POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Secretaría Distrital de Desarrollo Económico

2023

TABLA DE CONTENIDO

INTRODUCCIÓN

La implementación del modelo de seguridad y privacidad de la información-MSPI, busca desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de la secretaria con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de datos.

Por tal motivo, la Secretaria de Desarrollo Económico consciente de cumplir la normatividad que le aplica a las entidades del Estado Colombiano, define los lineamientos de la política de Seguridad y privacidad de la Información, y a través de la Subdirección de Informática y Sistemas se liderará su planeación, implementación, capacitación y ejecución, con el fin de mitigar los riesgos asociados a los activos de información, propendiendo así por su buen uso y privacidad

Este documento se estructura teniendo en cuenta la guía técnica colombiana ISO 27001, los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC desde el Modelo de Seguridad y Privacidad de la Información – MSPI. y la política de seguridad digital del Modelo Integrado de Planeación y Gestión - MIPG.

1. OBJETIVO GENERAL

Establecer lineamientos y directrices que propendan por la seguridad de los activos de información, con el fin de preservar la confidencialidad, integridad y disponibilidad de estos, durante todo el ciclo de vida de la información.

2. OBJETIVOS ESPECÍFICOS

Orientar la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad.

- Crear una cultura de apropiación de la seguridad y privacidad de la información en la Secretaría Distrital de Desarrollo Económico.
- Gestionar los riesgos de seguridad de la información a fin de mitigar los impactos negativos ante una eventual materialización.
- Proteger los activos de información de la Secretaría Distrital de Desarrollo Económico.

3. ALCANCE Y APLICABILIDAD

Esta política es transversal a todos los procesos y procedimientos institucionales de la Secretaría Distrital de Desarrollo Económico (en adelante SDDE).

Aplica a todos los usuarios internos y externos de la Secretaría de Desarrollo Económico (servidores públicos, funcionarios vinculados a la planta permanente y provisional, contratistas, consultores, pasantes, proveedores de bienes, entidades del Estado, entes de control) y otros terceros que desempeñen alguna actividad en las instalaciones de la Secretaría Distrital de Desarrollo Económico o a nombre de esta.

4. GLOSARIO DE TÉRMINOS

- **Activo de información:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2018]
- **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Contratista**: Persona natural o jurídica contratada por la SDDE para la adquisición de una obra, bien o servicio, no perteneciente al régimen laboral.
- **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Copias de Seguridad:** Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla y disponerla en caso de que ocurra un fallo que afecte a esta
- **Dato personal:** hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Es un activo de valor que hace parte de la SDDE, por la cual asume funciones como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato corporativo (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado.
- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.
- **Modelo Integrado de Planeación y Gestión- MIPG:** el Sistema de Gestión que deben aplicar las entidades públicas de la Rama ejecutiva, el cual integra y articula los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad con el Sistema de Control Interno.
- **Plan de continuidad del negocio:** plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Política de Seguridad de la Información**: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene el conjunto de lineamientos y procedimientos que deben ser implementados para gestionar la seguridad de la información.
- **Seguridad informática:** conjunto de medidas técnicas que son implementadas para asegurar los recursos e información contenida en los componentes tecnológicos institucionales.
- **Seguridad de la información:** conjunto de medidas que buscan la protección de la información física, electrónica, digital del acceso, uso, divulgación o destrucción no autorizada.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

5. MARCO NORMATIVO

La Secretaría Distrital de Desarrollo Económico por ser una entidad pública de la rama ejecutiva del nivel territorial, debe cumplir con la regulación y la normativa que establece el Estado Colombiano en materia de:

- Ley 1273 del 05 de enero de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado: de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
- Ley Estatutaria 1581 del 17 octubre de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”
- NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- Ley 1712 del 06 de marzo de 2014, “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Ley 1915 del 12 de julio de 2018, “Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”.
- Decreto 1074 del 26 de mayo de 2015. “Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo”. Reglamenta parcialmente

la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- Decreto 1078 del 26 de mayo de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones “
- Decreto 1083 del 26 de mayo de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, (“11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital)
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano.
- Decreto 612 de 4 de abril de 2018. “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.”
- Decreto 1008 del 14 de junio de 2018. “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. “
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP
- Resolución 004 del 28 de noviembre de 2017 "Por la cual se modifica la Resolución 305 de 2008 de la Comisión Distrital de Sistemas"
- CONPES 3995 del 1 de julio de 2020. Política Nacional de Confianza y Seguridad Digital.
- Resolución 1519 de 2020: “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
- Resolución 500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Decreto 454 del 21 de marzo de 2020. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la política de gestión de la información estadística a las políticas de gestión y desempeño institucional.
- Directiva Presidencia 03 de 15 de marzo de 2021: Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.
- Decreto 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del

Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones'"

6. ROLES Y RESPONSABILIDADES

A continuación, se determinan los roles y responsabilidades dentro del MSPI, con el fin de implementar la política de Seguridad y privacidad de la Información.

Otras responsabilidades y funciones que no se hacen referencia puntual en materia de seguridad y privacidad de la información, deberán consultarse en el manual de funciones de la entidad.

6.1. Alta dirección

Asignar y aprobar los recursos humanos y económicos para la implementación de la Política de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información.

6.2. Comité Institucional de gestión y desempeño

Es la instancia encargada de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con el Modelo Integrado de Planeación y Gestión - MIPG

6.3. 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 se 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.

- 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.
- Implementar y gestionar los controles de seguridad sobre los activos de información tecnológicos de la entidad
- Coordinar las acciones junto con el Oficial de seguridad o quien haga sus veces, para garantizar la seguridad y privacidad de los activos de información de la entidad.

6.4. 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.

6.5. Líder de procesos y su información

Los responsables de la Información en la entidad deben realizar su valoración, 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 relacionados con seguridad.
- 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.

6.6. Oficial de seguridad de la Información o quien haga sus veces en la entidad.

El Oficial de Seguridad de la Información es responsable de las siguientes actividades:

- Estructurar, orientar, liderar la implementación de la Política de Seguridad y Privacidad de la Información.
- Acompañar a las dependencias y/o procesos en la identificación y gestión de los riesgos de seguridad de la información, realizando la revisión, análisis y consolidación de la información.
- Prestar asistencia técnica en el análisis de resultados obtenidos y registrar los resultados de los análisis de vulnerabilidades y el reporte realizado en la base de conocimiento.
- Definir e implementar en coordinación con las dependencias de la entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.
- Establecer indicadores de gestión de calidad relacionados con seguridad de la Información.
- Atender los incidentes de Seguridad de la Información y ejecutar actividades de seguimiento.
- Asesorar en materia de Seguridad de la Información a la entidad.

6.7. Funcionarios y contratistas

Como usuarios que acceden a los sistemas de información y servicios tecnológicos institucionales para el cumplimiento de sus funciones y obligaciones tienen la responsabilidad de cumplir y aplicar la política de seguridad y privacidad de la información establecida.

7. PRINCIPIOS DE LA POLÍTICA

La política de seguridad y privacidad de la información de la Secretaría Distrital de Desarrollo Económico se rige por los siguientes principios, a fin de proteger los Activos de Información de cualquier pérdida de Confidencialidad, Integridad y/o Disponibilidad de forma accidental y/o intencionada:

1. La SDDE, asegurará la protección de la información generada, procesada y/o resguardada por los procesos de negocio y su infraestructura tecnológica, buscando mantener la Disponibilidad, Integridad y Confidencialidad de esta.

2. La responsabilidad de la seguridad de la información es de todos y debe ser parte integral del ciclo de vida de la información.
3. La SDDE, protegerá la información por medio de la identificación de los Activos de Información y la gestión de riesgos de Seguridad de la Información a través de controles se seguridad.

8. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La SDDE, entendiendo la importancia sobre la gestión de la información, se compromete con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer confianza en el ejercicio de sus funciones y la prestación de trámites y servicios con sus grupos de interés. Lo anterior enmarcado en el cumplimiento de la normatividad vigente y alineado con la misión y visión institucional.

Por tal motivo, adopta su Política de Seguridad y Privacidad de la Información con el fin de velar por la protección, confidencialidad, integridad y disponibilidad de los activos de información (procesos, hardware, software, infraestructura, información, funcionarios, contratistas, terceros) que soportan los procesos de la entidad, mediante la implementación de lineamientos, procedimientos y la asignación de responsabilidades, los cuales están orientados a mitigar los riesgos y prevenir incidentes de seguridad dentro de un proceso de mejora continua.

9. LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La presente política se desarrolla en 12 dominios para el cumplimiento de los objetivos planteados, los cuales se describen a continuación:

9.1. Gestión de activos

- La SDDE mediante un trabajo articulado de la Subdirección de Informática y Sistemas, a través del Oficial de Seguridad o quien haga sus veces, y los procesos institucionales, brindará herramientas y metodologías para la identificación, clasificación y etiquetado de los activos de información de la entidad.
- La SDDE debe mantener actualizado el inventario de los activos de información.
- La Subdirección de Informática y Sistemas, a través del Oficial de Seguridad o quien haga sus veces definirá los lineamientos, estándares y/o procedimientos para la gestión de activos de información.

- La Dirección de Gestión Corporativa en conjunto con la Subdirección de Informática y Sistemas deberán establecer procedimientos para la movilización, adquisición y baja (de manera técnica) de los equipos cómputo e infraestructura tecnológica de la entidad.
- Los servidores (funcionarios y contratistas) no deben divulgar, extraer, modificar y/o destruir información almacenada en los medios accesibles sin que medie autorización del dueño de la información.
- Ningún funcionario, contratista o proveedor está autorizado para realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto constituye una fuga de información, por tanto, los puertos USB permanecerán bloqueados.
- Todos los servidores (funcionarios y contratistas) que se desvinculen temporal o definitivamente de la entidad deberán realizar la devolución de activos de información que tenga asignados y en custodia, físico o virtual, al supervisor o jefe inmediato.
- La SDDE se reserva el derecho de monitorear el acceso y uso de los recursos electrónicos asignados a los funcionarios o contratistas de la entidad. La Subdirección de Informática y Sistemas es el área encargada de hacer las modificaciones o actualizaciones en los elementos y recursos tecnológicos.
- La información que reposa en los discos duros de los dispositivos móviles asignados por la Entidad (Directivos) es responsabilidad de quien tiene en uso el dispositivo móvil. Cuando se entreguen estos dispositivos, la dependencia encargada deberá garantizar que esta información permanezca en los directorios electrónicos del SGDA y eliminar los datos contenidos en el dispositivo móvil.

9.2. Control de acceso

- Las contraseñas serán de uso personal e intransferible, por tal motivo se deben implementar mecanismos para ser cambiadas periódicamente y cumplir con las condiciones de complejidad que defina la Subdirección de Informática y Sistemas.
- La Subdirección de Informática y Sistemas restringirá las cuentas de usuario con acceso privilegiado a las plataformas tecnológicas, para ser accedidas solo por el personal autorizado y no deberán ser utilizadas para tareas rutinarias o periódicas del sistema o aplicación.
- La creación, desactivación o activación de usuarios de la red, sistemas de información y repositorios de información de la entidad; al igual que los roles y permisos otorgados, los realizará la Subdirección de Informática y Sistemas a través del procedimiento establecido para tal fin.
- Todos los equipos de cómputo de propiedad de la SDDE deben estar registrados ante el Directorio Activo y protegidos con contraseña mediante el usuario de red brindado por la Subdirección de Informática y Sistemas.
- La Subdirección de Informática y Sistemas gestionará mecanismos de control de acceso a través de usuario y contraseña, a la red de la entidad, correo electrónico y a los sistemas de información que administre y definirá la política de control de acceso a estos.

- La Subdirección de Informática y Sistemas debe mantener actualizados los sistemas de directorio activo y monitoreará la asignación de permisos y roles otorgados a los usuarios.
- Es responsabilidad del funcionario y contratista el uso dado a su usuario y contraseña.

9.3. Cifrado de datos

- La SDDE, dispondrá de herramientas que permitan el cifrado de la información para proteger su confidencialidad, integridad y Disponibilidad. El cifrado de la información se realizará de acuerdo con la clasificación de privacidad y riesgo definido para la información.

- La SDDE, deberá identificar, definir e implementar los controles criptográficos que se consideren para proteger la confidencialidad, autenticidad e integridad de la información institucional.

- La SDDE utilizará sistemas y técnicas criptográficas para:

  ✓ La protección de claves de acceso a sistemas, bases de datos y servicios.
  ✓ La transmisión de Información Confidencial fuera del ámbito de SDDE
  ✓ El resguardo de información, cuando así lo recomiende la evaluación de riesgos realizada por el propietario de la información y el oficial de Seguridad de la Información.

9.4. Seguridad Física y del entorno

- La SDDE velará por prevenir el acceso físico no autorizado, el daño y la interferencia de la información en la infraestructura de procesamiento de esta.
- La SDDE velará por la aplicación de controles que permitan la protección contra desastres naturales, ataques maliciosos y accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.
- Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones físicas de la SDDE deben estar debidamente identificados con su carné, documento y/o distintivo que acredite su tipo de vinculación; en casó de carné debe portarse en un lugar visible.
- La SDDE, debe asegurar todas sus áreas físicas acorde con el valor de la información que allí sea procesada, almacenada y transmitida. Los sitios restringidos como cuartos técnicos, centro de datos y/o cualquier otro lugar donde se procese información deberán tener controles de acceso.

- Todos los funcionarios y contratistas de la SDDE son responsables de bloquear la sesión de su equipo de cómputo en el momento de dejarlo desatendido.
- Cuando un funcionario o contratista de la entidad tenga bajo su custodia un documento físico clasificado como Información Confidencial, deberá mantenerlo bajo llave cuando su puesto de trabajo se encuentre desatendido.
- El acceso por parte de personal externo a áreas restringidas de la entidad debe ser autorizado con el acompañamiento de un funcionario de la SDDE, cuando se requiera.

9.5. Seguridad de las operaciones

La SDDE a través de la Subdirección de Informática y sistemas velará por:

- Documentar, poner a disposición y aplicar los procedimientos de operación de los servicios e infraestructura tecnológica.
- Disponer de procedimientos de control de cambios en la infraestructura y sistemas de procesamiento de información que permitan que los cambios en ambiente de producción sean controlados y autorizados.
- Disponer de ambientes separados de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.
- Hacer monitoreo al uso de los recursos, ajustes y proyecciones de los requisitos sobre la capacidad de gestión tecnológica futura.
- Asegurarse de que la información y la infraestructura de procesamiento de información estén protegidas contra códigos maliciosos.
- Implementar controles de detección, prevención y recuperación ante incidentes de seguridad, combinados con estrategias de sensibilización y toma de conciencia sobre la seguridad de la información.
- Hacer copias de seguridad de la información, de los sistemas de información, bases de datos, repositorios de información y configuraciones de la infraestructura tecnológica y ponerlas a prueba regularmente de acuerdo con una política o procedimiento de copias de seguridad documentada y aprobada.
- Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Implementar procedimientos para controlar la instalación de software en sistemas operativos.
- Promover una política de escritorio limpio a fin de reducir los riesgos de acceso no autorizado, pérdida, daño o divulgación no autorizada de información durante todo su ciclo de vida, y frente a los recursos físicos y digitales de uso de los funcionarios de la Entidad.
- En el evento que alguna dependencia opere una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales de la

SDDE, se deberá cumplir con lo establecido en la presente Política y los procedimientos dispuestos por el Oficial de Seguridad y de la Información o quien haga sus veces, para tal fin.

- Obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
- Implementar controles de detección y monitoreo periódicos en busca de virus informáticos.

9.6. Seguridad de las comunicaciones

- La Subdirección de Informática y Sistemas, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes de comunicaciones y de los servicios tecnológicos que dependen de ella; así mismo, dispondrá de los mecanismos necesarios de monitoreos de seguridad para proteger la integridad, disponibilidad y confidencialidad de la información.

- Cuando se establezcan acuerdos de intercambio de información e interoperabilidad que requieren el desarrollo de servicio web (web service) o de cualquier otro mecanismo tecnológico, el intercambio deberá realizarse con controles de cifrado y será coordinado por la Subdirección de Informática y Sistemas con los mecanismos establecidos para tal fin.

- Las cuentas de correo electrónico institucional de los funcionarios y contratistas de la SDDE son personales y de uso exclusivo para el desarrollo de sus funciones. Por lo tanto, la información gestionada a través de este medio es propiedad de la entidad y cada usuario como responsable de su buzón debe cumplir con las condiciones de seguridad definidas.
- Los funcionarios y contratistas no deben utilizar el correo electrónico para el envío de cadenas de correo, mensajes con contenido religioso, político, racista, pornográfico o cualquier tipo de mensaje que atente contra la integridad de las personas, las leyes y la moral. Adicionalmente, el correo electrónico no debe ser utilizado para actividades que comprometan el buen nombre, los Activos de Información o los recursos de la SDDE.
- La conexión a las redes de la entidad será para acceder a los sistemas, aplicaciones y realizar actividades propias del cargo.
- Las redes inalámbricas de la SDDE deben contar con métodos de autenticación robustos, y cifrado de la información para prevenir incidentes de seguridad.
- La SDDE debe mantener segmentos de red independientes para los servidores, parte administrativa y visitantes.

9.7. Adquisición, desarrollo y mantenimiento de sistemas de información

- La Subdirección de Informática y Sistemas velará porque el desarrollo de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información, para lo cual deberá establecer lineamientos y arquitecturas de referencia de seguridad de la información que orienten los desarrollos.
- La SDDE, debe garantizar ambientes seguros de desarrollo, pruebas y producción.
- Todo sistema de información o desarrollo de software debe poseer un plan de pruebas de calidad que incluya pruebas de seguridad.
- La SDDE, debe mantener actualizada la documentación de los desarrollos de software realizados y estándares que aplican en su desarrollo.
- La SDDE, debe establecer un plan para el análisis y tratamiento de vulnerabilidades en los sistemas de información.
- La SDDE debe establecer como obligación específica contractual la entrega de la documentación de arquitectura y la necesaria para la administración y funcionamiento de los sistemas o aplicativos.

9.8. Relación con proveedores

- La SDDE establecerá, las disposiciones necesarias para asegurar que la información que se genere custodie, procese, comparta, utilice, recolecte, intercambie o que se tenga acceso con ocasión de establecimiento de contratos, se utilice dentro del marco de la seguridad y privacidad de la información por parte de los proveedores. En el mismo sentido y a través del seguimiento a la ejecución, los supervisores velarán por la aplicabilidad de las Políticas y procedimientos de seguridad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores.
- La SDDE, debe establecer y documentar los requisitos de seguridad de la información con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la entidad.
- Realizar seguimiento, revisar e inspeccionar con regularidad la prestación de servicios de los proveedores y los acuerdos de nivel de servicio.

9.9. Gestión de Incidentes de seguridad de la información

- La SDDE, debe establecer las responsabilidades, procedimientos de gestión y acuerdos de nivel de servicio para una respuesta rápida, eficaz y ordenada de los incidentes de seguridad de la información.
- Todos los funcionarios y contratistas deben reportar los incidentes de seguridad de la información a la Subdirección de Informática y Sistemas de manera inmediata cuando se tenga conocimiento de este o sospechen de alguno mediante los mecanismos establecidos para tal fin.
- La SDDE, debe definir y aplicar procedimientos para preservar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información con el fin de ser usado en la reducción de la posibilidad o el impacto de incidentes futuros.
- La SDDE, debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información de los incidentes de seguridad de la información que pueda servir como evidencia.
- Cuando en un incidente de seguridad, estén involucrados funcionarios y contratistas se le respetará el debido proceso. Los incidentes que involucren acciones legales o disciplinarias serán remitidos a la instancia que corresponda.

9.10. Continuidad de seguridad de la información

- La SDDE, debe determinar los aspectos de la continuidad de la gestión de la seguridad, para todos sus activos críticos de información (sistemas de información e infraestructura asociada) que le permita preservar la información y servicios tecnológicos en caso de una interrupción no deseada o un desastre.

9.11. Protección de datos personales

- La SDDE, deberá disponer de una política de Protección de datos personales, así como de un oficial de protección de datos personales o quien haga sus veces, de acuerdo con los términos de la Ley 1581 de 2012 y sus decretos reglamentarios.
- Realizar el registro nacional de bases de datos ante el ente correspondiente.
- El acceso a los datos contenidos en los sistemas de información de la SDDE debe ser a través de la creación de usuarios con roles o perfiles de usuario, de tal manera que se tenga el acceso únicamente a los datos personales requeridos para el cumplimiento de las funciones asignadas al usuario.

9.12. Cumplimiento

La Secretaria Distrital de Desarrollo Económico debe:

- Propender por la identificación, documentación y cumplimiento de las obligaciones legales y demás normatividad vigente relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
- Implementar procedimientos que permitan dar cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
- Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación en materia.
- Realizar revisión del SGSI, con el fin de identificar su adecuada implementación y operación conforme a las políticas definidas.
- La SDDE, deberá incluir para sus funcionarios y contratistas, una cláusula de confidencialidad y privacidad, de acuerdo con los requerimientos de Ley.

10. VIGENCIA

La Política de Seguridad y Privacidad de la Información, de la SDDE, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran.

La Política ha sido aprobada mediante acta número 004 del 6 de febrero de 2023 en el Comité Institucional de Gestión y Desempeño de la Secretaria Distrital de Desarrollo Económico.

CAMBIOS EN EL DOCUMENTO	RESPONSABLE	FECHA	VERSIÓN
Creación del Documento	Subdirector de Informática y Sistemas	06-02-2023	1

No.	ELABORÓ	REVISÓ	APROBÓ
1	Claudia Milena Rodríguez Álvarez. Contratista - SIS	Diego Alonso Arias Murcia Subdirector de Informática y Sistemas	CIGD – febrero de 2023