Girón E.S.P

Empresa de Servicios Públicos de Girón s.a.s / e.s.p.

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

2024

TABLA DE CONTENIDO

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa Girón S.A.S. E.S.P., tiene como directriz general identificar y dar a conocer la implementación de un plan el cual concientice a los trabajadores, contratistas y usuarios en general del correcto tratamiento de la información teniendo siempre muy presente la privacidad de la información como objetivo principal.

Es importante no confundir el concepto relacionado de la "Seguridad de la Información" con el de la "Seguridad Informática", ya que mientras la primera se refiere a la protección y resguardo de la información integral de un sujeto (Persona, Empresa, Institución, Organismo, Sociedad, Gobierno), la segunda solo se centra en salvaguardar los datos dentro de un sistema informático como tal.

La humanidad se ha visto envuelta e inmersa en una serie de cambios en todas las áreas de la vida pública, todo a causa del desarrollo progresivo, creciente y masificado de las Tecnologías de Información y Comunicación (TIC). Este nuevo término muy usual actualmente como lo son las TIC ha originado efectos que incluso, han cambiado nuestra forma de ver apreciar o evaluar nuestro pasado o presente, y hasta redimensionado la forma en la que vislumbramos nuestro futuro como sociedad.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la Empresa Girón S.A.S. E.S.P., con el fin de Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la empresa con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

1.2. OBJETIVOS ESPECIFICOS

- Orientar a los funcionarios y contratistas que trabajan para Girón S.A.S. E.S.P. acerca de la importancia que tiene el Tratamiento de Riesgos de Seguridad y Privacidad de la Información para disminuir los riesgos asociados a la misma.
- Controlar y mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, a través de las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para este plan.

1.3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y su política, son aplicables a todos los trabajadores de la empresa Girón S.A.S. E.S.P., a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad, contratistas y terceras partes, que usen activos de información que sean propiedad de la entidad.

Con este plan se formularán lineamientos y estrategias básicas para orientar la minimización en materia de riesgos, y uso correcto de la información tanto personal como de la entidad.

2. MARCO NORMATIVO

- **Ley 527 de 1999**: Por medio de 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.

- **Decreto 1122 de 1999**: Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fé.

- **Ley 962 de 2005**: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

- **Decreto 1151 de 2008**: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan 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.

- **Decreto 235 de 2010**: Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

- **Conpes 3670 de 2010**: Lineamientos de política para la continuidad de los programas de acceso y servicio universal a las tecnologías de la información y las comunicaciones.

- **Conpes 3701 de 2011**: Lineamientos de política para ciberseguridad y ciberdefensa.

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

- **Ley 1712 del 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.

- **Decreto 2573 de 2014**: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- **Decreto 0103 de 2015**: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- **Decreto 415 de 2016**: Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.

3. TÉRMINOS Y DEFINICIONES

- **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 controle en su calidad de tal.

- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

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

- **Confidencialidad**: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).

- **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 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, los datos biométricos. (Decreto 1377 de 2013, art 3).

- **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).

- **Disponibilidad**: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

- **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).

- **Estimación del riesgo**: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- **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. (Ley 1712 de 2014, art 6).

- **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. (Ley 1712 de 2014, art 6).

- **Integridad**: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).

- **Partes interesadas (Stakeholder)**: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **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.

- **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

- **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).

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Transferencia del riesgo:** Compartir con otra de las partes la pérdida o la ganancia de un riesgo. Nota: En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la transferencia del riesgo.

- **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/IEC 27000).

4. RECURSOS

La empresa Girón S.A.S. E.S.P., teniendo en cuenta que un recurso es una fuente o suministro del cual se produce un beneficio, y que comúnmente los recursos son materiales u otros activos que son transformados para producir un beneficio, a continuación, se relacionan los recursos necesarios:

- Humano: Junta Directiva, Gerente General, Directivos, Profesionales Universitarios, Apoyo y Líderes de los Procesos.
- Físico: Servidores, Firewall, PC y equipos de comunicación.

- Financiero: Plan de Adquisiciones.

5. METODOLOGÍA DE LA IMPLEMENTACIÓN

La empresa Girón S.A.S. E.S.P., implementará como metodología el ciclo PHVA (Planear – Hacer – Verificar – Actuar), que es una herramienta de mejora continua, permitiendo en la entidad una mejora integral de la competitividad y del servicio con el objetivo de optimizar continuamente la calidad ofrecida a los usuarios, aumentar la productividad y generar a través de las nuevas tecnologías la rentabilidad de la empresa.

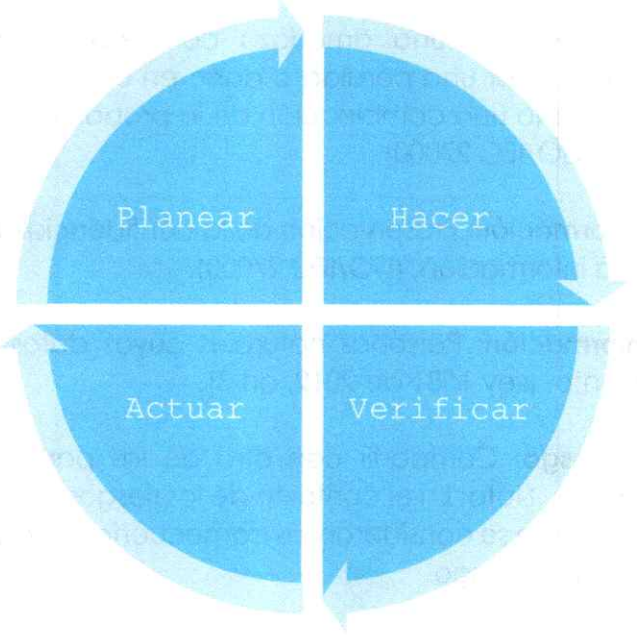

Fig. 1. Ciclo PHVA

6. ACTIVIDADES PARA LA IMPLEMENTACIÓN

- Realizar Diagnóstico.
- Implementar políticas enfocadas a la seguridad de la Información.
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- Realizar Inventario de Activos de Información con los líderes de cada Proceso.
- Realizar la Valoración de los Activos de Información con los líderes de cada Proceso.

- Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual).
- Socializar el Plan de Tratamiento de Riesgo.
- Realizar seguimiento del Plan de Tratamiento de Riesgo.

INDENTIFICACIÓN DEL RIESGO			SEGUIMIENTO PLAN DE TRATAMIENTO		
FACTOR DE RIESGO	**CAUSA**	**RIESGO**	**PLAN DE ACCIÓN**	**RESPONSABLE**	**SEGUIMIENTO**
Uso de dispositivos de almacenamiento de información externos en los equipos de la empresa	Falta de implementación y socialización de la política de seguridad de la información de la empresa	Pérdida de información por un error humano, un borrado accidental o provocado y violación a la confidencialidad de datos institucionales	Realizar una socialización al personal con acceso a un equipo de cómputo propiedad de la empresa con el fin de dar a conocer la Política de Seguridad de la Información de la entidad y hacer el seguimiento a su aplicabilidad	Sistemas e Informática	Semestral
Uso inadecuado y desactualización de los equipos de cómputo y demás dispositivos electrónicos de la empresa	Falta de procedimiento, control y asignación de responsabilidades a empleados a cargo de uno o más dispositivos electrónicos dados para poder llevar a cabo su labor. El acelerado paso en la innovación de los equipos y la modernización de Infraestructura y Nuevas Tecnologías en el mercado	Pérdida de información, mal funcionamiento del dispositivo electrónico a causa de actualizaciones no soportadas y dada de baja del equipo por daño o culminación de su vida útil	Realizar una socialización del buen uso de los dispositivos electrónicos al personal de la empresa. Dar cumplimiento al cronograma de mantenimientos preventivos establecido por el área de Sistemas e Informática para el año	Sistemas e Informática	Semestral
No realizar copias de seguridad y respectivo almacenamiento de los Sistemas de información propiedad de la entidad	Error en el procedimiento de copias de seguridad en el servidor por factores externos o humanos, entre otros. Disponibilidad de	Pérdida de información por un error humano, un borrado accidental, provocado o por desastre natural	Dar cumplimiento al procedimiento de copias de seguridad establecido por el área de Sistemas e	Sistemas e Informática	Semestral

	los recursos físicos para el almacenamiento de las copias de seguridad como CD, discos de almacenamiento		Informática para el año		
Afectación operacional y pérdida de información de cómputo	Falta de controles adecuados para la condiciones ambientales y conservación de la información ante desastres naturales, actos mal intencionados y demás factores de riesgo. Falta de reglamentación y el cumplimiento de normas por parte del responsable de la Seguridad y Salud en el Trabajo	Pérdida de información provocada por las malas condiciones ambientales, desastre natural o actos mal intencionado. Afectación de las operaciones administrativas y financieras de la entidad	Implementar la reglamentación y el cumplimiento de normas por parte del responsable de la Seguridad y Salud en el Trabajo	Sistemas e Informática / Dirección Administrativa y Financiera	Semestral

Tabla 1. Actividades para la implementación

7. CUMPLIMIENTO DE IMPLEMENTACIÓN

Para dar el total de cumplimiento de la implementación de la metodología mencionada anteriormente, se exponen las siguientes actividades y tareas a desarrollar de acuerdo con lo establecido por la empresa:

- Implementar la Política de Seguridad de la información.
- Implementar la Política de Administración de datos.
- Implementar las Políticas de Comunicaciones.
- Aspectos organizativos de la seguridad de la información.
- Seguridad de la Información enfocada a los recursos humanos.
- Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
- Revisión de los Controles de acceso.
- Gestión de Incidentes de Seguridad de la Información

8. CRONOGRAMA

N°	ACTIVIDAD	RESPONSABLE	FECHA TENTATIVA IMPLEMENTACIÓN
1	Realizar diagnóstico	Profesional Universitario y/o apoyo	Junio 2024
2	Implementar políticas enfocadas a la seguridad de la información	Profesional Universitario / Control Interno	Marzo 2024
3	Elaborar el alcance del plan de tratamiento de riesgos de seguridad y privacidad de la información	Apoyos TIC	Octubre 2024
4	Riesgos (Riesgo Inherente y Riesgo Residual)	Apoyos TIC	Octubre 2024
5	Realizar seguimiento del Plan de Tratamiento de Riesgo	Control interno	Noviembre 2024
6	Socializar el Plan de Tratamiento de Riesgo	Profesional Universitario / Control Interno	Noviembre 2024

Tabla 2. Cronograma

9. SEGUIMIENTO

La empresa Girón S.A.S. E.S.P., evaluará el desempeño del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información a través de la revisión de las acciones que se están llevando a cabo y evaluará la eficiencia en su implementación, adelantando verificaciones y seguimientos al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

10. MONITOREO

El monitoreo al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información debe estar a cargo del Control Interno y la Dirección Administrativa y Financiera, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo.

El constante seguimiento a los procesos y la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información deben ser ejecutados, monitoreados y actualizados constantemente. Por tal motivo es importante implementar dicho plan toda vez que su implementación permite prevenir posibles riesgos y amenazas encontradas en infraestructura tecnológica de la Entidad.

11. BIBLIOGRAFÍA

- https://www.funcionpublica.gov.co/web/mipg
- https://www.gironsantander.gov.co/Transparencia/Paginas/Planeacion-Gestion-y-Control.aspx
- https://www.funcionpublica.gov.co/planeacion-sectorialinstitucional