INSTRUCTIVO PARA LA DEFINICIÓN ROLES Y RESPONSABILIDADES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. PROPOSITO

El siguiente documento es una guía para la definición del equipo responsable del seguimiento y del cumplimiento del modelo de seguridad y privacidad de información dentro del Distrito de Cartagena.

2. ALCANCE

El presente documento aplica a todo el distrito de Cartagena y parte desde el planteamiento de la política de seguridad digital hasta las estrategias de seguimiento y mejora de este.

3. GLOSARIO

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la organización antes de crear nuevas políticas.
- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

- **Política:** Declaración de alto nivel que describe la posición de la organización sobre un tema específico.
- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.
- **Responsabilidad:** Cualidad de la persona responsable. "para cubrir ese puesto buscan a una persona con responsabilidad".
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **Rol:** Papel, función que alguien o algo desempeña.

4. DEFINICIÓN DE ROLES Y RESPONSABILIDADES

El mayor aporte que genera una definición de roles es que se tendrán establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, dejando un campo muy pequeño a que se presenten imprecisiones en referencia a las responsabilidades que cada personaje tiene.

Partiendo de este punto, la entidad tendrá asegurado que cada actividad establecida dentro de la etapa de planeación del MSPI, tenga un responsable claro y de igual forma que cada uno de los miembros del equipo responsable de la ejecución entiendan claramente sus roles y responsabilidades.

4.1 IDENTIFICACIÓN DE LOS RESPONSABLES

En primer lugar, se genera la necesidad de vincular de forma más efectiva al personal de alto nivel que estará vinculado al proceso de desarrollo del MSPI en el Distrito para que el apoyo se vaya garantizando desde el principio de la planeación del proyecto e ir marcando un punto de partida de éxito con la implementación del modelo de gestión de seguridad de la información planteado para la Entidad Distrital.

Los representantes de alto nivel de la entidad deben identificar y establecer, sin perjuicio de lo establecido en la Ley 489 de 1998, en el menor tiempo posible

organizar el grupo de trabajo responsable para implementar el Modelo de seguridad y Privacidad de la información en la entidad, definiendo el perfil y rol de conformidad con lo establecido en su documento de política.

Teniendo en cuenta lo anterior, al final del ejercicio el equipo directivo que lidera la implementación del MSPI, debe dar a conocer el perfil y responsabilidades de los responsables.

4.2 EQUIPO DE GESTIÓN AL INTERIOR DEL DISTRITO

El equipo será liderado por la mesa de transformación digital, quien se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad y Privacidad de la Información al interior del Distrito, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

Es importante resaltar la necesidad del compromiso de la Alta dirección de la entidad, de esta forma se presenta la figura No. 01, en la cual se presentan los perfiles de manera genérica el nivel al cual pertenecerían según lo propuesto.

Figura 1 Perfiles

4.3 PERFILES Y RESPONSABILIDADES

Con el fin de poder realizar la labor de la manera más eficiente, se sugiere el conjunto de integrantes para el equipo al interior de la entidad, denominados de la siguiente forma:

4.3.1 Responsable de la política de Seguridad de la Información

ROL	RESPONSABILIDADES	RESPONSABLE
Líder de la Política Seguridad Digital	• Emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial. De igual manera, a través de la Dirección de Gobierno Digital se desarrollan diferentes iniciativas y proyectos que buscan apalancar la implementación de la política en las entidades públicas.	Ministerio de Tecnologías de la Información y Comunicación a través de la Dirección de Gobierno Digital
Responsable Institucional de la Política de Seguridad Digital	• Responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Seguridad Digital. Debe garantizar el desarrollo integral de la política al interior de sus entidades, entendiendo que esta es un eje transversal y apalancador de su gestión interna, que apoya el desarrollo de las políticas de gestión y desempeño institucional.	Representante Legal - alcalde Mayor
Responsable de orientar la implementación de la Política de Gobierno Digital	• Orientar la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se encuentra seguridad Digital); debe articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que Gobierno Digital se desarrolle articuladamente con las demás políticas en el marco del sistema de gestión de la entidad. Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información. Hacer que los miembros del Gabinete sean conscientes de la criticidad de los activos de información para el desarrollo de los procesos de la Alcaldía Distrital de Cartagena de Indias. Divulgar las responsabilidades de seguridad y privacidad de la información de la Alcaldía Distrital de Cartagena de Indias con base en los lineamientos del MSPI.	Comité Institucional de Gestión y Desempeño
Responsable de Seguridad de la Información	• Hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad. Las demás áreas serán corresponsables de la implementación de la	Profesional independiente a la OAI y debe pertenecer a la alta dirección

	Política de Seguridad Digital en los temas de su competencia. Además de: Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la Alcaldía, Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información, Apoyar las actividades relacionadas con el MSPI. En este sentido, áreas o dependencias afines a los siguientes temas también son responsables en la implementación de la política de Seguridad Digital, dada su transversalidad en la gestión de la entidad: planeación, secretaría general, servicio al ciudadano, participación ciudadana, comunicaciones o prensa, desarrollo organizacional, talento humano, archivo y gestión documental. Una de las tareas principales del líder de esta implementación de la política es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol. • Personal de seguridad de la información. • Personal de la oficina asesora de informática • Un representante del área de Tecnología. • Un representante del área de Control Interno. • Un representante del área de Planeación. • Un representante de sistemas de Gestión de Calidad/ MIPG • Un representante del área Jurídica. • Un representante de cada dependencia del distrito de Cartagena • Funcionarios, proveedores, y ciudadanos.	
Otros roles e instancias importantes	• Estas instancias deben actuar en coordinación con el comité institucional de gestión y desempeño para la toma de decisiones. Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo. Alineación de los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI. Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles definidos en la dependencia a cargo. Proveer los recursos necesarios para la implementación del MSPI al interior de la dependencia a cargo. Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas de la dependencia a cargo que cumplan con el MSPI. Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista de la dependencia a cargo.	nivel directivo secretarios, asesores, directores y jefes de oficina.

Verificación, seguimiento y control de las políticas de seguridad digital	• Apoyar en definir y actualizar el inventario de los activos de información. Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI. • Definir y generar el modelo de seguridad y privacidad de la información - MSPI. • Identificar los requerimientos normativos, de servicios o software necesarios para implementar, mejorar y garantizar la eficacia del protocolo de seguridad informática, garantizando la integridad, la confidencialidad y la protección de todos los activos de la empresa a nivel tecnológico. • Definir la arquitectura de la seguridad de la red y sus políticas de acceso y control Potenciar la cultura de seguridad informática a nivel global en la Alcaldía. • Analizar los sistemas de información con el ánimo de encontrar eventos o incidentes que puedan afectar el procedimiento y ocasionar fugas de información, suplantación o corrupción de los datos, apoyando en definición del plan de tratamiento de los riesgos de seguridad y privacidad de la información. • Participar en el seguimiento y evaluación de las políticas, programas e instrumentos relacionados con la información pública, confidencial y sensible que esté bajo la responsabilidad de la alcaldía de Cartagena de Indias • Impartir lineamientos tecnológicos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información de la Entidad y la interoperabilidad de los sistemas que la soportan, así como el intercambio permanente de información. • Hacer seguimiento de los esquemas de seguridad operativa. Auditar procesos, aplicativos, gestión de usuarios y servicios. Investigar las posibles amenazas y vulnerabilidades a nivel de toda la Alcaldía. • Controlar la implementación de sistemas de información, Sistemas informáticos y/o servicios a nivel trasversal de la Alcaldía Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.	Oficial de seguridad y privacidad de la información
Oficina Jurídica	• Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.	

	• Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso. • Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.	
Director Talento humano	• Controlar y salvaguardar la información de datos personales del personal de planta de la entidad, en concordancia con la normatividad vigente. • Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.	

Tabla 1 Roles y responsabilidades de seguridad de la información

4.3.2 Responsabilidades por dominios del marco de arquitectura empresarial

Dentro de la definición de responsables en cada uno de los Dominios entregados en el Marco de arquitectura Empresarial, está contemplado el papel del responsable de seguridad y privacidad de la información de la entidad, de esta forma se tienen las siguientes responsabilidades específicas de acuerdo con el Dominio:

DOMINIO	RESPONSABILIDADES	RESPONSABLE
SERVICIOS TECNOLÓGICOS	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. • Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. • Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. • Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el	Oficina Asesora de informática

	desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.	
ESTRATEGIA TI	• Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la Alcaldía de Cartagena. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.	Comité de seguridad de la información
GOBIERNO TI	• Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información	Comité de gestión y desempeño institucional
SISTEMAS DE INFORMACIÓN	• Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro del Distrito de Cartagena. • Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. • Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. • Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio • Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. • Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información	Oficina Asesora de informática/ subproceso de seguridad estratégica
USO Y APROPIACIÓN	• Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de	

	seguridad de la información en diferentes niveles. • Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. • Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.	Mesa de transformación digital

Tabla 2 Responsabilidades y responsables por Dominio en el Marco de Arquitectura Empresarial

4.3.3 Roles y responsabilidades de los equipos y comités de gestión de seguridad

4.3.3.1 Comité de seguridad

Se debe conformar un equipo para la implementación del modelo de seguridad y privacidad de la información, al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Las funciones de este comité pueden ser asumidas por el comité de gestión y desempeño institucional, como instancia orientadora de la implementación del modelo de planeación y gestión MIPG, El Comité estará integrado así:

- El Jefe de la oficina asesora de informática.
- El Jefe de la secretaria de Planeación o su representante.
- El Jefe de la oficina Jurídica o su delegado.
- El Directivo encargado de los sistemas de Gestión de Calidad / MECI/MIPG o su delegado
- El Directivo encargado de la Gestión Documental o su delegado.
- El Directivo encargado de Control Interno o su delegado.
- El responsable de Seguridad de la información de la entidad.

El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo,

así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Funciones del comité.

El Comité de Seguridad de la Información tendrá dentro de sus funciones las siguientes:

- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad.
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
- Las demás funciones inherentes a la naturaleza del Comité.

Una vez reglamentado el comité se organizará el reglamento teniendo en cuenta la existencia de:

Secretaria Técnica: La Secretaría Técnica del Comité se definirá al interior del Comité y el secretario elegido será remplazado cada 12 meses.

Funciones de la Secretaría Técnica. Las funciones de la Secretaría Técnica serán las siguientes:

- Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
- Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias

- Remitir oportunamente a los miembros la agenda de cada comité.
- Llevar la custodia y archivo de las actas y demás documentos soporte.
- Servir de interlocutor entre terceros y el Comité.
- Realizar seguimiento a los compromisos y tareas pendientes del Comité.
- Presentar los informes que requiera el Comité.
- Las demás que le sean asignadas por el Comité

Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse cada tres meses en convocatoria del secretario técnico del Comité.

Sesiones Extraordinarias. Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo con temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

4.3.3.2 Papel de la Mesa De Transformación Digital y otras instancias

La mesa es quien conforma este comité, dado que tiene injerencia en la seguridad digital del Distrito. A continuación, se presentan las responsabilidades de la mesa de transformación digital:

- Apoyar al líder al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en la implementación
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas.

De manera particular se resaltan dos perfiles que deben estar participando de manera activa durante la implementación, a pesar de que no es de responsabilidad exclusiva del área de TI su papel es fundamental, y de acuerdo con la Ley de Protección de Datos Personales se debe tener muy presente el rol de responsable del tratamiento de los datos personales.

Teniendo en cuenta que el responsable del tratamiento de datos personales en la entidad, es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta que de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- Respetar las condiciones de seguridad y privacidad de información del titular.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

4.3.3.3 Equipo de Respuesta a Incidentes de Seguridad de la Información (CSIRT)

Se hace necesario crear el equipo de Respuesta a Incidencias de Seguridad Informática CSIRT (Computer Security Incident Response Team), como guía para resolver los percances de seguridad de la información que se generen sobre los activos avalados por la plataforma tecnológica de la entidad, la cual soporta el análisis de nuevas falencias y brechas de seguridad.

Se debe tener en cuenta que el equipo CSIRT no es responsable de la prevención de dichos percances, sino más bien es un pilar fundamental de los programas de respuesta. Este equipo debe ser un garante en el establecimiento de recomendaciones para el aseguramiento de los sistemas de información y la plataforma que los avala, a través de las siguientes responsabilidades:

- Establecer los parámetros para el manejo de incidentes informáticos.
- Seleccionar y clasificar los incidentes.
- Detectar Incidentes de Seguridad: Monitorear y examinar los factores de control para hallar los posibles incidentes de seguridad de la información.
- Atender Incidentes de Seguridad: Recibir y solucionar los incidentes de seguridad siguiendo los parámetros establecidos.
- Recopilar y Evaluar Evidencia Digital: Recopilar, almacenar, documentar y evaluar la evidencia cuando sea requiera.
- Realizar Anuncios de Seguridad: Brindar información oportuna a los funcionarios, contratistas o terceros sobre las nuevas falencias, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación en el que quede evidencia (Web, Intranet, Correo).

- Ejecutar Auditorias y trazabilidad de Seguridad Informática: El equipo debe hacer análisis periódicos del estado de la plataforma para analizar nuevas falencias y brechas de seguridad.
- Certificar productos: El equipo verifica el despliegue de las nuevas aplicaciones en producción para que se ajusten a los requisitos de seguridad informática establecidos por el equipo.
- Configurar y Administrar Dispositivos de Seguridad Informática: Responsables del manejo adecuado de los elementos de seguridad informática.
- Clasificar y priorizar servicios expuestos: Identificar los servicios vulnerables y aplicaciones expuestas para la prevención o solución de ataques informáticos.
- Investigar o Desarrollar nuevas herramientas: El equipo debe analizar constantemente los nuevos productos en el mercado o la creación de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad informática.

Equipo que lo conforma:

- Responsable de Seguridad de la Información
- Administradores de los Sistemas de Información
- Director del jefe de la oficina asesora de Informática
- Técnico de Mantenimiento subproceso de infraestructura

4.3.3.4 Comité de crisis

El Comité de gestión de crisis conforma un comité con el máximo nivel de decisión gestionando los incidentes disruptivos, de forma que se mitiguen los impactos que puedan afectar a la entidad, y con ello mantener la continuidad de negocio de la entidad:

- Tomar las decisiones estratégicas de alto nivel necesarias para que la Entidad proporcione una adecuada respuesta durante una situación de crisis.
- Activación de los protocolos establecidos o definidos en el momento de la crisis.
- Coordinar y asumir la responsabilidad de todas las medidas de respuesta a la crisis.
- Estar presentes sus componentes en las sesiones de formación y de pruebas.

Competencias:

- Conocimiento del “Plan de Continuidad de Negocio” implantado en la entidad.
- Conocimiento de los servicios prestados por la entidad.

Roles que lo conforman:

1. **Presidente del Comité de Gestión de Crisis:** El presidente del Comité es la persona encargada de dirigirlo, en compañía del resto de sus miembros, ya sean permanentes o condicionales. Sus responsabilidades serán las siguientes:

- Emitir instrucciones para dar respuesta sobre el terreno a incidentes menos relevantes, sin necesidad de convocar formalmente el Comité de gestión de crisis.
- Valorar la necesidad de convocar al Comité en caso de crisis o incidente.
- Evaluar la afectación del incidente.
- Declarar la activación/desactivación del “Plan de gestión de crisis” y de los diferentes planes asociados al incidente.

2. **Miembros del Comité de Gestión de Crisis:** Pueden ser miembros permanentes o condicionales de las diversas áreas organizacionales de la entidad, con la capacidad para poder asesorar adecuadamente al Presidente del Comité de gestión de crisis. Se debe asignar a un suplente para que realice las mismas funciones en caso de no estar disponible en cualquier momento que se requiera de su presencia y participación.

Las responsabilidades de los miembros permanentes del Comité son las siguientes:

- Participar en la evaluación de la afectación de la crisis.
- Asesorar en la toma de decisiones

3. DOCUMENTOS DE REFERENCIA:

- Guía de MinTIC para la definición de roles y responsabilidades
- Modelo de seguridad y privacidad de la información
- Procedimiento para la Gestión de incidentes de seguridad de la información
- Plan de continuidad del negocio versión 2

4. CONTROL DE CAMBIOS

VERSION	DESCRIPCION DE CAMBIOS
1.0	Elaboración del documento

5. VALIDACION DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: Diana Manrique Jasmín Herrera Cargo: Asesor externo Fecha: 13/04/23	Nombre: Carlos Gómez Aura Lucy Mora Cargo: Asesor Externo Fecha: 13/04/23	Nombre: Ingrid Solano Cargo: Jefe Oficina Asesora de Informática Fecha: 13/04/23