

PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

SECRETARÍA DE SALUD

TABLA DE CONTENIDO

1. OBJETIVO:.....	1
1.1 OBJETIVOS ESPECIFICOS	1
2. ALCANCE:	1
3. RESPONSABLE:.....	4
4. GLOSARIO.....	5
4.1 ABREVIATURAS.....	5
6. DESARROLLO DEL PLAN.....	6
7. ANEXOS	¡Error! Marcador no definido.
8. CONTROL DE CAMBIOS	5

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD</p>	<p>DIRECCIÓN TIC SISTEMA INTEGRADO DE GESTIÓN CONTROL DOCUMENTAL PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN Código: SDS-TIC-PL-004 v.1</p>	<p>Elaborado por: Juan Carlos Angarita Revisado por: John Jairo Triana Aprobado por: Arleth Patricia Saurith Contreras</p>	
---	---	--	--

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.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD</p>	<p>DIRECCIÓN TIC SISTEMA INTEGRADO DE GESTIÓN CONTROL DOCUMENTAL PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN Código: SDS-TIC-PL-004 v.1</p>	<p>Elaborado por: Juan Carlos Angarita Revisado por: John Jairo Triana Aprobado por: Arleth Patricia Saurith Contreras</p>	
---	---	--	--

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.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD</p>	<p>DIRECCIÓN TIC SISTEMA INTEGRADO DE GESTIÓN CONTROL DOCUMENTAL PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN Código: SDS-TIC-PL-004 v.1</p>	<p>Elaborado por: Juan Carlos Angarita Revisado por: John Jairo Triana Aprobado por: Arleth Patricia Saurith Contreras</p>	
---	---	--	--

- 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 2015, 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.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD</p>	<p>DIRECCIÓN TIC SISTEMA INTEGRADO DE GESTIÓN CONTROL DOCUMENTAL PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN Código: SDS-TIC-PL-004 v.1</p>	<p>Elaborado por: Juan Carlos Angarita Revisado por: John Jairo Triana Aprobado por: Arleth Patricia Saurith Contreras</p>	
---	---	--	--

4. RESPONSABLE:

Profesional Especializado Dirección TIC

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD</p>	<p>DIRECCIÓN TIC SISTEMA INTEGRADO DE GESTIÓN CONTROL DOCUMENTAL PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN Código: SDS-TIC-PL-004 v.1</p>	<p>Elaborado por: Juan Carlos Angarita Revisado por: John Jairo Triana Aprobado por: Arleth Patricia Saurith Contreras</p>	
---	---	--	--

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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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]

Riesgos: Efecto de la incertidumbre sobre los objetivos de la organización [ISO 31000]

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

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD</p>	<p>DIRECCIÓN TIC SISTEMA INTEGRADO DE GESTIÓN CONTROL DOCUMENTAL PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN Código: SDS-TIC-PL-004 v.1</p>	<p>Elaborado por: Juan Carlos Angarita Revisado por: John Jairo Triana Aprobado por: Arleth Patricia Saurith Contreras</p>	
---	---	--	--

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 ISMS.

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 herramientas provistas por normas como la ISO 31000, y con base en los riesgos determinados se han trazado controles (alineados con el Anexo A de la norma ISO/IEC 27001:2013 y las guías del Modelo de Seguridad y Privacidad de la Información) los cuales están expresados en este documento.

Finalmente, el plan muestra en color verde aquellas actividades ya realizadas por la entidad y en amarillo las que se encuentran en ejecución o por ser ejecutadas.



DOMINIO		CLÁUSULAS Y/O CONTROLES	ACCIONES	2017/08	2017/09	2017/10	2017/11	2017/12	2018/01	2018/02	2018/03	2018/04	2018/05	2018/06	2018/07	2018/08	2018/09	2018/10	2018/11	2018/12	
1	A5	Políticas SI/MSPI	Formulación																		
			Implementación																		
			Revisión																		
2	A18	Cumplimiento	Identificación																		
			Diseño procedimiento gestión cumplimiento/conformidad																		
			Implementación (proc)																		
			Evaluación periódica de cumplimiento y conformidad																		
3	A8	Gestión de activos	Inventario de activos																		
			Diseño procedimiento gestión de activos (con GDA e ITEP)																		
			Formulación reglas para manejo de medios																		
			Implementación																		
			Revisión																		
4	A6	Organización SI	A.6.1.1 y A.6.1.2																		

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.



DOMINIO		CLÁUSULAS Y/O CONTROLES	ACCIONES	2017/08	2017/09	2017/10	2017/11	2017/12	2018/01	2018/02	2018/03	2018/04	2018/05	2018/06	2018/07	2018/08	2018/09	2018/10	2018/11	2018/12	
		A.6.1.5	Lineamientos generales para gestión de SI en proyectos																		
		A.6.1	Implementación																		
			Revisión																		
5	A7	A7	Formulación lineamientos de SI en recursos humanos (funcionarios y contratistas)																		
			Implementación																		
			Revisión																		
6	A9	A9	Definición de reglas de gestión de acceso																		
			Implementación																		
			Revisión																		
7	#	8.1, A.12.1.2, A.14.2, A.15.2.2,	Definición procedimiento gestión integral del cambio																		
			Implementación																		
			Revisión																		
8	A11	A.11	Diseños de guías de seguridad física y ambiental																		
			Recomendaciones de controles físicos y ambientales																		
			Implementación																		
			Revisión																		

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.



DOMINIO			CLÁUSULAS Y/O CONTROLES	ACCIONES	2017/08	2017/09	2017/10	2017/11	2017/12	2018/01	2018/02	2018/03	2018/04	2018/05	2018/06	2018/07	2018/08	2018/09	2018/10	2018/11	2018/12		
9	A	Seguridad en operaciones	A.12	Diseño de guías de SI en operaciones																			
				Implementación																			
				Revisión																			
10	A	Seguridad en comunicaciones	A.13	Diseño de guías de SI en comunicaciones																			
				Implementación																			
				Revisión																			
11	A	Adquisición, desarrollo y m/to sistemas	A.14 (ISO 9001 8.3)	Formulación de lineamientos en diseño y desarrollo de sistemas																			
				Implementación																			
				Revisión																			
12	A	Relaciones con proveedores	A.15	Formulación de lineamientos para gestión de SI en relaciones con proveedores																			
				Implementación																			
				Revisión																			
13	A	Gestión de incidentes	A.16, A.12.6.*	Formulación de lineamientos para gestión de debilidades, vulnerabilidades e incidentes																			
				Implementación																			
				Revisión																			

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.



DOMINIO			CLÁUSULAS Y/O CONTROLES	ACCIONES	2017/08	2017/09	2017/10	2017/11	2017/12	2018/01	2018/02	2018/03	2018/04	2018/05	2018/06	2018/07	2018/08	2018/09	2018/10	2018/11	2018/12
1	A	SI en continuidad del negocio	A.17	Formulación de lineamientos en gestión de SI en continuidad de negocio																	
4	17			Implementación																	
				Revisión																	

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD</p>	<p>DIRECCIÓN TIC SISTEMA INTEGRADO DE GESTIÓN CONTROL DOCUMENTAL PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN Código: SDS-TIC-PL-004 v.1</p>	<p>Elaborado por: Juan Carlos Angarita Revisado por: John Jairo Triana Aprobado por: Arleth Patricia Saurith Contreras</p>	
---	---	--	--

7. 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

ELABORO			REVISÓ		APROBO	
Nombre:	Juan Carlos Angarita	FIRMA	John Jairo Triana	FIRMA	Arleth Patricia Saurith Contreras	FIRMA
Cargo:	Profesional Especializado		Profesional Especializado		Directora	
Fecha:	24/07/2018		24/07/2018		24/07/2018	

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.