AÑO
2020

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MSPI

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SALUD

TABLA DE CONTENIDO

1. OBJETIVO:

Asegurar la adopción integral del Modelo se Seguridad y Privacidad de la Información (MSPI) bajo un enfoque de mejora continua.

1.1 OBJETIVOS ESPECIFICOS

- Establecer un cronograma basado en el ciclo de mejora continua para la adopción integral del Modelo de Seguridad y Privacidad de la Información.
- Establecer medidas de implementación y de verificación de los controles previstos en el Modelo de Seguridad y Privacidad de la Información con base en los riesgos identificados de seguridad de la información en la entidad.

2. ALCANCE:

El plan está previsto para el alcance del sistema de gestión de seguridad de la información de la Secretaría Distrital de Salud de Bogotá, D.C., pero podrá igualmente, proveer herramientas de control en general a la gestión segura de la información en la totalidad de los procesos de la Secretaría.

3. MARCO LEGAL

- Constitución Política. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.
- Ley 527 de 1999. “Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”
- Ley 594 de 2000. “Ley General de Archivo”
- 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 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países
- 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”. Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418. Revelación de Secreto; Art. 419. Utilización de asunto sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Ley 1437 de 2011. “Procedimiento Administrativo y aplicación de criterios de seguridad”.
- Ley 1480 de 2011. “Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas”.
- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”.
- Decreto Ley 019 de 2012. “Racionalización de trámites a través de medios electrónicos.
- Criterio de seguridad”.
- Ley 1621 de 2013. “Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones”.
- Ley 1712 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.
- Decreto 1727 de 2009. “Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia,

comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información"

- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
- Decreto 2364 de 2012. "Firma electrónica"
- Decreto 2609 de 2012. "Expediente electrónico"
- Decreto 2693 de 2012. "Gobierno electrónico"
- Decreto 1377 de 2013. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
- Decreto 1510 de 2013. "Contratación pública electrónica"
- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- Decreto 1078 de 2015, por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de Información y las Comunicaciones
- Decreto 1008 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 Tecnologías de la Información y las Comunicaciones"
- Decreto 1413 de 2017. "Por la cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2018, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 415 de 2016. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2011 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones"
- Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad digital. CONPES Bigdata

4. RESPONSABLE:

Profesional Especializado Dirección TIC

5. GLOSARIO

Activo: Todo aquello que representa valor para la organización [ISO 27000]

Activo de información: Datos y conocimiento con valor para la organización [ISO 27000]

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701).

Cláusula: Capítulos principales de la norma (ej. ISO 27001)

Conformidad: Cumplimiento de un requisito de orden técnico u organizacional

Control: Políticas, procedimientos, lineamientos, dispositivos y en general todo aquello previsto para transformar un riesgo [ISO 31000]

Cumplimiento: Cumplimiento de un requisito de orden jurídico

Dominio: Categoría de seguridad de la información según se describe en el Anexo A de la ISO 27001 [ISO 27002]

Riesgo: De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la “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 de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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

5.1 ABREVIATURAS

SI: Seguridad de la información

GDA: Gestión Documental y Archivo

ITEP: Índice de Transparencia en Entidades Públicas

MSPI: Modelo de Seguridad y Privacidad de la Información

PROC: Procedimientos documentados

RRHH: Recursos humanos

SGSI: Sistema de Gestión de Seguridad de la Información

6. GENERALIDADES

La Secretaría distrital de Salud de Bogotá, D.C., buscando desarrollar el Modelo de Seguridad y Privacidad de la Información (MSPI) ha establecido una estrategia integral de aseguramiento de la información de forma tal que su adopción se está realizando de forma integrada con el Sistema de Gestión de Seguridad de la Información, considerando que la norma ISO/IEC 27001:2013 es base de ambos sistemas y que las guías técnicas desarrolladas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, se basan en dicha norma y consideran el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia de Gobierno Digital: TIC para el Estado y TIC para la Sociedad

A nivel metodológico, se ha seguido la estructura riesgo → control, de forma tal que las actividades iniciales están orientadas a conocer los riesgos de seguridad de la información (Guía 7 - Gestión de Riesgos), y las posteriores a tratarlo (Guía 8 - Controles de Seguridad de la Información) así como a asegurar la mejora continua en el proceso de gestión del riesgo y de seguridad de la información (Guía 9 - Indicadores Gestión de Seguridad de la Información, Guía 15 – Auditoria, Guía 16 - Evaluación de Desempeño, y Guía 17 - Mejora continua).

Las demás guías, dada su naturaleza de control, una vez alineadas con el Anexo A de la norma ISO/IEC 27001:2013 son aplicadas conforme a los resultados del análisis de riesgos: Guía 2 - Política General MSPI v1, Guía 1 - Metodología de pruebas de efectividad, Guía 5 - Gestión Clasificación de Activos, Guía 6 - Gestión Documental, Guía 4 - Roles y responsabilidades, Guía 3 - Procedimiento de

Seguridad de la Información, Guía 12 - Seguridad en la Nube, Guía 21 - Gestión de Incidentes, Guía 13 - Evidencia Digital, Guía 10 - Continuidad de Negocio, Guía 11 - Análisis de Impacto de Negocio, Guía 19 - Aseguramiento de protocolo IPv4_IPv6, y Guía 20 - Transición IPv4_IPv6.

7. ACTIVIDADES

Las actividades a desarrollar en el Plan de Seguridad y Privacidad de la Información se describen a continuación:

7.1 ANÁLISIS DE VULNERABILIDADES

Proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante.

7.2 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Realizar los procedimientos de seguridad que pueden generarse durante el diseño y la implementación del modelo de seguridad y privacidad de la información.

7.3 CONTINUIDAD DE NEGOCIO

Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.

7.4 ANÁLISIS DE IMPACTO DE NEGOCIO

Generar lineamientos de seguridad ante situaciones de emergencia a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente las operaciones del negocio.

7.5 EVIDENCIA DIGITAL

Como llevar a cabo una correcta identificación, recolección, análisis y manipulación de datos en caso de algún evento o incidente de seguridad que requiera de evidencias digitales para su investigación.

7.6 GESTIÓN Y CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

8. CRONOGRAMA

ACTIVIDADES		DEFINICIÓN	2020/02	2020/03	2020/04	2020/05	2020/06	2020/07	2020/08	2020/09	2020/10	2020/11	2020/12
1	Analisis de vulnerabilidades.	Proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante.											
2	Procedimientos de Seguridad de la Información	Realizar los procedimientos de seguridad que pueden generarse durante el diseño y la implementación del modelo de seguridad y privacidad de la información											
3	Continuidad de Negocio	Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones criticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.											
4	Análisis de Impacto de Negocio	Generar lineamientos de seguridad ante situaciones de emergencia a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente las operaciones del negocio.											
5	Evidencia Digital	Como llevar a cabo una correcta identificación, recolección, análisis y manipulación de datos en caso de algún evento o incidente de seguridad que requiera de evidencias digitales para su investigación.											
6	Gestión y clasificación de Incidentes de Seguridad de la Información	Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.											

9. ANEXOS

El Modelo de Seguridad y Privacidad de la Información, el cual puede ser consultado (en su versión vigente) en línea y descargar las guías pertinentes, en la dirección: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

10. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE ACTUALIZACIÓN
1	24/07/2018	Se estructura el Plan de Seguridad y Privacidad de la Información en cumplimiento a la normatividad vigente.
2	10/01/2019	Se estructura el Plan de Seguridad y Privacidad de la Información en cumplimiento a la normatividad vigente.
3	10/01/2020	Se estructura el Plan de Seguridad y Privacidad de la Información en cumplimiento a la normatividad vigente.