PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1040.26.09

PEDRO ANTONIO ORDÓÑEZ

Contralor

Equipo Oficina de Informática

CONTRALORÍA GENERAL DE SANTIAGO DE CALI

Santiago de Cali, enero de 2023

Tabla de contenido

Contenido

1 INTRODUCCIÓN.

La Contraloría General de Santiago de Cali, en su comité directivo del 30 de julio de 2018 aprobó el plan de acción que integró los planes de la entidad, los cuales daban cumplimiento al Decreto 612 de 2018, es por ello que se busca armonizar el presente plan con la política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios aprobada en 2016 y actualizada en 2021. La CGSC es consciente de que la información es el activo más valioso e indispensable para el ejercicio de sus funciones, por lo cual las estrategias buscan definir los lineamientos y límites que deben cumplir los funcionarios, contratistas y terceros frente a la seguridad de la información, propendiendo con ello salvaguardar la integridad, la confidencialidad y la disponibilidad de la información independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada; lo que se resume en reconsiderar puntos estratégicos como las habilidades del talento humano, la cultura, la estructura organizacional y la implementación de tecnologías emergentes, con el claro objetivo de establecer un tratamiento adecuado de la información que se maneja al interior de la entidad asegurando la seguridad y la privacidad de la misma.

2 OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad y privacidad de la información, seguridad digital y continuidad de los servicios.

3 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS.

La Contraloría General de Santiago de Cali, mediante la adopción de la política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios como parte del Modelo de seguridad y privacidad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad y autenticidad de la información de la Entidad, mediante la gestión integral de riesgos y la implementación de controles tanto físicos como digitales con el fin de dar cumplimiento a requisitos legales y prevenir la materialización de incidentes de seguridad.

3.1 OBJETIVOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS.

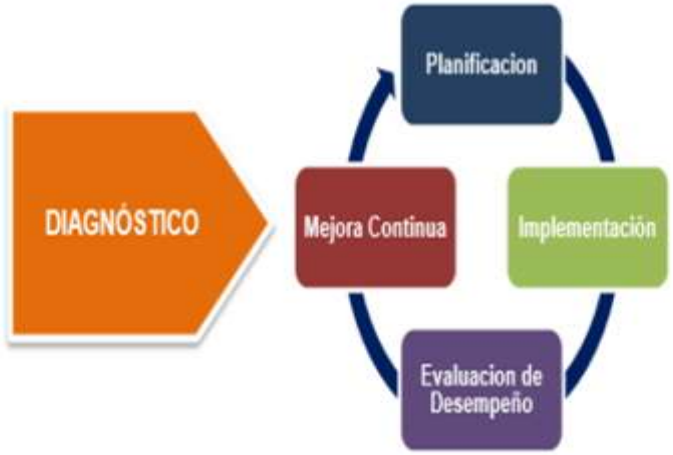
- Dar cumplimiento a los requisitos normativos y legales con respecto a seguridad y privacidad de la información, seguridad digital y continuidad de los servicios.
- .Mitigar de manera efectiva, eficaz y eficiente, los incidentes de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios.

- Gestionar integralmente los riesgos de seguridad y privacidad de la información y seguridad digital.
- Definir los lineamientos para el manejo de la información tanto física como electrónica de acuerdo al sistema de gestión documental basado en la seguridad y privacidad de la información.
- Establecer mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad y confiabilidad de la información de la entidad.
- Generar conciencia para el cambio organizacional que se requiere para la apropiación de la seguridad y privacidad de información en la entidad.
- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y demás partes interesadas.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros y demás partes interesadas de la Contraloría General de Santiago de Cali.
- Garantizar la continuidad de la entidad frente a incidentes de seguridad digital.

4 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Las políticas de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios son aplicables a todos los niveles de la entidad, son de obligatorio cumplimiento por los funcionarios, contratistas, proveedores y terceros que presten sus servicios o tengan algún tipo de relación con la Contraloría General de Santiago de Cali, y que para el adecuado cumplimiento de sus funciones y las de la entidad: compartan, utilicen, recolecten, procesen, intercambien o consulten su información independientemente de su ubicación, medio o formato de presentación.

5 METODOLOGÍA Y OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI



Metodología y Operación del SGSI

La implementación del sistema de Gestión de Seguridad de la Información - SGSI de la Contraloría General de Santiago de Cali, está basada en el Modelo de Seguridad y Privacidad de la Información - MPSI establecido por el MinTIC, el cual tiene como referencia la Norma ISO / IEC 27001:2013 con aplicación del ciclo de operación de la

mejora continua - PHVA (Planear, Hacer, Verificar y Actuar); el cual asegura que el SGSI el sistema se esté sometiendo a revisiones continuas, por la adaptación a cambios importantes en la infraestructura o dependiendo de los resultados obtenidos en la medición de parámetros claves de su operación cuando se requiera mejorar su efectividad.

6 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Mediante Resolución No. 0100.24.03.19.019 del 17 de octubre de 2019, las funciones del comité de Seguridad de la Información fueron asumidas por. el Comité de Gestión y Desempeño de la entidad.

7 PRESUPUESTO PARA EL SGSI

7.1 RECURSOS

7.1.1 Talento Humano

	Nombre Completo	Cargo
Ingeniero	Ingeniero de Sistemas	Jefe de Oficina de Informática
Ingeniero	Ingeniero de Sistemas	Profesional Universitario

Tabla 1. Talento Humano

7.1.2 Recursos tecnológicos

Cantidad	Descripción
1	Software Microsoft Office
1	Computador de escritorio.
2	Computador portátil.

Tabla 2. Recursos Tecnológicos

7.1.3 Recursos Materiales

Cantidad	Descripción
3	Memoria USB o Disco Duro Externo

Tabla 3. Recursos Materiales

7.1.4 Recursos Financieros

Ítem	Descripción	Cant	Vr. Unit	Vr. Total
Pago ingenieros	Integrantes del equipo de trabajo	1	$5.301.226	$5.301.226
Pago ingenieros	Jefe Oficina de Informática	1	10.000.0000	10.000.0000
Subtotal				$15.301.226

Tabla 4. Recursos Financieros – Talento Humano

Ítem	Descripción	Cant	Vr. Unit	Vr. Total
Microsoft Office	Licencia	1	$ 360.000	$ 360.000
Computador de escritorio	Procesador: Core i5 Memoria: 4 GB DDR3 Disco Duro: 1 Tera Pantalla: 20"	1	$ 1.699.0000	$ 1.699.000
Computador portátil	HP K43E-CI3 Procesador: Core I5 Memoria: 8 GB Disco Duro: 500 GB Pantalla: 14"	2	$ 1.199.000	$ 2.398.000
Subtotal				$ 4.427.000

Tabla 5. Recursos Financieros – Recursos Materiales

Ítem	Descripción	Cant	Vr. Unit	Vr. Total
Memoria USB	Memoria USB o Disco Duro Externo	2	$250.000	$500.000
Subtotal				$500.000

Tabla 6. Recursos Financieros – Rubros Recursos Materiales

Descripción	Valor
Subtotal Talento Humano	$15.301.226
Subtotal Recursos Tecnológicos	$4.427.000
Subtotal Recursos Materiales	$500.000
Total Recursos Financieros	**$ 18.927.000**

Tabla 7. Recursos Financieros

7.1.5 Recursos operativos

Se requiere personal altamente calificado en seguridad Informática para la implementación del Sistema de Gestión de Seguridad de la Información.

7.2 COSTOS DE IMPLEMENTACIÓN DEL SGSI

7.2.1 costo de capacitación

La implementación del SGSI para el área de Informática, demanda cambios en la entidad, y adquisición de nuevos conocimientos, para lo cual se debe capacitar en seguridad informática a los integrantes de la oficina de informática.

7.2.2 Costo de asistencia externa

Desafortunadamente, capacitar a los empleados no es suficiente. El coordinador no cuenta con experiencia en la implementación de la norma ISO 27001 y 27002; por lo tanto, se necesita alguien que sí tenga ese conocimiento; para ello, se puede contratar a un consultor externo o se puede optar por alguna alternativa en línea.

7.2.3 Costo de tecnología

No se requiere de grandes inversiones en hardware y software; el mayor desafío consiste en cómo utilizar la tecnología existente de forma más segura.

8 PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

Gestión	Actividades	Tarea	Responsible de la Tarea	Fechas Programación Tareas		Cumplimiento	Evidencia
				Fecha Inicio	Fecha Final		
Organización de la seguri*dad de la información A6*	1. Elaboración de protocolo de comunicación con las autoridades pertinentes en caso de incidentes que comprometan la seguridad de la información	Elaborar y solicitar la aprobación del protocolo.	Jefe Oficina de Informática	01-12-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.
		Definir los lineamientos de política de incidentes de Seguridad	Oficina de Informática	01-07-2021	30-11-2021	100%	Procedimiento gestión de incidentes de seguridad de la información.
		Incluir un ITEM en el SICIS	Oficina de Informática	01-07-2021	30-11-2022	100%	Procedimiento gestión de incidentes

		relacionado con los incidentes de seguridad					de seguridad de la información.
	Definir la política para el uso de dispositivos móviles al interior de la entidad	Incluir la política para el uso de dispositivos móviles al interior de la entidad en la política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios	Oficina de Informática a	01-07-2021	30-11-2021	100%	Poíitica de seguridad y privcidad de la información, seguridad digital y continuidad de los servicios.
Control de Acceso	Implementar políticas de gestión de contraseñas	Configurar en el servidor la gestión de contraseñas	Profesional Universitario	30-07-2021	30-11-2021	100%	Poíitica de seguridad y privcidad de la información, seguridad digital y continuidad de los servicios.

Cifrado	Definir la política de gestión y uso de claves criptográficas al interior de la entidad	Incluir la política de gestión de uso de claves criptográficas al interior de la entidad en la política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios	Oficina de Informática	30-07-2021	30-11-2021	100%	Poíitica de seguridad y privcidad de la información, seguridad digital y continuidad de los servicios.
Seguridad Física y Ambiental	Definir procedimiento para la disposición segura o reutilización de equipos, software licenciado y/o	Definir e implementar el procedimiento para la disposición segura o reutilización de equipos, software	Oficina de Informática	01-12-2021	30-11-2022	100%	Procedimiento de bajas de elementos devolutivos.

	elementos que contengan medios de almacenamiento de información confidencial de la entidad	licenciado y/o elementos que contengan medios de almacenamiento de información confidencial de la entidad					
	política de escritorio limpio y pantalla limpia en la entidad	Incluir la política de escritorio limpio y pantalla limpia al interior de la entidad en la política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios	Oficina de Informática	30-07-2021	30-11-2021	100%	Poíitica de seguridad y privcidad de la información, seguridad digital y continuidad de los servicios.

Gestión de incidentes de seguridad de la información	Definir procedimiento de gestión de incidentes de seguridad	Reportar los eventos de seguridad de información, a través de los canales que se establezcan.	Oficina de Informática	01-12-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.
		Desarrollar e implementar procedimientos de reporte, respuesta y escalación en incidentes de seguridad	Oficina de Informática	30-07-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.
		Definir e implementar procedimientos que aseguren que todos los empleados deben	Oficina de Informática	30-07-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.

		reportar cualquier incidente en la seguridad en los servicios o sistemas de información					
		Definir procedimientos y responsabilidades de gestión para asegurar una rápida, efectiva y ordenada respuesta a los incidentes de seguridad de información	Oficina de Informática	30-07-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.
		Definir mecanismos para identificar y cuantificar el tipo, volumen y costo	Oficina de Informática	30-07-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.

		de los incidentes de seguridad					
		Utilizar información obtenida de la evaluación de incidentes de seguridad que ocurrieron en el pasado, para determinar el impacto recurrente de incidencia y corregir errores	Oficina de Informática	30-07-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.
		Recolectar Las evidencias relacionadas con incidentes, y presentada conforme las disposiciones	Oficina de Informática	01-12-2021	30-11-2022	100%	Procedimiento gestión de incidentes de seguridad de la información.

		legales vigentes en las jurisdicciones pertinentes					

9 MEDICIÓN

La medición del avance en la implementación del Modelo de seguridad y privacidad de la información en la entidad se realizará mediante los siguientes indicadores:

Nombre del indicador	Variables	Meta	Medición	Fuente de información
Grado de avance en la implementación de los controles del modelo de seguridad y privacidad de la información.	(Número de controles Implementados en el período / Número de controles que se planearon implementar en el período) * 100.	Mínima 50 – 75% Satisfactoria 75 – 85% Sobresaliente 85 – 100%	12/12 = 100%	Actas de comité de control y seguimiento SICIS
Cumplimiento de políticas de seguridad de la	La entidad ha definido la política de seguridad de	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y

información en la entidad.	la información?			continuidad de los servicios
Cumplimiento de políticas de seguridad que debe aplicar en los recursos humanos	La entidad ha definido los Lineamientos antes de asumir el empleo? La entidad ha definido los Lineamientos durante la ejecución del empleo? La entidad ha definido los Lineamientos en la Terminación y cambio de empleo	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de políticas de gestión de activos	La entidad ha definido los Lineamientos para la gestión de activos Identificación de Activos? La entidad ha definido los Lineamientos para la Clasificación de activos?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios

	La entidad ha definido los Lineamientos para el Etiquetado de la Información?			
Cumplimiento de políticas de retención y archivo de datos	La entidad ha definido la Lineamientos de retención y archivo de datos?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de intercambio de información	La entidad ha definido los Lineamientos	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de uso de los equipos de cómputo	La entidad ha definido los Lineamientos	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de uso del correo electrónico	La entidad ha definido los Lineamientos	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de uso adecuado de	La entidad ha definido los Lineamientos para el	Cumple 1	1	Política de seguridad y privacidad de la información, seguridad digital y

internet	uso adecuado de internet	No cumple 0		continuidad de los servicios
Cumplimiento de políticas de seguridad en las operaciones	La entidad ha definido los Lineamientos para Respaldo de la información La entidad ha definido los Lineamientos para Protección contra códigos maliciosos?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de control de acceso	La entidad ha definido los Lineamientos de Gestión de Acceso de Usuarios? La entidad ha definido los Lineamientos sobre Responsabilidades de los usuarios? La entidad ha definido los Lineamientos para	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios

	Control de Acceso a Sistemas y Aplicaciones?			
Cumplimiento de política de seguridad física y del entorno	La entidad ha definido los Lineamientos para áreas seguras?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de privacidad y confidencialidad	La entidad ha definido la política de privacidad y confidencialidad?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política para el reporte y tratamiento de incidentes de seguridad	La entidad ha definido la política para el reporte y tratamiento de incidentes de seguridad?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de la política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de	La entidad ha definido los la política de continuidad, contingencia, recuperación y retorno	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios

seguridad de la información	a la normalidad con consideraciones de seguridad de la información?			
Cumplimiento de la política de redundancia	La entidad ha definido de la política de redundancia?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de seguridad en las comunicaciones	La entidad ha definido los Lineamientos para la Gestión de la seguridad de las redes?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de seguridad para la relación con proveedores	La entidad ha definido la de política de seguridad para la relación con proveedores	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de política de seguridad para dispositivos móviles	La entidad ha definido la política de seguridad para dispositivos	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios

	móviles?			
Cumplimiento de la política de seguridad para criptografía	La entidad ha definido los Lineamientos para el uso de Claves Criptográficas?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
Cumplimiento de la política de escritorio limpio y pantalla limpia.	La entidad ha definido la política de escritorio limpio y pantalla limpia.?	Cumple 1 No cumple 0	1	Política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios

10 DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 2093. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 2099. Por 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 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- 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 y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- 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 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 de espectro y se dictan otras disposiciones.

- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

- 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.

- Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario

- Ley 2055 de 2020. Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”.

- Decreto 2609 de 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.

- Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.

- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 1008 del 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 de Tecnologías de la Información y las Comunicaciones.

- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

- Plan de Seguridad y Privacidad de la Información Versión 2.0 del Ministerio de Tecnologías de la Información y las Comunicaciones.

	Nombre	Cargo	Firma
Proyectó tó	Noralba Hoyos Ruiz	Profesional Universitario	
Revisó	Equipo Informatica	Profesional Universitario	
Aprobó	Comité Directivo	Comité Directivo	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			

ANEXO No. 1

CONTRALORÍA
GENERAL DE SANTIAGO DE CALI

ANEXO No. 1

PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CONTRALORÍA GENERAL DE SANTIAGO DE CALI

EQUIPO OFICINA DE INFORMÁTICA

TABLA DE CONTENIDO

INTRODUCCIÓN

En un mundo cada vez más digital, donde las formas y medios que utilizamos para comunicarnos, trabajar e interactuar con otros, se realiza por medios electrónicos, nos debemos preguntar: ¿Cómo puedo garantizar la seguridad de la información en medios digitales?, para dar respuesta a este planteamiento, se crea este plan que ayudará a la Contraloría General de Santiago de Cali a cumplir con la estrategia de gobierno digital de Mintic, y servirá de guía para actuar de forma efectiva ante un incidente de la seguridad de la información.

1. OBJETIVO

Gestionar incidentes de seguridad y privacidad de la información, seguridad informática o seguridad digital (en el documento se denominará incidentes de seguridad), teniendo en cuenta los lineamientos y estándares definidos, a través de una oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la Contraloría General de Santiago de Cali (en adelante se denominará como CGSC).

2. ALCANCE

La gestión de incidentes de seguridad inicia desde la identificación de un evento, detección, contención y solución de este, finalizando con la documentación y las lecciones aprendidas.

Este procedimiento aplica para la CGSC en la sede CAM piso 7, CAM torre Emcali piso 16 y el edificio Fuente Versalles pisos 5, 7 y mezanine primer piso.

3. POLÍTICAS DE OPERACIÓN

3.1. Solicitud reporte de Incidentes

Los posibles incidentes de seguridad se reportaran al equipo de la Oficina de Informática por medio de:

- Llamando a la mesa de servicio extensiones IP: 121, 127 y 621 para todas las sedes.
- Al Correo electrónico: oinformatica@contraloriacali.gov.co

El servidor público que identifique el posible incidente de seguridad debe reunir la información que llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención de este, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos entre otros.

3.2. Categorización del Incidente.

Cuando se recibe el reporte del posible incidente de seguridad, el equipo de informática debe realizar una categorización del mismo, bajo alguno de los siguientes criterios:

- Hubo daño o pérdida de información física o digital.
- Hubo fuga y/o robo de información física o digital.
- Hubo robo de credenciales o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presentó un comportamiento anormal del computador y/o sistema de información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware, Ransomware”.
- Se presentó una denegación del servicio.
- Se presentó algún ciberataque.
- Uso indebido de imagen institucional.

Todos los incidentes de seguridad deben ser registrados en el aplicativo SICIS en la sección de soportes, con información detallada del caso, como causas, consecuencias y soluciones, teniendo en cuenta el impacto y el tipo de urgencia.

Tabla 1 Valoración del Impacto.

IMPACTO	DESCRIPCIÓN	VALORACIÓN
Catastrófico	**Extremadamente Nocivo**: Si el hecho llegara a presentarse, tendría consecuencias desastrosas o efectos sobre la entidad a nivel de: • Afectación Imagen a Nivel Nacional e Internacional. • Sanciones de Contraloría, Procuraduría y Fiscalía. • Daños totales de la infraestructura de la entidad. • Fuga de información sensible para la entidad. • Pérdidas monetarias.	**ALTO**
Moderado	**Moderado:** Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. • Afectación Imagen del proceso o área a Nivel de la entidad. • Sanciones a nivel de Oficina Jurídica o Control Interno. • Daños parciales de la infraestructura de la entidad. • Llamados de atención a nivel Organizacional	**MEDIO**

Menor	**Menor:** Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad: • Afectación Imagen grupo o área a nivel del proceso. • Sanciones a nivel procesos. • Daños pequeños de la infraestructura de la entidad • Llamados de atención a nivel proceso	**BAJO**

La tabla anterior permite identificar en una escala el impacto que el incidente puede tener al interior de la CGSC, lo cual sirve como insumo para determinar el tiempo de respuesta del incidente.

Tabla 2 Tiempo de Respuesta

Urgencia	Tiempo de Respuesta en Minutos
ALTO	0 a 180 min.
MEDIO	0 a 240 min.
BAJO	0 a 480 min.

La tabla 2 indica un tiempo de respuesta máximo durante el cual el incidente debe ser recibido y solucionado, según el impacto que este tenga en la entidad.

3.3. Equipos de Respuesta.

Los equipos de respuesta están conformados según el impacto y los recursos que afecte el incidente.

3.3.1. Equipo para Incidentes de Alto Impacto

Dentro de los incidentes de alto Impacto podemos tener la afectación de recursos como BD, servidores y página web, los grupos son sugeridos y no es una limitante a la hora de tomar decisiones para atender un incidente, dependiendo del tipo del incidente se debe evaluar la posibilidad de solicitar consultoría a expertos especializados en un tema.

Incidente a Bases de Datos (BD).

Los incidentes a bases de datos involucran a:

- El secretario(a) que es el encargado de recibir por correo o llamada telefónica el reporte del incidente.
- El administrador(a) de BD, quien determina el tipo de afectación.
- El administrador(a) del dominio que brindará el apoyo necesario para ayudar a

aislar y/o solucionar el incidente.
- La Dirección Administrativa y financiera que se encargará de comunicar a las diferentes áreas del incidente, además de proveer recursos en caso de que se necesiten.

Incidente a Servidores.

Los incidentes a servidores involucran a:

- El secretario(a) que es el encargado de recibir por correo o llamada telefónica el reporte del incidente.
- El administrador(a) del dominio que brindará el apoyo necesario para ayudar a aislar y/o solucionar el incidente.
- El técnico de que se encargará de brindar apoyo en actividades a nivel de hardware en los servidores y la red.
- La Dirección Administrativa y financiera que se encargará de comunicar a las diferentes áreas del incidente, además de proveer recursos en caso de que se necesiten

Incidente a la Página Web.

Los incidentes a la página web involucran a:

- El secretario(a) que es el encargado de recibir por correo o llamada telefónica el reporte del incidente.
- El administrador de la página web.
- El personal de soporte del hosting donde se aloja la página web.

3.3.2. Equipo para Incidentes de Impacto Medio.

En esta categoría tenemos los incidentes al software misional, el servidor de correo electrónico e infecciones por software malicioso en carpetas compartidas.

Incidentes al Software Misional.

Los incidentes al software misional involucran a:

- El secretario(a) que es el encargado de recibir por correo o llamada telefónica el reporte del incidente.
- El administrador del software misional de la CGSC.
- El administrador del dominio.

Incidentes al servidor de correo electrónico.

Los incidentes al correo electrónico involucran a:

- El secretario(a) que es el encargado de recibir por correo o llamada telefónica el reporte del incidente.
- El administrador del dominio.
- El personal de soporte del prestador de servicios de correo.

Incidentes en Carpetas Compartidas.

Los incidentes en carpetas compartidas involucran a:

- El secretario(a) que es el encargado de recibir por correo o llamada telefónica el reporte del incidente.
- El administrador del dominio.
- El técnico de apoyo.

3.3.3. Equipo para Incidentes de Bajo Impacto.

En esta categoría encontramos incidentes de tipo usuario final, este tipo de incidentes involucran a:

- El secretario(a) que es el encargado de recibir por correo o llamada telefónica el reporte del incidente.
- El administrador del dominio.
- El técnico de apoyo.

3.4. Restauración de la Información.

Algunos incidentes se pueden contener y no se hace necesario restaurar información, para los casos que aplique la CGSC debe contar con copias de seguridad de las BD, imágenes de los servidores, copias de seguridad de archivos y configuraciones.

Estas copias de seguridad garantizan la continuidad del negocio en caso de un incidente de tipo catastrófico, al momento de restaurar la información se debe registrar en el aplicativo SICIS la fecha y hora de la copia de seguridad, e informar a las partes afectadas, con el fin de que puedan validar la integridad de la misma y establecer que información debe ser generada nuevamente.

3.5. Recolección de evidencias

Se deben conservar y proteger las evidencias recopiladas, con el fin de que estás no puedan ser modificadas, lo anterior para analizar la información y poder establecer por qué se generó el incidente, y que a su vez sirvan de pruebas para entes investigativos si el caso lo amerita.

Dentro de las evidencias se pueden considerar.

- El reporte del o los usuarios que generaron el reporte.
- Los logs generados por los servidores.
- Los logs generados por el software de la CGSC.
- El procedimiento de que siguió el grupo que atendió el incidente.
- Capturas de pantalla, fotos y videos.
- Entre otros.

Estás evidencias deben ser protegidas contra escritura y modificación, e inventariadas, se debe redactar un documento donde resida el inventario de las evidencias, los lineamiento para tratar las evidencias se encargará la Dirección Administrativa y Financiera.

3.6. Gestión del Conocimiento Tecnológico.

Cuando el grupo que atendió el incidente lo considere necesario deberá crear un manual o instructivo que sirva de guía para solucionar el incidente, y así reducir los tiempos de atención del mismo, dicho documento debe quedar a disposición del personal que conforme la oficina de informática y debe ser socializado para que el equipo en general se retroalimente de lo ocurrido.

3.7. Reportes Externos.

Al presentarse un incidente de seguridad de la información y en caso de ser necesario el Director Administrativo o quien el delegue, debe realizar el reporte a entes externos.

Los reportes se pueden realizar a través de los siguientes canales:

- **COLCERT** (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+57) 601 344 2222, o ingresando al sitio web https://www.colcert.gov.co/800/w3-article-198656.html, y buscar la opción reportar un incidente.
- **CSIRT** Gobierno reportar al correo **csirtgob@mintic.gov.co**
- Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/

3.8. Activación del plan de contingencias

Si al realizar el análisis del incidente se determina que la solución del mismo supera los límites de tiempo estipulado, se debe informar de la situación al líder del equipo informático o quien haga sus veces, para que autorice la activación del plan de contingencias, para la recuperación lo antes posible del incidente ocurrido.

3.9. Lecciones aprendidas

Una vez superado el incidente se debe realizar un análisis grupal, para evidenciar las fortalezas y debilidades en el procedimiento, y ajustar las inconsistencias para fortalecer el procedimiento.