AÑO
2020

PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SALUD

TABLA DE CONTENIDO

1. OBJETIVO:

Asegurar que la arquitectura de control prevista para los riesgos en seguridad de la información sea implementada, y se verifique su eficacia.

1.1 OBJETIVOS ESPECIFICOS

- Establecer un cronograma de línea base para la adopción e implementación del plan de tratamiento de riesgos y que sirva, a la vez, de mecanismo de control de eficacia en cuanto a la ejecución del plan.
- Establecer medidas de implementación y de verificación de los controles previstos para los riesgos en seguridad de la información.

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 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 Big-data
- 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.

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

Los Sistemas de Gestión de Seguridad de la Información (ISMS/SGSI) proveen un modelo con enfoque sistemático para establecer, implementar, operar, supervisar, revisar, mantener y mejorar de forma continua la protección de los activos de información de la organización, en su contexto, con el fin de alcanzar los objetivos de negocio, teniendo como base la evaluación del riesgo para efectivamente tratar y gestionar el riesgo. El análisis de requisitos para la protección de los activos y la aplicación de los controles apropiados para la protección de esos activos de información, tal como se requiere, contribuye a la implementación exitosa del MSPI.

Considerando lo anterior, y el marco normativo actual vigente en Colombia, ha llevado a la Secretaria de Salud Distrital de Bogotá, D.C., dentro de su compromiso institucional con la ciudadanía y el cumplimiento normativo, a establecer un Sistema de Gestión de Seguridad de Información complementado con lineamientos técnicos relacionados tales como el Modelo de Seguridad y Privacidad de la Información, Gestión Documental y Archivo, Gestión de la Transparencia, y la Protección Integral de los Datos Personales y el Habeas Data, tomando como base la norma técnica ISO/IEC 27001:2013.

Como primera medida la entidad ha realizado actividades de conocimiento de los riesgos en seguridad de información que le son aplicables, empleando algunas herramientas provistas por la guía para la administración del riesgo y el diseño de controles en entidades públicas, y con base en los riesgos determinados se han trazado controles alineados con el Anexo A de la norma ISO/IEC 27001:2013.

7. ACTIVIDADES

Las actividades a desarrollar en el plan de tratamiento de riesgos de Seguridad de la Información se describen a continuación:

7.1 ESTABLECER EL CONTEXTO

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Se debe establecer el contexto tanto interno como externo de la entidad, además del contexto del proceso y sus activos de seguridad digital.

7.2 IDENTIFICACIÓN DE RIESGOS

Se determinan las causas fuentes del riesgo y los eventos con base en el análisis de contexto para la entidad y del proceso, que pueden afectar el logro de los objetivos.

Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos y los institucionales.

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos.

Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

7.3 ANÁLISIS DE RIESGOS

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

7.4 EVALUACIÓN DE RIESGOS

Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

7.5 MONITOREO Y REVISIÓN

Se busca generar indicadores para medir la gestión realizada en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados.

8. CRONOGRAMA

ACTIVIDADES		DEFINICIÓN	01/2020	02/2020	03/2020	04/2020	05/2020	06/2020	07/2020	08/2020	09/2020	10/2020	11/2020	12/2020
1	Establecer el contexto.	Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC-ISO 31000). A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.												
2	Identificación de riesgos	La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos.												
3	Análisis de riesgos	Establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).												
4	Evaluación de riesgos	Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).												
5	Monitoreo y revisión	Generar indicadores para medir la gestión realizada en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados.												

9. CONTROL DE CAMBIOS

Registre en este cuadro, la versión, fecha de aprobación de la versión y los cambios generados en cada versión del documento.

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE ACTUALIZACIÓN
1	24/09/2018	Se estructura Plan de Tratamiento de Riesgos en Seguridad de la Información en cumplimiento a la normatividad vigente
2	10/01/2019	Se estructura Plan de Tratamiento de Riesgos en Seguridad de la Información en cumplimiento a la normatividad vigente.
3	10/01/2020	Se estructura Plan de Tratamiento de Riesgos en Seguridad de la Información para la vigencia 2020, en cumplimiento a la normatividad vigente.