PLAN DE SEGRURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MUNICIPIO DE PROVIDENCIA Y SANTA CATALINA ISLAS

JORGE NORBERTO GARY HOOKER
ALCALDE 2020-2023

SECRETARÍA GENERAL Y ADMINISTRATIVA

Junio de 2020

Palacio Municipal, Santa Isabel
Providencia y Santa Catalina Islas
Tel. (57) 8 514 8227

Insular Consulting Group S.A.S

AGRADECIMIENTOS

El presente Plan de Seguridad y Privacidad de la Información es resultado del valioso aporte de todas las dependencias de la Alcaldía del Municipio de Providencia y Santa Catalina que brindaron la información necesaria y de manera oportuna para la formulación del presente Plan, cuyos resultados se presentan en este documento.

1. Introducción

Es cada vez más evidente el rol estratégico y potenciador que tienen las Tecnologías de la Información y las Comunicaciones – TIC en la competitividad, eficiencia y sostenibilidad, tanto en las entidades públicas del país, como en los territorios que estas administran. Asimismo, en la actualidad, la información se ha constituido en el activo mas importante de una organización, por lo tanto, se hace indispensable planificar y promover medidas que garanticen, no solamente el uso, sino también un óptimo aprovechamiento de la información de la Alcaldía del Municipio de Providencia y Santa Catalina.

2. Objetivo del Plan de Seguridad 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 Digital y Continuidad del servicio, en el Mapa de Procesos de la Alcaldía del Municipio de Providencia y Santa Catalina.

3. Alcance del Sistema de Gestión Seguridad de la Información

Aplica a todos los niveles de la Alcaldía de Providencia y Santa Catalina Islas, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que, en razón del cumplimiento de sus funciones y las del Ministerio, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por la Alcaldía, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

4. Operación del Sistema de Gestión de Seguridad de la Información – SGSI

Modelo de Operación por Gestiones del Dimensión de Seguridad de la Información

5. Comité de Seguridad de la Información

La Alcaldía del Municipio de Providencia y Santa Catalina deberá crear un Comité para el proceso de ejecución y seguimiento de la Seguridad de la Información en la entidad. A este Comité deberán pertenecer el alcalde, como cabeza visible de la entidad, el Líder TIC o quien haga sus veces, el Jefe de Talento Humano o quien haga sus veces, los Líderes de los procesos de Planeación y Jurídicos.

6. 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 estimado y se le debe hacer seguimiento mes a mes:

Gestión	Actividades	Tareas	Responsable de la tarea	Días estimados para la ejecución de tareas
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Elaboración metodología e instrumento de levantamiento de activos de información.	Equipo Activos	23
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	Equipo Activos	5
		Validar activos de información preexistentes.	Enlace de cada proceso, Equipo Activos	10
		Identificar nuevos activos de información en cada dependencia.	Enlace de cada proceso, Equipo Activos	10
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo Activos	10
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información.	Enlaces de cada proceso	12

		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Enlaces de cada proceso	153
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación por cada líder de proceso.	Enlace de cada proceso, Equipo Activos	15
		Consolidar el instrumento de activos de Información.	Equipo de Activos	8
		Publicar los instrumentos de activos de información consolidado.	Oficina Asesora de Planeación	3
	Registros activos de información ley 1712	Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información.	Equipo de Activos	10
		Enviar a control de legalidad el instrumento de Registro Activos de información.	Equipo de Activos, Oficina Asesora Jurídica.	5
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	Oficina Asesora Jurídica	1

	Reporte Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos.	Equipo de Activos	1
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos.	Equipo de Gestión de Riesgos	30
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Equipo de Gestión de Riesgos	9
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Equipo de Gestión de Riesgos	2
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes).	Equipo de Gestión de Riesgos	153
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento.	Equipo de Gestión de Riesgos	153
	Publicación	Publicación Matriz de riesgos.	Equipo de Gestión de Riesgos	153
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias.	Equipo de Gestión de Riesgos	154

	Evaluación de riesgos residuales	Evaluación de riesgos residuales.	Equipo de Gestión de Riesgos	184
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales.	Equipo de Gestión de Riesgos	184
		Actualización Plan de Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados.	Equipo de Gestión de Riesgos	184
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores.	Equipo de Gestión de Riesgos	184
Gestión de Incidentes de Seguridad de la Información	Elaboración de procedimiento de gestión de incidentes de seguridad	Elaboración del procedimiento de gestión de incidentes basados en la ISO 27035.	Equipo Incidente	30
	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Publicar el procedimiento de gestión de incidentes de Seguridad de la Información.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	5
		Socializar el procedimiento a los soportes en sitio y Mesa de Servicios, indicando los cambios en el procedimiento.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	5
		Socializar el procedimiento a los colabores de la Entidad.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	5

	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido.	Gestión de la Información	184
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	302
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	12
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	2
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI.	Gestor de procesos	244
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI.	Encargado de la Gestión de Incidentes de Seguridad de la Información.	214

Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información.	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	27
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información.	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	210
Plan de Continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Actualización del Análisis de Impacto del Negocio.	Equipo de Continuidad del Negocio	184
		Publicación del Análisis de Impacto del Negocio.	Equipo de Continuidad del Negocio	184
	Documentación de Valoración de Riesgos de Interrupción	Actualización del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación.	Equipo de Continuidad del Negocio	184
		Publicación Valoración de Riesgos de interrupción.	Equipo de Continuidad del Negocio	184
	Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación.	Equipo de Continuidad del Negocio	184
		Publicación Estrategias de Continuidad de la Operación.	Equipo de Continuidad del Negocio	184
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación.	Equipo de Continuidad del Negocio	184
		Aprobación del Plan de continuidad de la Operación.	Equipo de Continuidad del Negocio	184

Acciones correctivas y Notas de mejoras SGSI	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar reporte del estado actual de las AC y OM	Planeación	325
		Solicitar el cargue del análisis de causas o plan de tratamiento según sea requerido.	Planeación	325
	Generar observaciones o recomendaciones a los acompañamientos realizados a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos.	Planeación	325
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información.	Oficial de Seguridad de la Información	27
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.).	Oficial de Seguridad de la Información	244
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Oficial de Seguridad de la Información	22
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Oficial de Seguridad de la Información	30
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad.	Oficial de Seguridad de la Información	30

		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información.	Oficial de Seguridad de la Información	302
		Cumplimiento requerimientos infraestructuras críticas del gobierno.	Oficial de Seguridad de la Información	322
Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.	Oficial de Seguridad de la Información	322
Indicadores SGSI	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI.	Oficial de Seguridad de la Información	107
		Reportar indicadores.	Gestores de procesos	183
Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pentest	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades.	Oficial de Seguridad de la Información	11
	Contratar Análisis de Vulnerabilidades y Pentest	Definir estudios previos y procesos de contratación para realizar el pentest y análisis de vulnerabilidades teniendo en cuenta el alcance y metodología.	Oficial de Seguridad de la Información, Contratación	30
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo con el	Pentester	30

		alcance y la metodología establecida.		
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades y pentest.	Oficial de Seguridad de la Información	92
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC.	Oficial de Seguridad de la Información	5
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos.	Oficial De Seguridad y Gestor de procesos	302
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información.	Oficial de Seguridad de la Información	275

7. Documentos de Referencia

- **Constitución Política de Colombia.** Artículo 15.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

- **Ley 527 de 1999.** 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.
- **Plan de Seguridad y Privacidad de la Información,** versión 1.0, del Ministerio de Tecnologías de la Información y Comunicaciones.

(ORIGINAL FIRMADO)
Dr. Andrés Guzmán Montes
Representante Lega ICG – S.A.S.