PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MARÍA FERNANDA AYALA ZAPATA
Contralor

Equipo oficina de informática

CONTRALORIA GENERAL DE SANTIAGO DE CALI
Cali, Diciembre de 2020

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 2020. La Contraloría General de Santiago de Cali es consciente de que la información es el activo más valioso e indispensable para el ejercicio de sus funciones, es por ello que la presentes 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 las mismas.

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 ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y 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.

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 OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI

Modelo de Operación por Gestiones de Seguridad y Privacidad de la Información, seguridad digital y continuidad de la Operación

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 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.

			Responsible de la Tarea	**Fechas Programación Tareas**	
Gestión	**Actividades**	**Tarea**		**Fecha**	**Fecha**
				Inicio	**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	Solicitar la aprobación del procedimiento que existe en la actualidad	Jefe Oficina de Informática	01-07-2021	30-11-2021
		Definir la política de incidentes de Seguridad	Oficina de Informatica	01-07-2021	30-11-2021
		Incluir en un ITEM en el formato de atención a Usuarios relacionado con los incidentes de seguridad	Oficina de Informatica	01-07-2021	30-11-2021
	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 politica de seguridad y privacidad de la	Oficina de Informatica	01-07-2021	30-11-2021

		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
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
Seguridad Física y Ambiental	Definir procedimiento establecido para la disposición segura o reutilización de equipos, software licenciado y/o elementos que contengan medios de almacenamiento de información confidencial de la entidad	Definir e implementar el procedimiento establecido para la disposición segura o reutilización de equipos, software licenciado y/o elementos que contengan medios de almacenamiento de información confidencial de la entidad	Oficina de Informática	30-07-2021	30-11-2021

	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 politica de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios	Oficina de Informática	30-07-2021	30-11-2021
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	30-07-2021	30-11-2021
		desarrollar e implementar procedimientos de reporte, respuesta y escalación en incidentes de seguridad	Oficina de Informática	30-07-2021	30-11-2021
		Definir e implementar procedimientos que aseguren que todos los empleados deben reportar cualquier incidente en la seguridad en los servicios o sistemas de información	Oficina de Informática	30-07-2021	30-11-2021

		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	30-11-2021
		Definir mecanismos para identificar y cuantificar el tipo, volumen y costo de los incidentes de seguridad	Oficina de Informática	30-07-2021	30-11-2021
		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	30-11-2021
		Recolectar Las evidencias relacionadas con incidentes, y presentada conforme las disposiciones legales vigentes en las jurisdicciones pertinentes	Oficina de Informática	30-07-2021	30-11-2021

8 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 2015 de 2018. Por la cual se modifica la Ley 23 de 2082 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- 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			
Revisó			
Aprobó			
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.			