ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO

PLAN GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá Distrito Capital
SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO

Enero de 2020

TABLA DE CONTENIDO

INTRODUCCION

El Plan de Seguridad y privacidad de la Información bajo los lineamientos de la norma ISO 27001 y la metodología MSPI de MINTIC, se encuentra enfocada en proteger y controlar los datos de posibles amenazas que ponen en riesgo la confidencialidad la integridad y disponibilidad de la información en la Secretaria Distrital de Desarrollo Económico.

En este sentido, se hace necesario activar medidas propias para preservar y resguardar la información bajo los tres pilares fundamentales, cumpliendo de forma correcta los criterios de eficiencia y eficacia.

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

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

1. OBJETIVO

El objetivo del presente documento es el de presentar y mantener las estrategias que conducen a la protección de la información asegurando los principios de confidencialidad, integridad y disponibilidad de la información en la Secretaria Distrital de Desarrollo Económico mediante un monitorio continuo y preciso y enmarcado en el ciclo de mejora continua PHVA.

2. ALCANCE

Fortalecer el subsistema de Seguridad de la Información del Sistema de Gestión de Seguridad de la Información – SGSI, en la Secretaria Distrital de Desarrollo Económico.

3. MARCO LEGAL

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Ley	1273	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".	2009	X		
Decreto	235, Art.1-4	Por el cual se regula el intercambio de información entre Entidades para el cumplimiento de funciones pública	2010	X		
Ley	1581	Por el cual se dictan disposiciones generales para la protección de datos personales.	2012	X		
Decreto	1377	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.	2013	X		
Ley	1712	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.	2014	X		
Decreto	2573	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones	2014	X		
Decreto	1074	Por el cual Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.	2015	X		

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Decreto	415	Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.	2016	X		
DECRETO	1008	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones	2018	X		
LEY	1928	"por medio de la cual se aprueba el «convenio sobre la ciberdellncuencia», adoptado el 23 de noviembre de 2001, en Budapest.	2018	X		

4. DOCUMENTOS DE REFENCIA

Tipo Documento	Descripción del documento
Modelo de Seguridad y Privacidad de la Información	Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información del El Ministerio de Tecnologías de la Información y las Comunicaciones
Conpes 3854	Lineamientos de seguridad digital del Consejo Nacional de Política Económica y Social República de Colombia, Departamento Nacional de Planeación

Tipo Documento	Descripción del documento
Norma Técnica Internacioal ISO 27001, 27002, 27005	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información.

5. TERMINOS Y DEFINICIONES

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

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, transforme o controlo en su calidad de tal.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

***Gestión de incidentes de seguridad de la información*:** procesos para detectar, reportar, evaluar, responder y tratar los incidentes de seguridad de la información. (ISO 27000)

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

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

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

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

Ley de Transparencia: se refiere a la Ley Estatutaria 1712 de 2014.

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

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

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

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

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

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

Plan de tratamiento de Riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la Información inaceptables e implantar los controles necesarios para proteger los datos.

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

Privacidad: Es el derecho que se tienen relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

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

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

***Riesgo*:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

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

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

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

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

***Seguridad de la Información*:** Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO 27000)

***Sistema de gestión de la seguridad de la información - SGSI*:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

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

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

***TI*:** se refiere a tecnologías de la información

***TIC*:** se refiere a tecnologías de la información y comunicaciones

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

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

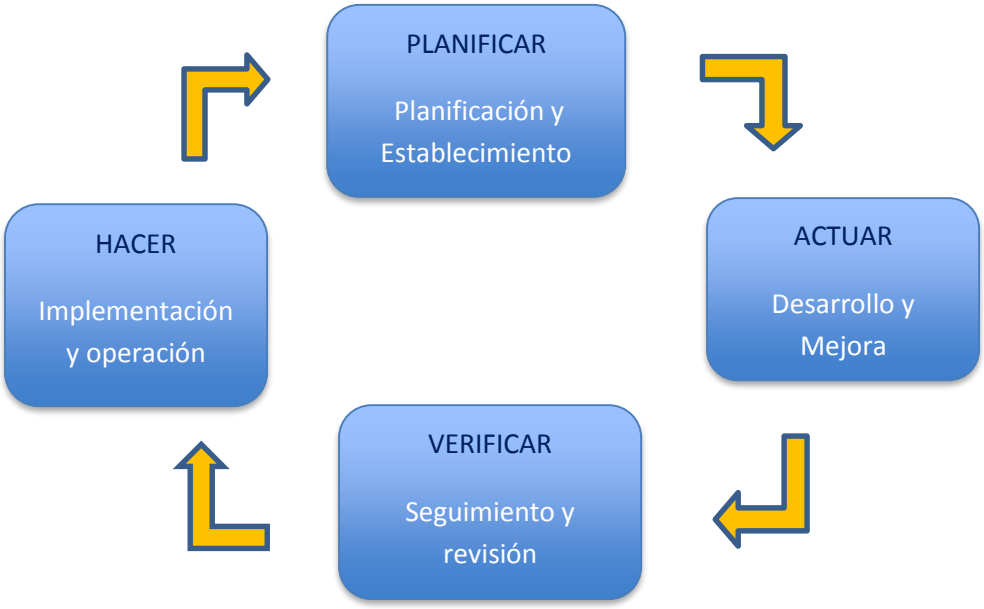
***Valoración del riesgo*:** proceso global de análisis y evaluación del riesgo.

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

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

6. CICLO – PHVA

El ciclo PHVA presenta el conjunto de actividades principales que deben llevar a cabo dentro de la Gestión de Seguridad de la Información, en un ciclo de mejora continua PHVA, bajo el cual se concentran varias gestiones que alineadas complementan el objetivo de Seguridad de la Información y que satisfacen las necesidades de la Entidad.



7. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION

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

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

8. RESPONSABILIDADES Y COMPROMISOS EN SEGURIDAD DE LA INFORMACIÓN EN LA SDDE

- Asegurar que los funcionarios, contratistas y demás colaboradores de la entidad, entiendan sus responsabilidades, funciones y roles, con el fin de reducir y/o mitigar riesgos relacionados con hurto, fraude, filtraciones, uso inadecuado de la información y de las instalaciones.
- El Comité de Gestión de Seguridad de la Información debe asumir el rol y la responsabilidad de su cargo, y debe existir un documento firmado y autorizado con roles y responsabilidades como gestores. así como asignar el rol de Oficial de seguridad de la información y su equipo de apoyo, junto con las funciones y responsabilidades respectivamente.
- El proceso de Gestión TIC debe establecer roles, funciones y responsabilidades de operación y administración de los sistemas de información, los servicios tecnológicos e infraestructura. a los funcionarios dispuestos para esto.
- Cada aspecto mencionado deberá estar debidamente documentado y publicado.

- Los directores, subdirectores y jefes de oficina deben asegurarse 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. Al igual, todos los usuarios de los sistemas de información, servicios tecnológicos e infraestructura tecnológica, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en las políticas específicas para tal fin.

9. ESTADO DEL SGSI EN LA SDDE

La Secretaria Distrital de Desarrollo Económico es una entidad del Distrito que maneja determinados volúmenes de información, el uso de datos es el principal activo de la entidad por lo que se debe tomar medidas para prevenir posibles riesgos de alteración, pérdida o robo de la información.

Actualmente la SDDE, no cuenta con un área propia en el desarrollo de temas de seguridad de la información, ni tampoco tiene subcontrato con una empresa externa para realizar tareas en torno a este tema tan importante.

La manera de trabajar el tema de seguridad de la información se enfoca y direcciona en la Subdirección de informática y sistemas que es el área responsable en supervisar los temas de seguridad de la información, pero no como una tarea principal sino como complemento del buen funcionamiento de los objetivos de la entidad. Por lo tanto, el equipo de la subdirección de Informática y sistemas está trabajando para implementar el SGSI en la SDDE.

PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION						
ACTIVIDAD	TAREA	AREAS INVOLUCRADAS	FECHA		ENTREGABLE	HERRAMIENTA DE CONSULTA
			INICIO	FIN		
Inventario de Activos de información	Actualización para la identificación, clasificación del activo de información validado por el comité de Seguridad de la Información y aprobado por la alta dirección. Actualización de la Matriz de clasificación de Activos de Información.	*Secretaria de Despacho *Oficina Asesora de Planeación *Oficina Asesora Jurídica *Oficina Asesora de Comunicaciones *Oficina de Control Interno *Subsecretaría de Desarrollo Económico y Control Disciplinario *Dirección Estudios de Desarrollo Económico *Subdirección de Información y Estadísticas *Subdirección de Estudios Estratégicos	01/02/2020	30/04/2020	Inventario activos de información actualizado	GUIA 5 - Gestión de Activos en el marco de Seguridad de la información de MINTIC

		*Dirección de Competitividad *Subdirección de Ciencia Tecnología e Innovación *Subdirección de Internacionalización *Dirección de Desarrollo Empresarial y Empleo *Subdirección de Emprendimiento y Negocios *Subdirección de Empleo y Formación *Subdirección de Financiamiento *Subdirección de Intermediación *Dirección de Economía Rural y Abastecimiento Alimentario *Subdirección Economía Rural *Subdirección de Abastecimiento Alimentario				

		*Dirección de Gestión Corporativa *Subdirección Administrativa y Financiera *Subdirección de Informática y Sistemas				
Riesgos de Seguridad de la Información	De acuerdo a la identificación del activo de información, se debe tratar el riesgo en el marco de la seguridad de la información.	*Secretaria de Despacho *Oficina Asesora de Planeación *Oficina Asesora Jurídica *Oficina Asesora de Comunicaciones *Oficina de Control Interno *Subsecretaría de Desarrollo Económico y Control Disciplinario *Dirección Estudios de Desarrollo Económico *Subdirección de Información y Estadísticas	01/05/2020	31/08/2020	Mapa de Riesgos de Seguridad de la información de la entidad.	Guía 7 - Gestión de Riesgos en el marco de Seguridad de la Información de MINTIC

		*Subdirección de Estudios Estratégicos *Dirección de Competitividad *Subdirección de Ciencia Tecnología e Innovación *Subdirección de Internacionalización *Dirección de Desarrollo Empresarial y Empleo *Subdirección de Emprendimiento y Negocios *Subdirección de Empleo y Formación *Subdirección de Financiamiento *Subdirección de Intermediación Formalización empresarial *Dirección de Economía Rural y Abastecimiento Alimentario				

		*Subdirección Economía Rural *Subdirección de Abastecimiento Alimentario *Dirección de Gestión Corporativa *Subdirección Administrativa y Financiera *Subdirección de informática y Sistemas				
Procedimiento de Gestión de riegos de Seguridad de la Información	Elaboración del procedimiento de gestión de riesgo de Seguridad de la Información.	*Subdirección de Informática y Sistemas	01/02/2020	30/04/2020	Procedimiento de Gestión de Riesgo de Seguridad de la Información publicado en la Intranet de la entidad.	Guía 3 - Procedimientos de Seguridad y Privacidad de la Información en el marco de Seguridad de la Información de MINTIC
Política de Seguridad y Privacidad de la Información	Aprobación del Manual de las Políticas de Seguridad de la información	*Subdirección de informática y Sistemas	01/02/2020	31/03/2020	-Manual de Políticas de Seguridad de la información publicado.	Guía 2 - Política General MSPI en el marco de Seguridad de la

	y socialización en la SDDE.				-Lista de asistencia	Información de MINTIC
Roles y Responsabilidades del MSPI	Elaboración del Acto Administrativo que incluya temas de Seguridad de la información de la SDDE, revisado y aprobado por el Comité de gestión y revisión de funciones de dicho comité.	*Subdirección de informática y Sistemas	01/02/2020	31/03/2020	Acto Administrativo	Guía 4 - Roles y Responsabilidades en el marco de Seguridad de la Información de MINTIC
Trato Incidentes de Seguridad y Privacidad de la Información	Elaboración del Procedimiento de Gestión de Incidentes para la SDDE	*Subdirección de informática y Sistemas	01/02/2020	30/04/2020	Procedimiento Gestión de incidentes publicado en la Intranet de la entidad.	Guía 21 - Gestión de Incidentes en el marco de Seguridad de la Información de MINTIC
Integración del Modelo de	Integración del Modelo de	*Subdirección de informática y	01/05/2020	31/12/2020	Modelo Integrado	Guía 6 - Gestión Documental en el

Seguridad de la información con el Sistema de Gestión Documental	Seguridad de la información con el Sistema de Gestión Documental	Sistemas - Gestión Documental				marco de Seguridad de la información de MINTIC
Plan de sensibilización y capacitación de SGSI	Ejecutar el plan de Capacitaciones y presentarlo a la SDDE.	*Subdirección de Informática y Sistemas	01/02/2020	31/12/2020	-Lista de asistencia -Presentación Power Point. -Gestión de comunicación (correo electrónico, circular sensibilización.	Guía 14 - Plan de comunicación, sensibilización, capacitación en el marco de Seguridad de la Información de MINTIC
transición de IPV4 a IPV6	Documentar la transición de IPV4 a IPV6	*Subdirección de Informática y Sistemas	01/02/2020	31/12/2020	Documento aprobado y publicado por el Comité de gestión	Guía 20 - transición de IPV4 a IPV6 en el marco de Seguridad de la Información de MINTIC