INFORME APROPIACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

OCTUBRE 2024

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Instituto Distrital de la participación y Acción Comunal – IDPAC – tiene como prioridad la implementación de los tres (3) pilares fundamentales de seguridad de la información, (confidencialidad, integridad y disponibilidad) , definiendo roles y responsabilidades en seguridad digital, separación de deberes, contacto con las autoridades y grupos de interés, incorporación de seguridad digital en la gestión de los proyectos, definición de controles para la mitigación del riesgo, alineado en el Modelo de Seguridad y Privacidad de la Información (MSPI).

La información es uno de los activos[1] más preciado, por tanto, el IDPAC ha tomado todas las precauciones necesarias y las integra en el plan de seguridad y privacidad de la información como objetivo para su conservación y mejorar la eficiencia y productividad en la gestión y las capacidades tecnológicas de la entidad.

El Modelo de Seguridad y Privacidad de la Información (MSPI) de acuerdo con la Política de Gobierno Digital para la sociedad y TIC para el estado y seguridad digital, liderada por el Ministerio de las Tecnologías y las Comunicaciones – MinTIC-, busca garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un servicio más participativo, más eficiente y transparente.

La planificación e implementación del MSPI, en la Entidad está determinado por las necesidades, objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura del IPDAC.

2. OBJETIVO

Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en todas las actividades que desarrolle el Instituto en su entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta Distrital en un marco de cooperación, colaboración y asistencia.

Definir las estrategias y mecanismos mediante los cuales se desarrolla e implementa la Modelo de Seguridad y Privacidad de la Información (MSPI) del Instituto Distrital de La Participación y Acción Comunal – IDPAC atendiendo el ciclo de vida de MSPI.

3. ALCANCE

El presente informe brinda un estatus de la aplicabilidad Modelo de Seguridad y Privacidad de la Información (MSPI) del IDPAC liderada por el Proceso de Tecnología de la Información en cabeza de la secretaria general, la implementación de dicha política y de acuerdo con el mapa de procesos, vigente del Instituto Distrital de La Participación y Acción Comunal está en cabeza del proceso estratégico de Comunicación estratégica y Nuevas tecnologías y del de apoyo Gestión de bienes, servicios e infraestructura.

[1] ISO/IEC 27000.

Ilustración 1Mapa de procesos del IDPAC

4. DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

La política del Instituto Distrital de la Participación y la Acción Comunal – IDPAC, está enfocada en proteger sus activos de información, los procesos, las tecnologías de información incluido el hardware y el software, con la elaboración de procedimientos, asignación de responsabilidades generales y específicas, concernientes a la gestión de seguridad de la información.

Con la política se busca contrarrestar los riesgos de perdida de la información, dando cumplimiento a los principios de seguridad de la información, realizar acciones vitales para la protección e innovación de la infraestructura tecnológica del IDPAC, elaborar instrumentos que midan la seguridad de la información salvaguardando los activos de la información con el cumplimiento de las políticas y procedimientos que garanticen la estabilidad de los recursos tecnológicos, mediante el correcto funcionamiento de la tecnología conservado la integridad de la información producida y almacenada en el IDPAC.

5. MARCO DE REFERENCIA

La normatividad descrita a continuación hace referencia a la norma vigente referenciada por el Estado colombiano y el Ministerio de Tecnologías de la Información y las comunicaciones, como autoridad en materia de seguridad de la información que hace referencia en el desarrollo de la apropiación del MSPI en la Entidad, que ha sido considerada en la elaboración de la presente informe.

NORMA	DESCRIPCIÓN
CONPES 3701 de 2011	Define los lineamientos de política ciberseguridad y ciberdefensa.
CONPES 3854 de 2017	Política Nacional de Seguridad Digital
CONPES 3920 de 2018	Política Nacional de Explotación de datos
Decreto 235, Art. 1-4 de 2010	Por el cual se regula el intercambio de información entre Entidades para el cumplimiento de funciones públicas
Decreto 2609 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". De este decreto se extracta lo relacionado con el expediente electrónico.

NORMA	DESCRIPCIÓN
Decreto 1377 de 2013	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2573 de 2014	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
Decreto 1078 de 2015	Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones
Decreto 1081 de 2015	Se expide el Decreto Reglamentario Único del Sector Presidencia de la República
Decreto 415 de 2016	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.
Decreto 1008 de 2018	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.
Directiva 2 de 2019	Simplificación de interacción digital entre los ciudadanos y el Estado.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
Ley 603 de 2000	Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales
Ley 962 de 2005	Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150 de 2007	Seguridad de la información electrónica en contratación en línea.
Ley 1273 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 1341 de 2009	Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones

Tabla 1. Marco normativo de referencia.

La implementación del Modelo de Seguridad y Privacidad de la Información con el cual se elaboró la política, dando alcance al contenido relacionado en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

6. DEFINICIONES

TÉRMINO	DEFINICIÓN
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, adquiera, transforme o controle en su calidad de tal.
Amenazas	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)
Análisis de riesgo	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
Lineamientos	Directriz o disposición establecida por el Ministerio TIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.

TÉRMINO	DEFINICIÓN
Estándar	Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización.
Arquitectura	Este habilitador busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar
Seguridad de la información	Este habilitador busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales; este habilitador tiene su soporte en el MSPI.
Innovación	En virtud de este principio el Estado y los ciudadanos deben propender por la generación de valor público a través de la introducción de soluciones novedosas que hagan uso de TIC, para resolver problemáticas o necesidades identificadas.
Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos.
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.
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.

Tabla 2. Términos y definiciones.

7. IMPLEMENTACIÓN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La política de seguridad de la información del Instituto Distrital de la Participación y la Acción Comunal – IDPAC, es aprobada por el Comité Institucional de Gestión y Desempeño, con el objeto de realizar la planificación desde el diagnóstico; con su implementación y mejora continua, se puede evaluar el desempeño, planificar la programación de recursos, metodologías y estrategias para asegurar la correcta implementación de Modelo de Seguridad y Privacidad de la Información (MSPI).

Es por esto por lo que el comité designó como responsable de la seguridad de la Información en la entidad, al proceso de Gestión de Tecnologías de la Información -GT: la implementación de la política por parte del IDPAC, se realizará a través de la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, dispuesto por el MinTIC.

7.1. Implementación

La implementación de la Modelo de Seguridad y Privacidad de la Información del IDPAC se desarrollará conforme a principios, elementos y estándares establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones que permitirán el logro de sus propósitos a partir de la adaptación de las TIC, como mejorar la relación con otras entidades públicas y fortalecer la relación con la ciudadanía en un entorno confiable y de calidad.

Para lograr la implementación del MSPI el IDPAC realizará siguiendo la metodología PHVA, el siguiente ciclo:

Ilustración 2Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

En esta fase de implementación en la norma ISO 27001:2013[2], capítulo 8 - Operación, indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

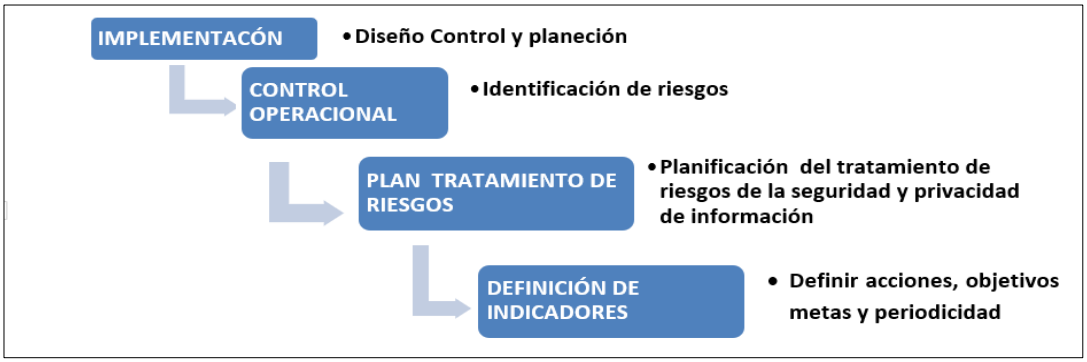

Ilustración 3Diseño de la implementación

ACTIVIDADES DE GESTIÓN	ESTRATEGIA O MECANISMO DEL IDPAC	DEPENDENCIA RESPONSABLE	PERIODICIDAD
Diseño, definición o actualización de los documentos y controles de Sistema de Gestión de Seguridad de la Información - SGSI.	MSPI	GTI	Anual
	Plan de Seguridad y Privacidad de la Información	GTI	Permanente
Diseño, definición o actualización de la gestión de	Activos de información	GTI	Anual

[2] Norma ISO 27001:2013[2], capítulo 8.

ACTIVIDADES DE GESTIÓN	ESTRATEGIA O MECANISMO DEL IDPAC	DEPENDENCIA RESPONSABLE	PERIODICIDAD
levantamiento de activos de información			
Diseño, definición o actualización de la gestión de los riegos de seguridad digital	Plan de riesgos de información del	GTI	Semestral
Seguimiento y evaluación	Seguimiento de cumplimiento	GTI	Semestral
	Revisión de políticas de Seguridad Digital y mecanismos que permitan verificar su cumplimiento.	GTI	Anual
	Revisión y aprobación de los activos y riegos de Seguridad Digital	GTI	Anual
Divulgación de SGSI.	Realizar campañas de concientización en temas de Seguridad Digital teniendo en cuenta los diferentes roles definidos dentro de la “Matriz de roles y responsabilidades” del SGSI.	GTI	Semestral

Tabla 3. Planeación reimplantación

8. HERRAMIENTAS E INSTRUMENTOS

Con el fin de dar cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013, verificando el cumplimiento de las disposiciones planificadas y comprobando que se mantienen de manera eficaz los controles, el Modelo de Seguridad y Privacidad de la Información (MSPI) implementada en IDPAC, el seguimiento y control conforme a los procesos definidos en el Mapa de Procesos del IDPAC el proceso de Gestión Tecnologías de la Información -GT, dentro del marco operativo de la política de Seguridad y Privacidad de la información se realizará con la siguiente metodología.

8.1. Metodología

La Metodología empleada para desarrollar la implementación se soporta en la verificación y análisis de documentos y/o registros físicos y virtuales, la recolección de información será a través del diligenciamiento de encuestas, aporte de evidencias de ser necesario, además se hará la revisión de las respuestas a solicitudes de información escrita y verbal, selectivas, pruebas de observación, visitas de inspección, entrevistas, mesas de trabajo con los servidores públicos y contratistas que lideran y apoyan los proceso de Gestión de Tecnología de la Información, Gestión Contractual, Oficina Asesora Jurídica, Secretaria General - Bienes y Servicios, Gestión Documental, Gestión Financiera, Oficina de Planeación, con el fin de valorar su estado y nivel de cumplimiento frente a los requisitos técnicos, de oportunidad y legales que le aplican.

8.2. Muestra

La selección de la muestra propuesta se fundamenta en el muestreo aleatorio simple revisando la información relevante del proceso y con la que se puede demostrar el cumplimiento del estado actual del IDPAC con respecto a la ISO/IEC 27001:2013

Se realizará un análisis que permita evaluar el estado de contexto de la entidad, respecto de los aspectos de: organización, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejoras, los cuales se convertirán en elementos esenciales en el proceso de mejoramiento continuo, para el IDPAC desde la pertinencia del subsistema de gestión de seguridad de la información

La Evaluación y Control se realizará a funcionarios líderes de cada proceso, está la ejecutará quien ejerza el rol de Oficial de Seguridad de la Información -OSI para el en cumplimiento del MPSI y la Política de Seguridad Privacidad de la Información, sobre el cumplimiento relacionado con los 14 dominios y 114 controles de seguridad que establece la norma ISO/IEC 27001:2013[3].

Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.

[3] norma ISO/IEC 27001:2013[3].

Descripción	Calificación	Criterio
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 4. Escala de Valoración de Controles ISO 27001:2013 ANEXO A

8.3. Ficha seguimiento implementación para el de evaluación para MSPI instrumento de identificación de la línea técnica

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD TÉCNICA				
ITEM	**DESCRIPCIÓN**	**ISO**	**MSPI**	**NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001**
CONTROL DE ACCESO		**A.9**	**Componente planificación y modelo de madurez nivel gestionado**	**100**
REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	**Se debe limitar el acceso a información y a instalaciones de procesamiento de información.**	**A.9.1**	Modelo de madurez definido	**100**
Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		100
Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		100
GESTIÓN DE ACCESO DE USUARIOS	**Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**	**A.9.2**	Modelo de madurez gestionado cuantitativamente	**100**
Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	A.9.2.1		100
Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	A.9.2.2		100
Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	A.9.2.3		100

Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	A.9.2.4		100
Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	A.9.2.5		100
Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	A.9.2.6		100
RESPONSABILIDADES DE LOS USUARIOS	**Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.**	**A.9.3**	Modelo de madurez definido	**100**
Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	A.9.3.1		100
CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	**Se debe evitar el acceso no autorizado a sistemas y aplicaciones.**	**A.9.4**	Modelo de madurez gestionado cuantitativamente	**100**
Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	A.9.4.1		100
Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	A.9.4.2		100
Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	A.9.4.3		100
Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	A.9.4.4		100
Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	A.9.4.5		100
CRIPTOGRAFÍA	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización** **Garantizar la seguridad del teletrabajo y el uso de los**	**A.10**	**Componente planificación y modelo de madurez nivel gestionado**	**80**

	dispositivos móviles			
CONTROLES CRIPTOGRÁFICOS	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**	**A.10.1**		**80**
Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	A.10.1.1	Modelo de madurez gestionado cuantitativamente	80
Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	A.10.1.2		80
SEGURIDAD FÍSICA Y DEL ENTORNO		**A.11**	**Componente planificación y modelo de madurez nivel gestionado**	97
ÁREAS SEGURAS	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**	**A.11.1**		**93**
Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	A.11.1.1	Modelo de madurez definido	100
Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	A.11.1.2		100
Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	A.11.1.3		100
Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	A.11.1.4		80
Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	A.11.1.5	Componente planeación	80

Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	A.11.1.6		100
EQUIPOS	**Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.**	**A.11.2**	Modelo de madurez definido	**100**
Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	A.11.2.1		100
Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	A.11.2.2		100
Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.	A.11.2.3		100
Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	A.11.2.4		100
Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	A.11.2.5		100
Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	A.11.2.6		100
Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	A.11.2.7		100
Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	A.11.2.8		100
Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones	A.11.2.9		100

	de procesamiento de información.			
SEGURIDAD DE LAS OPERACIONES		**A.12**	**Componente planificación y modelo de madurez nivel gestionado**	100
PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**	**A.12.1**		**100**
Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	A.12.1.1		100
Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	A.12.1.2		100
Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	A.12.1.3	Modelo de madurez definido	100
Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	A.12.1.4		100
PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	**Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.**	**A.12.2**		**100**
Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	A.12.2.1	Modelo de madurez gestionado	100
COPIAS DE RESPALDO	**Proteger contra la pérdida de datos.**	**A.12.3**		**100**
Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	A.12.3.1	Modelo de madurez gestionado	100
REGISTRO Y SEGUIMIENTO	**Registrar eventos y generar evidencia.**	**A.12.4**	Modelo de madurez gestionado cuantitativamente	**100**

Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	A.12.4.1	Modelo de madurez gestionado cuantitativamente	100
Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	A.12.4.2		100
Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	A.12.4.3		100
Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	A.12.4.4		100
CONTROL DE SOFTWARE OPERACIONAL	**Asegurar la integridad de los sistemas operacionales.**	**A.12.5**	Modelo de madurez definido	**100**
Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	A.12.5.1		100
GESTIÓN DE LA VULNERABILIDAD TÉCNICA	**Prevenir el aprovechamiento de las vulnerabilidades técnicas.**	**A.12.6**	Modelo de madurez gestionado	**100**
Gestión de las vulnerabilidades técnicas	Se debe 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.	A.12.6.1		100
Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	A.12.6.2		100
CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	**Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.**	**A.12.7**	Modelo de madurez gestionado cuantitativamente	**100**
Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	A.12.7.1		100
SEGURIDAD DE LAS COMUNICACIONES		**A.13**	**Componente planificación y modelo de madurez nivel gestionado**	100

GESTIÓN DE LA SEGURIDAD DE LAS REDES	**Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**	**A.13.1**		**100**
Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	A.13.1.1		100
Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	A.13.1.2	Modelo de madurez definido	100
Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	A.13.1.3		100
TRANSFERENCIA DE INFORMACIÓN	**Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**	**A.13.2**		**100**
Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	A.13.2.1		100
Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	A.13.2.2	Modelo de madurez definido	100
Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	A.13.2.3		100
Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	A.13.2.4		100
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		**A.14**	**Componente planificación y modelo de madurez nivel gestionado**	83
REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	**Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**	**A.14.1**	Modelo de madurez definido	**90**

Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se debe incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	A.14.1.1		100
Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2		80
Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	A.14.1.3		80
SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	**Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**	**A.14.2**	Modelo de madurez definido	**80**
Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	A.14.2.1		80
Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se debe controlar mediante el uso de procedimientos formales de control de cambios.	A.14.2.2		80
Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	A.14.2.3		80
Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	A.14.2.4		80
Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	A.14.2.5		80

Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	A.14.2.6		80
Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	A.14.2.7		80
Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	A.14.2.8	Modelo de madurez gestionado cuantitativamente	80
Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	A.14.2.9		80
DATOS DE PRUEBA	**Asegurar la protección de los datos usados para pruebas.**	**A.14.3**	Modelo de madurez definido	**80**
Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	A.14.3.1		80
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		**A.16**	**Componente planificación y modelo de madurez nivel gestionado**	91
GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	**Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**	**A.16.1**	Modelo de madurez definido	**91**
Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	A.16.1.1		80
Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible.	A.16.1.2		80
Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	A.16.1.3	Modelo de madurez definido	100

Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	A.16.1.4	Madurez Inicial	100
Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	A.16.1.5	Modelo de madurez gestionado cuantitativamente	100
Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	A.16.1.6	Modelo de madurez gestionado cuantitativamente	80
Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	A.16.1.7	Modelo de madurez gestionado Modelo de madurez definido	100

Tabla 5. Modelo de evaluación para MSPI según norma ISO/IEC 27001:2013

9. LÍDER DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Este líder será el responsable de la Seguridad y Privacidad de la Información en la Entidad, algunas de sus responsabilidades son identificar la brecha entre los requerimientos del Modelo de seguridad y privacidad de la información y la situación actual de la entidad, liderar la implementación del Modelo de Seguridad y Privacidad de la Información, liderar el equipo de trabajo que implementará y mantendrá el Modelo de Seguridad y Privacidad de la Información – MSPI, definiendo roles, responsabilidades, entregables y tiempos, representar a la Entidad en temas de Seguridad y Privacidad frente a requerimientos externos, etc.

La designación del Líder Oficial de Seguridad de la Información será realizada por la Dirección General.

Se realizará la revisión de los actuales procedimientos, con el objeto de identificar las necesidades de documentación y/o actualización de procedimientos en el marco de la implementación del Modelo de Seguridad y Privacidad de la información.

El propósito de esta actividad se fundamenta en desarrollar y formalizar procedimientos que permitan gestionar la seguridad y privacidad de la información en todos los procesos de la Entidad.

10. ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección General deberá garantizar la asignación de roles y responsabilidades en todos los niveles (directivo, de procesos, operativo), para lo cual acorde con lo establecido en el Modelo Integrado de Planeación y Gestión – MIPG se deberán designar al Comité Institucional de Gestión y Desempeño como el organismo encargado de la gestión y toma de decisiones.

También se debe conformar el equipo de trabajo que apoyará al Oficial de Seguridad y Privacidad de

la Información durante la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información – MSPI, para lo cual se debe establecer y dar a conocer el perfil y responsabilidades de los integrantes del equipo de trabajo.

El equipo de trabajo designado se encargará de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades incluidas en la adopción del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad, así mismo, estará encargado de planear las actividades necesarias para una adecuada administración y sostenibilidad del Modelo.

11. PROCESO DE GESTION DE LA TECNOLOGIA

El proceso se encuentra dentro de los procesos de apoyo para establecer lineamientos, estrategias, acciones e iniciativas en materia de tecnología de información y comunicaciones a través de la administración de la infraestructura tecnológica, sistemas de información para garantizar la disponibilidad, integridad y confidencialidad de esta y contribuir con el logro de los objetivos estratégicos del IDPAC.

Se encuentra en los procesos estratégicos donde se implementan estrategias de comunicación y nuevas tecnologías para la formulación, ejecución y diseños de acciones y el posicionamiento de la entidad mediante la aplicación de los lineamientos institucionales y distritales.

Se relaciona la gestión realizada publicada en EL Sistema Integrado de Gestión (SIGPARTICIPO):

IDPAC-CENT-FT-01 Matriz de inventario y clasificación de activos de información V4
IDPAC-CENT-FT-02 Indicé Información Clasificada Reservada v1
IDPAC-CENT-PL-01 Plan para la renovación de la infraestructura TIC
IDPAC-CENT-PL-02 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información V3
IDPAC-CENT-PL-03 Anexo 1 Catalogo de Sistemas de Información
IDPAC-CENT-PL-03 Anexo 3 Matriz Sistemas de información y datos o categorías de información
IDPAC-CENT-PL-03 Plan Estratégico Tecnologías información - PETI V2
IDPAC-GTI-PL-03 Plan de Recuperación de Desastres
IDPAC-GTI-PL-04 Plan de contingencias de tecnologías de la Información
IDPAC-CENT-PR-03 Actualización de Inventario de Activos de información V4
IDPAC-GTI-FT-06-Inventario-Bases-de-Datos
IDPAC-GTI-FT-07-Formato-Diccionario-de-Datos
IDPAC-GTI-FT-08-Solicitud-Recursos-de-Tecnologias-de-la-Informacion
IDPAC-GTI-FT-09-Solicitud-de-Desarrollo-o-Mantenimiento-de-Software
IDPAC-GTI-FT-10-Definicion-Desarrollo-y-Puesta-en-Produccion-del-Producto-de-Software
IDPAC-GTI-FT-11HojadeVidaEquipoComputo
IDPAC-GTI-FT-12AtencionEvaluacionServicioSoporteTIaUsuarios
IDPAC-GTI-FT-13InventarioConsolidadoEquiposdeComputo
IDPAC-GTI-FT-16RegistroIngresoalCentrodeComputo
IDPAC-GTI-FT-17SolicitudApoyoaJornadasdeAprendizajeconRecursosdeTI
IDPAC-GTI-GU-01 Guía Elaboración de Inventario y Clasificación de Activos de Información
IDPAC-GTI-GU-02 Guía Formato Diccionario Datos
IDPAC-GTI-GU-03 Guía de Inicio de Sesión
IDPAC-GTI-IN-01-Instructivo-Mesa-de-Ayuda-GLPI
IDPAC-GTI-MN-01 Manual de políticas de seguridad de la Información
IDPAC-GTI-OT-01 Aviso de privacidad
IDPAC-GTI-OT-02 Política de tratamiento de datos personales

IDPAC-GTI-PR-06-Administracion-Base-Datos
IDPAC-GTI-PR-17-Administracion-de-Servidores
IDPAC-GTI-PR-19-Gestion-Cuentas-de-Usuario
IDPAC-GTI-PR-20-Analisis-Adquisicion-Infraestructura-Tecnologica
IDPAC-GTI-PR-22MantenimientoCorrectivoySoporteTecnico
IDPAC-GTI-PR-24InventarioEquiposdeComputo
IDPAC-GTI-PR-25 Administración de Centros de Computo

Elaboro: José Antonio Chaparro Gómez Profesional especializado 222 – 04

Reviso: Omar Orlando Coronado Cacua – Contratista 569 Proceso de Tecnología de la Información

Firmado digitalmente por BARAJAS AGUILERA YULY MARCELA

YULY MARCELA BARAJAS AGUILERA
Secretaria General IDPAC