DISTRISEGURIDAD

TECNOLOGÍA, PREVENCIÓN, ARTICULACIÓN

Sistema Integrado De Gestión

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Código: MGTICS - 002

CARTAGENA DE INDIAS D. T. y C, 20 DE ENERO DE 2023

Este Plan Institucional fue socializado y aprobado mediante acta de Comité de Gestión y Desempeño – MIPG realizado los días 23 y 26 de enero de la presente vigencia.

OBJETIVOS

Objetivo General

Crear y gestionar un plan que permita controlar y minimizar los riesgos de seguridad y privacidad de la información, relacionados a los procesos TIC, existen en Distriseguridad Cartagena de Indias

Objetivos Específicos

Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.

Aplicar las metodologías del DAFP e ISO respectivamente en seguridad y riesgo de la información, para Distriseguridad Cartagena de Indias.

Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.

Definir los principales activos a proteger en Distriseguridad.

Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.

Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

Marco Legal

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.

MARCO TEÓRICO

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la ESAP.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La importancia de que las administraciones cuenten con un plan de tratamiento de riesgos de seguridad y privacidad de la información, este aporta la evidencia de los niveles de riesgos en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar a los funcionarios a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recurso.

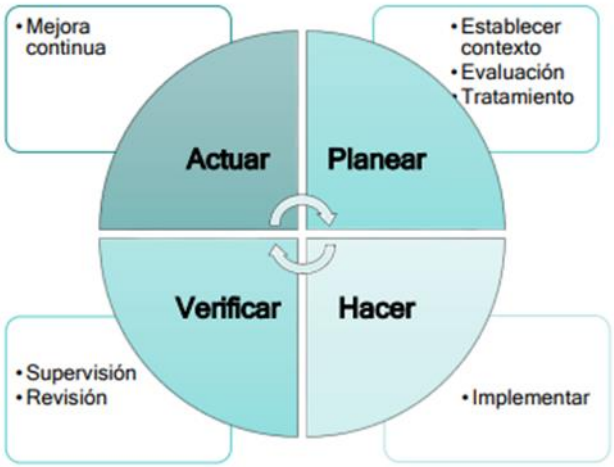
Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades

principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la metodología emitida por el Departamento Administrativo de la Función Pública, en su versión vigente. A continuación, se presenta las actividades generales para la implementación del Plan:

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

METODOLOGÍA DE IMPLEMENTACIÓN

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.



Plan (planificar): establecer el SGSI.
Do (hacer): implementar y utilizar el SGSI. Check (verificar): monitorizar y revisar el SGSI. Act (actuar): mantener y mejorar el SGSI.

ACTIVIDADES

- Realizar Diagnóstico
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y
- Privacidad de la Información.
- Valoración del riesgo y del riesgo residual.

- Realizar Mapas de calor donde se ubican los riesgos.
- Plantear al plan de tratamiento de riego aprobado por los líderes

CRONOGRAMA

Actividades	1	2	3	4	5	6	7	8	9	10	11	12
Elaborar el Diagnostico												
Elaborar el alcance del Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información												
Realizar la identificación de los riesgos con los líderes de los procesos												
Entrevista con los líderes de los procesos												
Valoración del riesgo residual												
Mapas de calor donde se ubican los riesgos												
Seguimiento y control												

SEGUIMIENTO y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con el Encargado de los Planes de la oficina de Distriseguridad y Oficina de control Interno para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

ENTREGABLES

- Informe de avances o resumen ejecutivo.
- Acta de reunión.
- Plan de tratamiento de riesgo aprobado por los líderes.
- Política Seguridad.
- Productos de cada etapa.

Glosario

Acceso a la Información Pública
Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin

restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de
2014, art 6).

Datos Personales

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información–SGSI, de la organización tras el resultado de los procesos de

evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO
27001. (ISO/IEC27000).

Derecho a la Intimidad

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos

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. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo
18 de la ley 1712 de 2014.

Información Pública Reservada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

Plan de continuidad del negocio

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

Privacidad

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL (Manual Estrategia Gobierno en línea) la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada

Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos

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. (Ley
1581 de 2012, art 3).

Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad (ISO 27000).

Riesgos

ID	ESCENARIO DE RIESGO	AMENAZA	VULNERABILIDAD
R1	Posibilidad de eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad	Tecnologico	Cronograma de Gestión TICS Diagnostico de Seguridad Digital Actualización de Política de Seguridad Digital
R2	Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación	Tecnologico	Diagnostico TICS Presupuesto TICS Oficio a la Dirección General y Dirección Administrativa y Financiera
R3	Posibilidad de ineficacia en los control de acceso.	Seguridad Digita	Cronograma de Gestión TICS Diagnostico de Seguridad Digital Actualización de Política de Seguridad Digita
R4	Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación	Financiero	Diagnostico TICS Presupuesto TICS Oficio a la Dirección General y Dirección Administrativa y Financiera

Revisar matriz de riesgo institucional página web

https://www.distriseguridad.gov.co/download/matriz-de-riesgos-planeacion-institucional/

PLANES DE ACCION

PLAN DE ACCION DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DESDE EL ENFOQUE DE SEGURIDAD INFORMATICA SOBRE LOS ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN			
No	. DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	TIEMPO
1	Diagnósticos de necesidades de TICS y solicitud de compra de bienes y soluciones TICS	TIC	feb-23
2	Elaboración Cronograma proceso de TICS	TIC	feb-23
3	Adquisición de Controles de Seguridad informática frente a Ciber amenazas	PLANEACION	may-23
4	Implementación de Controles de Seguridad Informática frente a Ciber amenazas	TIC	may-23
5	Actualizar la matriz de riesgo	TIC	ANUAL

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo corporativo que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

Atentamente,

ENRIQUE BRIEVA JURADO
PUE Planeación
Coordinador grupo de Trabajo TIC`s
Secretario técnico MIPG

Elaborado por: Ing. Victor Santiz P
Fecha de elaboración: 20/01/2023