o base afectada.
- Nombre del usuario que realizará la actividad.
- La conexión remota a la red de área local u otros recursos o servicios de la SDDE debe ser hecha a través de una conexión de VPN u otro medio de comunicación segura definida por la Entidad.

ix. El manejo de la información y los servicios en la nube están autorizados siempre y cuando se cumpla con los acuerdos de confidencialidad, integridad y disponibilidad, además, que exista un contrato de servicio y el proveedor cumpla con los requerimientos de las normas y legislaciones vigentes.

x. Se deben establecer mecanismos de autenticación con el nivel de complejidad (clasificación y criticidad) necesarios para la protección de los activos de información que requieran acceso.

xi. Cuando se solicite tener acceso a algún recurso o servicio de la SDDE, la Subdirección de Informática y Sistemas deberá realizar o verificar el análisis de riesgos para definir los privilegios se pueden otorgar y los mecanismos de protección necesarios. Para lo cual se debe elaborar el formato de Perfil de seguridad en donde se identifica por cargos los controles de acceso, el software autorizado, los permisos de los productos corporativos y no corporativos, el nivel de acceso a internet, los permisos sobre medios removibles, acceso a los tipos de información y acceso múltiple factor de autenticación.

xii. La Subdirección de Informática y Sistemas tiene exclusivamente los privilegios de administración de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, o equipo activo de red).

xiii. Los administradores de la Infraestructura, Sistemas, Datos, Información y Procesos, en el desarrollo de sus actividades de administración deben tener un usuario diferente al usado diariamente.

xiv. La Subdirección de Informática y Sistemas realiza al año por lo menos un análisis de vulnerabilidades internas / externas y una prueba de Ethical hacking a todos los servicios y servidores del ambiente de producción. De las vulnerabilidades detectadas se atenderán aquellas que son críticas, altas y medias.

xv. Se debe retirar y dar de baja aquellos equipos (servidores, desktop o portátiles) que, por sus características técnicas, software base, soporte han cumplido su vida útil y son punto vulnerable de seguridad.

2.7.1.2 Control de Acceso Físico

i. Se establece como áreas seguras aquellas ubicaciones sobre las cuales existen mecanismos de control que garanticen la seguridad de la información solo a personal autorizado. Estas son:
   - Sede Santa Helenita.
   - Plataforma Logística los Luceros.
   - Data Center.
   - Área de oficina.

ii. Para el monitoreo de las instalaciones, se cuenta con un circuito cerrado de televisión, con un periodo de conservación de la información de mínimo 2 meses

iii. La protección física de las instalaciones de la SDDE, de las instalaciones de procesamiento de información y del archivo documental debe contar con diferente tipo de barreras o medidas de control físico.

iv. Para el caso de ingreso por parte de proveedores, clientes o visitantes se tramita por el responsable de la actividad mediante una solicitud al oficial de seguridad para la autorización de ingreso, donde se especifica el nombre de la persona, número de cédula, fecha, hora, duración y actividad a realizar por parte del responsable de la actividad.

v. Todos los elementos tecnológicos deben registrar el modelo y serie cuando ingresen a la Entidad, y confrontarlos al ser retirados de las instalaciones. Si se trata de elementos de propiedad de la Entidad, requieren la debida autorización para su retiro, verificando los datos de estos.

vi. Todo aquel elemento o equipo de hardware retirado de las instalaciones de la entidad debe tener su respectiva orden de salida con la firma del líder de proceso o administrador de infraestructura y gerencia administrativa y financiera.

vii. Todas las puertas que utilicen sistema de control de acceso deben permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados evitar que las puertas se encuentren abiertas.

2.7.1.3 Acceso a áreas seguras

i. Las áreas protegidas deben contemplar la posibilidad de daños producidos por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre y los controles necesarios para mitigar los posibles daños.

ii. Se debe tener un Procedimiento de Trabajo en Áreas Seguras en donde se incorpore las condiciones del acceso a Áreas Protegidas.

iii. Para acceso a las áreas seguras se cuenta con un dispositivo de control de acceso con huella donde queda registrado el ingreso de los funcionarios de la entidad.

iv. Cuando un visitante se encuentre dentro de alguna de las áreas restringidas de la Entidad debe estar acompañado en todo momento por un funcionario de la SDDE.

v. Todas las áreas restringidas, así como los activos de información que las componen, deben ser protegidos de acceso no autorizado mediante controles y tecnologías de autenticación fuerte.

vi. En las áreas restringidas donde se encuentren activos informáticos y de archivo documental, como mínimo se debe seguir las siguientes obligaciones:

   a. Se debe evitar el consumo de alimentos y bebidas.
   b. Está prohibido el ingreso de elementos inflamables.
   c. Se restringe el almacenamiento de elementos ajenos a los requeridos de acuerdo con la actividad que se realice en el área segura.
   d. El acceso de personal ajeno, está restringido al acompañamiento permanente de un funcionario.
   e. No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del responsable de dichas áreas.

f. No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), así como maletas o contenedores, a menos que haya una justificación para esto.

2.7.1.4 Acceso al data center

i. Para el acceso al Data Center2 ubicado en Santa Bárbara, se tiene establecido contractualmente las condiciones que contemplan las políticas y procedimientos de seguridad de la ETB.

ii. Para el ingreso al data center de la ETB se tiene establecido un formato de ingreso permanente en el horario 7 * 24.

iii. El acceso al data center de la ETB está restringido únicamente al personal autorizado y bajo la supervisión del área de TI.

iv. Para solicitar autorización de acceso al data center de la ETB se diligencia el formato de ingreso quien mediante comunicación escrita notificará la autorización con fecha y hora de ingreso.

2.7.1.5 Uso apropiado de credenciales de acceso asignadas

i. El uso de las credenciales de acceso para los servicios y sistemas asignados es exclusivo para fines laborales.

ii. Se debe modificar cada noventa (90) días las contraseñas de los sistemas de información o servicio tecnológicos autorizados y para los sistemas de información que no cuenten con solicitud de cambio automático este se deberá solicitar a la mesa de Ayuda. Teniendo en cuenta que las contraseñas deben estar compuestas por mínimo ocho (8) caracteres alfanuméricos y contar con caracteres especiales (Ej. #, @, $, &, etc.) o mayúsculas.

iii. Las contraseñas de uso privilegiado a recursos tecnológicos, debe estar compuesto por mínimo catorce (14) caracteres alfanuméricos y con caracteres especiales.

iv. Está prohibido el uso de una única contraseña para el acceso a los diferentes sistemas operativos, bases de datos u otras aplicaciones.

v. No se deben registrar las credenciales de acceso en libretas, agendas, post-it, hojas, etc. En caso de necesitar un respaldo físico de las contraseñas serán bajo su propia responsabilidad.

vi. No se debe incluir contraseñas en ningún proceso de registro automatizado, por ejemplo, almacenadas en una macro, una clave de función, entre otros.

vii. La clave de acceso será desbloqueada sólo por la Subdirección de Informática y Sistemas, luego de la solicitud formal por parte del responsable de la cuenta.

viii. Las credenciales de acceso son de uso personal e intransferible, por ende, es responsabilidad del usuario el manejo que les dé a aquellas que le sean asignadas, asimismo las claves criptográficas establecidas.

ix. La Subdirección de Informática y Sistemas suministrará, de manera segura, una contraseña temporal para el primer ingreso a cualquier sistema de información, contará con un sistema de forzamiento de cambio inmediatamente realice el siguiente ingreso al sistema. Así como aquellas contraseñas predeterminadas por el fabricante después de la instalación de los sistemas o del software.

x. En caso de que exista duda, sospecha o certeza de que alguna contraseña se ha comprometido, esta debe ser cambiada de manera inmediata y el incidente debe ser reportado según el procedimiento definido.

2.7.1.6 Acceso Remoto

i. El acceso remoto a los servidores críticos y bases de datos, se realizan por el líder, administrador de TI.
ii. Se establece que el tiempo de desconexión por inactividad de la sesión es de 5 minutos.
iii. El Subdirector de informática y sistemas autoriza los accesos remotos de los empleados y proveedores.

iv. Está prohibido copiar, mover o almacenar información de las bases de datos de los servidores cuando se acceda mediante tecnologías de acceso remoto.

2.7.1.7 Acceso Inalámbrico

i. Los puntos de acceso inalámbrico autorizados por la entidad son la red identificada como Plaza Artesanos SDDE para los funcionarios de la Secretaría Distrital de Desarrollo Económico y la red identificada como Invitados para los usuarios externos.

ii. No está permitido la utilización y conexión de la red inalámbrica Plaza Artesanos SDDE de la entidad para actividad diferente a la labor del empleado (se aplica la Políticas de Internet).

2.7.1.8 Acceso por Múltiple Factor de Autenticación

i. Está prohibido copiar, mover o almacenar datos en discos duros locales, dispositivos electrónicos extraíbles al acceder con tecnologías de acceso remoto.

2.7.2 Teletrabajo

***Lineamiento**:*

Todo teletrabajador deberá acceder a través de la red de datos de la SDDE en un equipo que se encuentre dentro del inventario de activos de la Entidad o a través de una red privada virtual que cuente con los requisitos mínimos de integridad y confidencialidad en la transferencia de la información. Los teletrabajadores sólo podrán acceder a los sistemas, aplicativos y servicios que les han sido asignados para el teletrabajo y en los horarios en los cuales se ha pactado dicha actividad.

Normas de Seguridad de la Información para el teletrabajo

i. La SDDE para el desarrollo de las actividades de teletrabajo deberá realizar un análisis de riesgos para las actividades de teletrabajo, y adoptar los mecanismos de control para la protección de la información y los sistemas de información de la Entidad.

ii. La SDDE determinará a través de los líderes de proceso los controles de seguridad alineados con las Políticas Generales de Seguridad y Privacidad de la Información para el desarrollo de las actividades de teletrabajo de acuerdo con los riesgos identificados.

iii. Para la preservación de las características de integridad, disponibilidad y confidencialidad de la información la SDDE establecerá mecanismos de seguridad lógica para los equipos e información usados dentro de las actividades de teletrabajo.

iv. Antes del inicio de las actividades de teletrabajo, la SDDE definirá y autorizará la información a acceder, el horario en que se encuentra disponible, y los sistemas de información requeridos para la actividad.

v. En caso de pérdida o hurto de un equipo o cualquier medio de almacenamiento que contenga información relacionada con la SDDE, es responsabilidad del funcionario notificar el evento a la Subdirección de Informática y Sistemas, con el fin de establecer las medidas de seguridad para la protección de la información y servicios de la Entidad, así como poner la respectiva denuncia, si aplica.

vi. El acceso a la información o sistemas de información a través de los equipos usados para las actividades de teletrabajo, se puede hacer previa solicitud del dueño o responsable del sistema de información o recurso a acceder.

vii. El acceso remoto únicamente se podrá realizar desde equipos propiedad de la SDDE o desde los personales siempre que cumplan con contar con un software adquirido legalmente y con niveles adecuados de seguridad y sobre los cuales se pueda confirmar el cumplimiento de requerimientos de seguridad, antes de permitir la conexión remota a los servicios o recursos de la infraestructura tecnológica, sistemas, datos, información y procesos de la Entidad.

viii. Las labores que requieren el uso de base de datos o sistemas de información con restricción de licenciamiento remoto y que estén con acceso exclusivo desde la SDDE se debe realizar el teletrabajo con equipos de la Entidad únicamente.

ix. La conexión remota a servicios o información de la SDDE se debe realizar a través de canales de comunicación seguros, como redes privadas virtuales, escritorios virtuales, entre otros tipos.

x. En el esquema de teletrabajo se prohíbe el almacenamiento de información clasificada, en los equipos personales o en servicios de la nube públicos o híbridos, salvo los servicios de nube que estén establecidos como corporativos y provistos por la Entidad.

xi. La SDDE determinará las condiciones de los acuerdos necesarios a suscribir con los funcionarios en lo que corresponda a los equipos y la información de la Entidad en los eventos de teletrabajo.

2.7.3 Uso de Internet

Lineamientos:

El uso del servicio de internet provisto por la SDDE es exclusivo para las actividades relacionadas con las funciones asignadas.

La información que se publique en redes sociales debe controlarse de tal manera que no se comprometa los principios de seguridad de la información de la Entidad.

Normas de seguridad de la información para el Uso de Internet:

i) El servicio de Internet deberá destinarse únicamente para ejecutar las actividades lícitas que apoyen y mejoren las funciones específicas del trabajo encomendado a los funcionarios y contratistas que laboran en la entidad.

ii) El acceso y uso de Internet estará controlado y sujeto a revisión por las Subdirección de Informática y Sistemas.

iii) Solo se permite el acceso a la red de internet corporativa a los equipos que están en el inventario de activos.

iv) Los permisos de navegación por Internet únicamente se asignarán a cuentas de usuario institucionales (dominio de la SDDE). Para los equipos fuera de la red de dominio y visitantes estará disponible una Zona pública mediante una solicitud vía correo electrónico o herramientas de gestión del funcionario responsable de seguridad para su respectiva aprobación. La cual podrá ser controlada en su ancho de banda para evitar degradación del servicio de red institucional.

v) Toda la información transferida por la red de la SDDE podrá ser monitoreada a través de los equipos de seguridad perimetral de la Entidad.

vi) No se permite el uso de los recursos de internet corporativo para la descarga, distribución y/o reproducción de música, videos y similares.

2.7.3.1 Redes sociales

i) El uso de servicios de mensajería instantánea solo se utilizará para actividades de la entidad y el acceso a las redes sociales estará autorizado

sólo a un grupo restringido de usuarios teniendo en cuenta su perfil y funciones.

ii) Para el manejo de los perfiles en redes sociales relacionados con la SDDE se deben utilizar contraseñas fuertes, que no permitan el acceso a las mismas por terceros ajenos a la Entidad.

iii) Los usuarios de las redes sociales de la Entidad deben verificar el ingreso al sitio oficial y este debe contar con un certificado de autenticidad y cifrado que garantice que la información se está transmitiendo en forma segura.

iv) La información clasificada como confidencial o privada no debe ser publicada en ninguna red social.

v) Los funcionarios y contratistas de la Entidad que expresen sus opiniones personales en las redes sociales, deben informar que dichas opiniones son personales y no comprometen la opinión de la SDDE.

2.7.4 Respaldo de la Información

***Lineamiento**:*

La información clasificada de la SDDE que se almacena, procesada y transmitida debe contar con la generación de copias de respaldo, periodos de retención, rotación y métodos de restauración.

Normas de Seguridad de Información para el Respaldo de Información:

i. La información de la Entidad debe contar con adecuado respaldo dependiendo de su sensibilidad y criticidad.

ii. Los medios de copias de almacenamiento se deben contar con retención de acuerdo con su criticidad, y mecanismos de protección ambiental y de control de acceso físico.

iii. Se debe contar con lineamientos de copias de seguridad incluyendo tiempo de retención de la información, tanto de base de datos, sistemas de información, herramientas tecnológicas y contar con sus correspondientes pruebas de restauración a las copias de seguridad de acuerdo con el procedimiento GT-P3 Copia de Respaldo.

iv. Los responsables de la información definirán los tiempos de retención, frecuencia y tipo de las copias de respaldo, de acuerdo con las necesidades o requerimientos del proceso.

v. La Subdirección de Informática y Sistemas garantiza los respaldos de información que reposa en los ambientes productivos de la Secretaría Distrital de Desarrollo Económico y de recuperación de desastres bajo los RTO y RPO definidos en los acuerdos contractuales.

vi. Las copias de respaldo de la información, se debe resguardar en espacios lógicos, que garantice su disponibilidad en caso de un evento adverso que afecte a toda la Entidad.

vii. Se debe realizar copias de respaldo diario completo de las bases de datos en la herramienta de backup de la Entidad.

viii. Se realiza un backup de los logs, cada 2 horas de las bases de datos clasificadas como críticas.

ix. El backup generado de las bases de datos críticas, se almacena en una unidad externa de almacenamiento debidamente cifrado.

x. Cuando un funcionario se retira de la entidad se realiza el backup de la información por parte de la Subdirección de Informática y Sistemas. Adicionalmente, se realiza la cancelación de la cuenta en el directorio activo

xi. Los funcionarios son responsables de realizar y actualizar los respaldos de la información que tiene en el equipo asignado mínimo cada 30 días.

xii. Para los cargos de la alta dirección, se realizará el backup de manera automática.

xiii. Una vez al mes se realiza la restauración del backup full de las bases de datos de producción y de los servidores definidos como críticos.

xiv. Bajo ninguna eventualidad ni solicitud se entregará copia de las bases de datos y servidores en dispositivos como discos duros externos, USB, CD, DVD. Salvo por la solicitud escrita del funcionario y/o contratista y con la aprobación del Subdirector de Informática y sistemas.

2.7.5 Dispositivos Móviles

***Lineamiento**:*

Los dispositivos móviles que manejan información confidencial deben estar controlados, para evitar que se comprometa la integridad de la información de la Entidad.

Normas de Seguridad de Información para Dispositivos Móviles

i. Los dispositivos móviles autorizados a conectarse a la red inalámbrica corporativa (WLAN) son los portátiles que hacen parte del inventario de activos o equipos propios de la alta dirección.

ii. Los dispositivos móviles autorizados para contener, administrar o manejar información privada y/o confidencial de la entidad son de propiedad de la Secretaría Distrital de Desarrollo Económico.

iii. Los portátiles están permanentemente asegurados dentro de las oficinas con una guaya que no permita su movilidad sin previa autorización.

iv. El acceso a través de dispositivos móviles[1] a la información, recursos y sistemas que se encuentren en la infraestructura de la entidad, se realizará exclusivamente a través de una VPN provista por la Entidad.

v. El funcionario al cual se le asigna el equipo móvil es responsable por su seguridad y correcta operación dentro de la red interna y en lugares públicos.

vi. Se deben tomar medidas para proteger los dispositivos móviles de propiedad de la SDDE, con el fin de evitar el hurto, acceso o divulgación no autorizada de la información, dependiendo de su nivel de clasificación.

vii. Toda la información de los dispositivos móviles debe estar almacenada en la carpeta de File Server o similares que le fue asignada al usuario por parte de la Subdirección de Informática y Sistemas.

viii. La SDDE debe contar con un inventario actualizado de dispositivos móviles utilizados para almacenar, procesar o transmitir información de la Entidad.

ix. Todo dispositivo debe contar con un software instalado y actualizado contra códigos maliciosos.

x. Todos los dispositivos móviles deben contar con mecanismos de autenticación configurados.

xi. En los dispositivos móviles desde los cuales se requiera conexión remota a los servicios e información de la SDDE, se debe revisar previamente que esté libre de infección y cumpla con los demás controles de seguridad los cuales deberán permanecer activos y actualizados.

xii. Todo equipo móvil como portátil, Tablet, disco duro externo que ingrese a las instalaciones de la Secretaría Distrital de Desarrollo Económico, se debe registrar.

[1] Computadores portátiles, smartphone, tablets, etc.

xiii. La entidad ha establecido un procedimiento para el transporte de los equipos portátiles, servidores u otro medio de transporte de información.

xiv. Al realizar la disposición final o reasignación del dispositivo a otro usuario, se deberá realizar una copia de seguridad de la información y posteriormente un borrado seguro de toda la información allí almacenada.

xv. No se deben modificar las configuraciones de seguridad de los dispositivos móviles, ni desinstalar el software provisto al momento de su entrega.

2.7.6 Escritorio y Pantalla Limpios

***Lineamiento**:*

Los escritorios y pantallas que almacenen y manejen información clasificada de la Entidad deben mantenerse limpios y seguros.

Normas de seguridad de la Información para el escritorio y pantalla limpios:

2.7.6.1 Escritorio limpio

i. Cuando el usuario no se encuentre en el puesto de trabajo, debe guardar bajo llave los documentos y medios de almacenamiento que contengan información clasificada como pública reservada e información sensible o crítica de la SDDE, asimismo destruirla de manera segura usando buenas prácticas de reciclaje, siempre y cuando no contenga información sensible.

ii. Ejecutar el procedimiento de clasificación, etiquetado y manejo de la información de forma segura y ordenada en rutas de acceso recordables.

iii. Evitar el consumo de bebidas y alimentos que puedan provocar daños a la información o a los equipos.

iv. La documentación impresa no deberá quedar expuesta en las impresoras, scanner o lugares de copiado.

2.7.6.2 Pantalla limpia

i. La pantalla del equipo no debe tener íconos diferentes a los preestablecidos por la Entidad.

ii. Los equipos de cómputo cargarán por defecto y de manera automática el fondo de pantalla corporativo, el cual no podrá ser modificado y deberá permanecer activo.

iii. Las pantallas deberán bloquearse automáticamente después de un tiempo sin actividad.

iv. En la pantalla no debe permanecer ningún icono, acceso directo o archivo, esta debe estar completamente despejada.

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

2.7.7 Gestión de Activos

***Lineamiento**:*

La información de la SDDE se clasifica en pública y privada o confidencial. El ciclo de vida de la información debe constar de las siguientes etapas: captura o generación, mejoramiento de calidad, uso, modificación, almacenamiento y preservación y, destrucción.

La SDDE garantiza los principios de seguridad de la información a lo largo de todo el ciclo de vida.

Normas de seguridad de la Información para la gestión de Activos:

2.7.7.1 Activos de Información

i. Se deben identificar, clasificar y valorar los activos de información de la SDDE de acuerdo con el procedimiento de “Activos de Información”.

ii. Se debe mantener un registro actualizado y exacto de todos los activos de información en el documento “Matriz inventario de activos de Información”, el cual debe ser actualizado al menos dos veces por año. El propietario de la información debe hacer su clasificación y actualización y a su vez debe informar a la Subdirección de Informática y Sistemas de su clasificación para que tomen las medidas para su preservación.

iii. Todos los activos de información deben tener asignado un propietario quienes deben asegurarse de revisar periódicamente las restricciones de acceso a los activos, y que estos se encuentren clasificados apropiadamente. Los funcionarios y/o contratistas de la Subdirección de Informática y Sistemas son los custodios de los activos de información. En el momento en que la información sea almacenada en un computador personal, el usuario inmediatamente será su custodio.

iv. Todos los activos de información deben tener asignado un custodio que tiene la responsabilidad de hacer efectivos los controles de seguridad que el propietario del activo haya definido.

v. Sin excepción, al término de la relación laboral o contractual en el caso de terceros, se deben devolver los activos fijos y de información a cargo de los responsables definidos.

vi. Los activos de tipo “información” deben clasificarse de acuerdo con los niveles de clasificación de la información, de acuerdo con lo establecido en la Ley 1712 del 6 de marzo de 2014 (Ley de Transparencia y del derecho de acceso a la información pública nacional).

vii. Los documentos de la SDDE que contengan información relacionada con diferentes niveles de clasificación de la información asumirán la del nivel más alto que tenga la información contenida en ellos.

viii. El oficial de Seguridad de Información o quien haga sus veces verificará que los activos de información se encuentren debidamente etiquetados de acuerdo con su clasificación.

2.7.7.2 Base de datos

i. La información de los clientes que se maneja en la plataforma tecnológica se tiene durante los 2 últimos años con corte al 01 de enero de cada año.

ii. La información correspondiente a los años anteriores deberá ser entregada al cliente mediante carta y posteriormente eliminada a excepción que exista una cláusula contractual donde se tenga la responsabilidad de custodia o almacenamiento por más tiempo.

iii. Se realizan planes de mantenimiento de la información de tal modo que las bases de datos de producción tienen un tamaño menor a 500 GB.

iv. Una vez cumplido este tiempo se deberá hacer entrega al cliente mediante acta y posteriormente eliminación dejando acta firmada.

2.7.8 Ciberseguridad

***Lineamiento**:*

- El Firewall es el único punto autorizado para conexión con redes externas de la infraestructura tecnológica. No está permitido establecer conexiones directas con redes externas.

- Los servicios de Cloud Computing que sean contratados por la SDDE deben garantizar la integridad, disponibilidad y confidencialidad de la información allí almacenada.

Normas de seguridad de la Información para la Ciberseguridad:

2.7.8.1 Firewall

i. La Secretaría Distrital de Desarrollo Económico tiene dispositivos de seguridad perimetral (Firewall) en todas las sedes donde tiene infraestructura y controla el tráfico y seguridad de la información.

ii. Al realizar cambios o actualizaciones en el firewall se debe realizar un backup en un medio externo con el fin de garantizar la integridad e inmediato retorno a un escenario funcional.

iii. En la bitácora de firewall se debe registrar todo cambio realizado en la consola de control perimetral.

iv. El intercambio de información con entidades se hace a través de una conexión VPN punto a punto cumpliendo con los requerimientos de cifrado y seguridad que exige la norma y legislación vigente.

v. Se debe establecer pruebas del firewall antes de iniciar su funcionamiento o cuando se realicen cambios en su configuración.

vi. La SDDE debe monitorear el acceso de los usuarios a la configuración del firewall para detectar intrusiones primarias en el sistema. Este monitoreo debe registrar los cambios incrementales, progresivos o indeseados en el SGSI.

vii. Para todos los equipos de escritorio de la entidad se tiene habilitado el servicio de firewall local de acuerdo con las políticas de la herramienta de antimalware.

viii. Para todo firewall nuevo que se conecte a la plataforma tecnológica se incluye en los diagramas de red, guías de hardening y configuración. La última versión liberada de firmware está aplicada.

ix. Por parte del área de seguridad de la información se realizará auditorías en los activos de criticidad de acuerdo con la programación de Auditorías.

2.7.8.2 Seguridad en la Nube

i. Se deben tener en cuenta los requerimientos de seguridad de la información con terceros que tengan acceso a la información y a los activos tecnológicos de la SDDE antes de iniciar cualquier proceso de contratación. Estos requerimientos deben tener en cuenta el nivel de clasificación y confidencialidad y el riesgo de TI.

ii. Los proyectos de Cloud Computing que se realicen deben documentar los servicios y sistemas de información que se alojarán en dicho ambiente, la descripción del modelo de servicio a implementar y contar con arquitecturas y demás documentos de soporte para su diseño, implementación y mantenimiento.

iii. El proveedor de servicios de Cloud Computing debe tener implementado un sistema de seguridad de la información que cuente con roles y responsabilidades definidos dentro del sistema. Además, debe tener un contacto oficial para la SDDE, frente a los asuntos relacionados con la seguridad de la información.

iv. El proveedor de servicios debe contar con una conexión segura para la transferencia de información entre la Entidad y el proveedor.

v. En el momento en que un servicio de Cloud Computing sea dado de baja, la SDDE debe utilizar técnicas de borrado seguro para eliminar la información allí almacenada.

vi. Se debe realizar un monitoreo a los log de transferencia de datos hacia la nube.

vii. Se debe proteger los volúmenes de su exposición a un clonado mediante snapshot.

viii. Toda la información que se envía al servicio debe contar con un respaldo en un sitio diferente del servicio de Cloud Computing.

2.7.9 Uso de Controles Criptográficos y Gestión de Llaves Criptográficas

***Lineamiento**:*
La SDDE debe tener definidos controles criptográficos para la transmisión de información clasificada.

Normas de seguridad de la Información para el Uso de Controles Criptográficos y Gestión de Llaves Criptográficas:

i. La información digital clasificada como pública reservada se debe transmitir bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad. No obstante, en caso de no poderse aplicar un mecanismo criptográfico, se deberá asignar clave compleja de apertura a los archivos digitales que contengan este tipo de información.

ii. Al retirarse un funcionario de la entidad debe entregar los mecanismos criptográficos que tenga a su cargo, los cuales se deberán revocar, deshabilitar o cambiar según sea el caso, de manera inmediata.

iii. Se debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información tanto pública clasificada como pública reservada cuente con mecanismos de cifrado de datos.

iv. Implementar mecanismos para la recuperación de información cifrada en caso de pérdida, compromiso o daño de las llaves y reemplazo de las llaves de cifrado.

v. Se deben definir mecanismos que permitan gestionar las llaves criptográficas en todo su ciclo de vida (emisión, uso, expiración, eliminación, revocación, auditoría, copias de respaldo).

vi. Asegurar que el método utilizado para el envío de la llave sea seguro, que esta solo sea conocida por el emisor y el receptor.

vii. Se debe gestionar de manera oportuna la generación de llaves criptográficas que permitan con tiempo suficiente, dependiendo la complejidad de su adquisición o del cambio a realizar en la plataforma tecnológica, reemplazar las que pronto vayan a caducar.

2.7.10 Transferencia de Información

***Lineamiento**:*
La SDDE transfiere e intercambia información con diferentes usuarios internos y externos. Este intercambio debe darse en condiciones seguras para que no se comprometa la integridad y confidencialidad de la información.

Normas de seguridad de la Información para la Transferencia de Información:

i. Se debe usar mecanismos criptográficos para garantizar la confidencialidad, integridad y disponibilidad de la información durante su transferencia, de acuerdo con su nivel de clasificación.

ii. Los propietarios de la información a transferir deben asegurar que la clasificación de ésta se encuentre actualizada teniendo en cuenta las propiedades de seguridad: confidencialidad, integridad y disponibilidad, con el fin de permitir el acceso únicamente a los autorizados.

iii. Transferir información únicamente a receptores autorizados, quienes garanticen por escrito la confidencialidad de la información que se les vaya a suministrar, por medio de acuerdos de confidencialidad.

iv. No se permite el intercambio de información por medios no autorizados.

v. Para acceder a la carpeta compartida como el file server, se debe diligenciar el formato de “permisos de acceso al File Server” a través de la mesa de ayuda de la entidad y el Subdirector de Informática y Sistemas tendrá la potestad para aprobar la solicitud.

vi. Para la entrega de información, se establecen mecanismos de protección de la información como puertos seguros, cifrado y la contraseña se entrega por otro medio.

vii. Los emisores deben verificar previamente al envío, el nombre de los destinatarios de la información clasificada como pública reservada, con el fin de reducir la posibilidad de envío de este tipo de datos, a destinatarios no deseados.

viii. Se prohíbe el envío de archivos que contengan extensiones ejecutables y otras que puedan ser utilizadas para envío de códigos maliciosos, por medio del correo electrónico corporativo.

ix. Los datos que se extraigan de las bases de datos y que correspondan a información de los usuarios a través de diferentes medios removibles debe quedar cifrada y bajo custodia en condiciones de seguridad.

x. La transferencia de la información debe ser liderada por la Subdirección de Informática y Sistemas, con la coordinación y acompañamiento de la dependencia que manifiesta la necesidad.

xi. Se deben realizar acuerdos de transferencia de información que incluyan la reserva y compromiso del cumplimiento de la normativa nacional e internacional frente al tratamiento de la información.

xii. No se debe tener conversaciones confidenciales en lugares públicos, oficinas abiertas o mediante canales de comunicación no seguros.

xiii. Antes de transferir cualquier información, se debe revisar con un software antivirus y antimalware, para garantizar que no esté comprometida con algún código malicioso.

2.7.11 Seguridad de la Información para las Relaciones con Proveedores y Terceros

***Lineamiento**:*
Los Proveedores y/o Terceros que tengas acceso a la información y los servicios tecnológicos de la SDDE deben acoger y aplicar las normas de Seguridad de Información del SGSI de la Entidad.

Normas de seguridad de la Información para la Seguridad de la Información para las Relaciones con Proveedores y Terceros:

i. Realizar acuerdos con los proveedores y contratistas que incluyan como mínimo, los siguientes requisitos de seguridad de la información.
   a. Cláusula de confidencialidad.
   b. Cláusula que defina las responsabilidades que continúan después de terminado el contrato por el tiempo acordado entre las partes.
   c. Cumplimiento de los lineamientos de seguridad de la información de la SDDE.
   d. Reporte de eventos o incidentes de seguridad de la información a través de los mecanismos definidos por la Entidad.
   e. Clasificación, etiquetado y manejo de la información dependiendo lo acordado con el proveedor o contratista.

f. Cláusula de seguimiento y revisión de los servicios prestados por los proveedores y/o contratistas para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan.
g. Todos los controles de seguridad aplicables según el alcance del contrato.

ii. Se debe controlar la documentación relacionada con los servicios, infraestructura de TI, sistemas de información y activos a los cuales tengan acceso los proveedores, teniendo en cuenta los permisos de acuerdo con las actividades a realizar.

iii. Cuando el proveedor o contratista requiera acceso a servicios de la SDDE, se debe realizar siempre una evaluación de riesgos con la participación del propietario de la información, para identificar los controles existentes y los requisitos de los controles que se deban implementar, teniendo en cuenta entre otros los siguientes aspectos:

a. El tipo de acceso requerido (físico, lógico y a qué recurso)
b. Los motivos por los cuales solicita el acceso
c. La criticidad de la información
d. Los controles empleados por el proveedor

iv. El supervisor del contrato en conjunto con el proveedor, deben realizar sobre los productos o servicios brindados, una adecuada y completa gestión de los riesgos de seguridad de la información.

v. En ningún caso se debe otorgar acceso de los proveedores a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta que se hayan implementado los controles adecuados, y firmado un contrato o acuerdo que definan las condiciones para el acceso.

vi. El acceso de los proveedores a cualquier activo de información debe ser solicitado por el supervisor, al propietario de dicho activo, y éste junto con el Subdirector de Informática y sistemas, aprobará y autorizará el acceso y uso de la información.

2.7.12 Gestión de Incidentes de Seguridad de la Información

***Lineamiento**:*

Todos los incidentes o aquellos eventos o serie de eventos que puedan afectar la Seguridad de Información y comprometan la integridad, disponibilidad y confidencialidad de la información y de los servicios informáticos de la Entidad deben tener un tratamiento adecuado en cuanto a la detección, atención, recolección y análisis de la evidencia, y definición de acciones preventivas y correctivas.

Normas de seguridad de la Información para la Gestión de Incidentes de Seguridad de Información:

i. La gestión de los incidentes de Seguridad está a cargo del responsable de seguridad, y deberá estar tratado de inicio a fin a través de un procedimiento en donde se garantice la atención, análisis y recolección de evidencia, documentación, solución y seguimiento de los mismos.

ii. Cuando se presenten incidentes o eventos de seguridad de la información se deben reportar de manera oportuna, clasificar, asignar responsable, responder y registrar las lecciones aprendidas de acuerdo con lo definido en el procedimiento “Gestión de Incidentes de Seguridad”.

iii. En los casos que sea necesario realizar recolección y preservación de la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información, esta actividad se debe llevar a cabo de acuerdo con las directrices del procedimiento “Recolección de Evidencias Digitales”.

iv. La información sobre la gestión del incidente y su respectiva investigación debe ser tratada como confidencial y su divulgación y/o distribución será responsabilidad del Subdirector de informática y sistemas.

v. Se debe cuantificar y monitorear los volúmenes, tipos y costos de los incidentes de seguridad a través de un registro de incidentes y de los indicadores del SGSI.

vi. Se debe informar de forma completa e inmediata al ColCert (Grupo de respuesta a emergencias cibernéticas de Colombia), la existencia de un potencial incidente de seguridad informática que afecte a activos de información críticos del Estado.

2.7.13 Privacidad y Confidencialidad

***Lineamiento**:*
La SDDE garantiza la confidencialidad y reserva de la información y datos personales que no estén bajo la clasificación de información pública.

Normas de seguridad de la Información para la Privacidad y Confidencialidad:

i. Se debe firmar el acuerdo de confidencialidad establecido por la Entidad, el cual implica que la información conocida por todo funcionario, contratista y/o tercero, en ninguna circunstancia debe ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con autorización del titular de esta.

ii. El tratamiento de datos personales debe estar sujeto a lo establecido en la Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, o por la que la modifique, aclare, adicione o sustituya, así como al artículo 15 de la Constitución Política de Colombia.

iii. La información que maneje la Entidad debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. El acuerdo de confidencialidad debe indicar la vigencia de este.

iv. La información sujeta a tratamiento se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad

evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

v. Se debe identificar a través de un sistema de etiquetado comprensible para los usuarios autorizados todo documento o soporte que contenga datos personales sensibles.

vi. Se debe garantizar el almacenamiento y preservación de la documentación física y digital que contenga datos objeto de tratamiento a través de procedimientos de conservación, localización y consulta por parte de usuarios autorizados, y a su vez se permita el correcto ejercicio de los derechos de los titulares.

2.7.14 Desarrollo Seguro de Software

***Lineamiento**:*
La SDDE debe garantizar que el software que se desarrolle al interior de la Entidad aplique los requisitos y estándares de seguridad y arquitectura del software tales que permitan la integridad y confidencialidad de la información.

Normas de seguridad de la Información para el Desarrollo Seguro del Software:

i. Las áreas deben solicitar formalmente, los nuevos desarrollos de software o cambios/mejoras a los sistemas de información existentes, a la Subdirección de Informática y Sistemas estableciendo las necesidades, requisitos a satisfacer, requisitos de seguridad, incluyendo puntos de control.

ii. Para el desarrollo de cualquier software, se debe prever la existencia y disponibilidad de al menos dos ambientes separados, los cuales corresponden a: desarrollo/pruebas y producción; evitando así las modificaciones no autorizadas al código fuente o acceso no autorizado a información sensibles de los ambientes de producción, cumpliendo con los lineamientos definidos por la Subdirección de Informática y Sistemas.

iii. Se debe realizar en conjunto con la Subdirección de Informática y Sistemas, un análisis de los riesgos de seguridad de la información en el análisis de requerimientos y diseño de la aplicación, de tal manera que permita definir los controles para su tratamiento.

iv. Se debe realizar pruebas de seguridad y de aceptación en un ambiente controlado con el fin de identificar brechas, las cuales deben ser resueltas antes del paso a producción, y que tendrán dentro de sus objetivos detectar entre otros: vulnerabilidades en plataforma base, problemas de seguridad en códigos fuente y objeto, validaciones de datos ingresados, puertas traseras, etc.

v. El paso de software de un ambiente a otro debe ser controlado y gestionado de acuerdo con lo definido en el procedimiento de Gestión de Cambios.

vi. En caso de ser necesario, hacer copia de la información del ambiente de producción al ambiente de pruebas, se podrá realizar únicamente si la información sensible (aquella catalogada como información pública clasificada o pública reservada, y aquella información que deba ser protegida de acuerdo con la Ley 1581 de 2012 o las demás que la modifiquen, aclaren o adicionen) se encuentra enmascarada y/o ofuscada, con el fin de evitar la pérdida de confidencialidad de esta.

2.7.15 Disponibilidad del Servicio e Información – Continuidad en el Negocio.

***Lineamiento**:*

Toda la información crítica, incluye bases de datos y sistemas de información, utilizados por las diferentes dependencias de la Secretaría Distrital de Desarrollo Económico debe contar con las copias de respaldo requeridas en caso de la ocurrencia de eventos no previstos o desastres naturales.

Normas de seguridad de la Información para la Disponibilidad del Servicio e Información:

i. La SDDE debe contar con un Plan de Continuidad de TI que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

ii. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, deben estar incorporados y definidos en el Plan de Continuidad de TI.

iii. El plan debe contar con: análisis de impacto, actividades, punto recuperación, objetivo de recuperación, contar con pruebas del plan periódicamente

iv. Se debe implementar redundancia para las instalaciones de procesamiento de información, con el fin de asegurar la continuidad de las operaciones para la Plataforma Tecnológica.

v. Realizar pruebas periódicas de restauración de la información crítica para garantizar el funcionamiento de la misionalidad de la SDDE.

vi. Todos los colaboradores y contratistas de la SDDE deben estar capacitados en sus responsabilidades y roles frente a la continuidad del negocio y los procedimientos establecidos.

vii. Realizar periódicamente un monitoreo de los riesgos de continuidad y actualizar el plan de Continuidad acorde con dichos riesgos.

viii. Los procesos o servicios que sean desarrollados por terceros deberán contar con un plan de continuidad que garantice la prestación de los servicios en caso de materializarse un riesgo, este debe ser conocido por el supervisor.

2.7.16 Auditoría

***Lineamiento**:*
El Sistema de Gestión de Seguridad de la Información se debe someter a auditorías internas periódicas que verifiquen el cumplimiento de las medidas de seguridad.

Normas de seguridad de la Información para la Auditoría:

i. Las auditorías internas al Sistema de Gestión de Seguridad de la Información (SGSI) se deben programar y llevar a cabo por personal auditor calificado, e independiente del área que se audite, de acuerdo con las directrices del documento “Perfil auditor interno o líder de seguridad de la información”.

ii. El plan de auditoría debe contemplar: plan, alcance, se debe conservar la información del proceso y estar basados en la normatividad vigente relacionada con la seguridad de la información.

iii. Los directores, subdirectores y jefes de Oficina deben suministrar los medios necesarios para el adecuado desarrollo de la auditoría interna dentro de su área, y es responsable de establecer y aplicar las acciones correctivas que se deriven de ella.

iv. Se debe evaluar la eficacia de los controles implementados para verificar el cumplimiento a los criterios de la auditoría.

v. Por parte del área de seguridad de la información se realizará auditorías en los activos de criticidad alta cada 6 meses

2.7.17 Propiedad Intelectual

***Lineamiento**:*
Todos los desarrollos de Software, productos y servicios de la Entidad deben estar protegidos bajo los principios de la Propiedad Intelectual.

Normas de seguridad de la Información para la Propiedad Intelectual:

i. Se deben establecer acuerdos que determinen con claridad la propiedad intelectual del software desarrollado y cesión de derechos según corresponda.

ii. Los productos, servicios y software desarrollado para y por la SDDE deberá contener avisos de protección de la Propiedad Intelectual y las restricciones a su reproducción parcial o total sin autorización de los autores.

iii. No está permitido que los colaboradores de las SDDE distribuyan o reproduzcan servicios, software y/o productos de propiedad Intelectual de la SDDE sin la debida autorización de la Entidad.

iv. No se permite el envío de mensajes electrónicos o de información desde las cuentas corporativas de la SDDE que vaya en contra de la protección de los derechos de autor y de la propiedad Intelectual.

2.7.18 Capacitaciones en el SGSI

***Lineamiento**:*
Todos los colaboradores, contratistas y terceros de la SDDE deben estar capacitados en el SGSI.

Normas de seguridad de la Información para la Capacitación en el SGSI:

i. Se debe contar con un plan de capacitaciones para todas las dependencias en los diferentes temas del SGSI.

ii. Se debe realizar capacitaciones periódicas a todo el personal sobre el SGSI, en caso de cambios o modificaciones a este sistema, proponer ciclos extraordinarios de capacitación para actualizar a todos los colaboradores en las nuevas condiciones del Sistema.

iii. Al ingreso de cualquier funcionario, contratista o tercero la Oficina de Talento Humano deberá capacitarlo en el SGSI y sus responsabilidades frente a la Seguridad de la Información.

iv. Periódicamente se debe analizar y verificar el conocimiento de los colaboradores sobre el Sistema, especialmente aquellos cuyas responsabilidades y tareas son críticas frente a la Seguridad de la Información.

v. Adelantar programas de concientización con el apoyo de la subdirección de informática y sistemas que propendan en el cumplimiento de los lineamientos y normas del SGSI.

vi. Al menos una vez al año se debe evaluar la efectividad de los programas de capacitación y concientización en el SGSI.

2.7.19 Gestión Documental

***Lineamiento**:*

El manejo de los archivos y documentación de la SDDE tiene en cuenta las normas establecidas por el Archivo General de la Nación, la normativa existente y las buenas prácticas internacionales en cuanto a la recepción distribución, organización, conservación, recuperación y consulta.

Normas de seguridad de la Información para la Gestión Documental:

i. La documentación debe estar organizada e indexada de acuerdo con las clasificaciones de los activos de información.

ii. La documentación debe almacenarse de forma tal que se preserve su integridad y nivel de confidencialidad.

iii. Se debe contar con el espacio físico adecuado para la conservación de los archivos físicos y digitales de la información.

iv. Todo el personal al terminar sus labores con la SDDE debe entregar la documentación debidamente identificada, clasificada, organizada y preservada.

v. El control de la documentación y los archivos de la SDDE deberá realizarse de acuerdo con lo dispuesto en el Manual de Gestión Documental de la Entidad.

2.7.20 Virtualización

Lineamiento:

Los servicios virtuales que presta la SDDE contarán con accesos seguros a internet que garanticen la disponibilidad e integridad de la información para los usuarios.

Normas de seguridad de la Información para la Virtualización:

i. La información intercambiada entre el usuario interno y externo y el servicio virtual debe encontrarse encriptada.

ii. Los datos personales que se transmitan durante la prestación del servicio virtual deben acogerse a las normas de tratamiento de datos personales del presente manual.

iii. Los sitios web de la SDDE y sus dependencias deberán contar con certificados de autenticidad y privacidad.

iv. Se deben efectuar pruebas periódicas de penetración en la prestación de los servicios virtuales de la Entidad.

v. Se debe garantizar la prestación de los servicios virtuales durante eventos imprevistos y desastres naturales como parte del plan de continuidad del Negocio.

vi. Se debe informar a los usuarios de los planes de mantenimiento aplicables al servicio y de los tiempos en los cuales no estará disponible para evitar contratiempos en su utilización.

3 GLOSARIO

i. **Clasificación de la información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. (Tomado de la Guía para la Gestión y Clasificación de Activos de Información de MinTIC).

ii. **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Tomado de la norma ISO 27000:2016).

iii. **Contraseña:** Cadena de caracteres protegidos, generalmente cifrados por computadora, que autentican a un usuario de computadora en el sistema informático. (Glosario de ISACA: https://www.isaca.org/Pages/Glossary.aspx?tid=1665&char=P).

iv. **Custodio:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (Tomado de la Guía para la Gestión y Clasificación de Activos de Información de MinTIC).

v. **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada. (Tomado de la norma ISO 27000:2016).

vi. **Dispositivo móvil:** Dispositivos que contienen información importante, sensible o crítica para el negocio, en algunos se podría instalar software, y permitir conexión a otras redes, y se pueden usar fuera de las instalaciones de la organización (Interpretado de lo que se indica en el Control 6.2.1 “Política para dispositivos Móviles” de la ISO 27002:2013).

vii. **Oficial de seguridad:** El Gestor de Seguridad de la Información de la Entidad es responsable de ejecutar los procedimientos operativos de identificación, autenticación y control de acceso y demás procedimientos de seguridad tendientes a proteger los activos de información, también es conocido como oficial de seguridad y privacidad de la información.

viii. **Integridad:** Propiedad de la información relativa a su exactitud y completitud. (Tomado de la norma ISO 27000:2016).

ix. **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Tomado de la Ley N°1712 del 6 de marzo de 2014 - Ley de Transparencia y del derecho de acceso a la información pública nacional).

x. **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014. (Tomado de la Ley N°1712 del 6 de marzo de 2014 - Ley de Transparencia y del derecho de acceso a la información pública nacional).

xi. **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso

a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley. (Tomado de la Ley N°1712 del 6 de marzo de 2014 - Ley de Transparencia y del derecho de acceso a la información pública nacional).

xii. **Integridad:** Propiedad de la información relativa a su exactitud y completitud. (Tomado de la norma ISO 27000:2016).

xiii. **ISO:** International Organization for Standardization (Organización Internacional de Estandarización.

xiv. **Líder de Seguridad:** El Líder de Seguridad de la Información de la Entidad es responsable del diseño, desarrollo, implantación, mantenimiento y verificación del correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en línea con el Modelo de Seguridad y Privacidad de la Información y bajo las directrices del Comité Institucional de Gestión y Desempeño. También es conocido como el CISO (Chief Information Security Officer).

xv. **Malware:** El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías. (Tomado de Symantec: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad)

xvi. **Política:** Intenciones y dirección de una organización, tal como lo expresó formalmente su alta dirección. (Tomado de la norma ISO 27000:2016)

xvii. **Propietario de la Información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar

periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. (Tomado de la Guía para la Gestión y Clasificación de Activos de Información de MinTIC).

xviii. **SGSI**: Sistema de Gestión de Seguridad de la Información.

xix. **Teletrabajo**: El teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual". (Tomado de la norma ISO 27002:2013).

xx. **TIC:** Tecnologías de la Información y las Comunicaciones.

xxi. **Usuario:** Persona que utiliza un sistema informático.

xxii. **Vulnerabilidad:** Debilidad de un activo o de control, que puede ser explotada por una o más amenazas. (Tomado de la norma ISO 27000:2016).

3.1 PROCESOS Y PROCEDIMIENTOS

Se relacionan a continuación el proceso y procedimientos que hacen parte del SGSI, así:

PROCESO	GESTIÓN DE TIC
PROCEDIMIENTOS	Gestión Cuentas Usuario
	Activos de Información
	Acceso Monitoreo Uso Medios de Información
	Gestión de Medios removibles
	Trabajo en áreas seguras
	Copia Respaldo