

# PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y

2019



## PRIVACIDAD DE LA INFORMACION

## INTRODUCCION

La información de EMPODUITAMA, se considera como un activo decisivo para el desarrollo de sus procesos, su correcto desempeño dentro de la política y su relación con el ciudadano es por ello que debe ser protegida de cualquier posibilidad de eventos que generen un potencial riesgo de seguridad de la información y que pudiese dar como resultado en un impacto indeseado generando una consecuencia negativa para el normal desarrollo de las actividades de la entidad.

### OBJETIVOS

#### Objetivo General

Generar los lineamientos de administración de riesgos de seguridad de la información

#### ALCANCE

Inicia con la identificación del riesgo y termina con el seguimiento de los controles. Aplica a todos los procesos de la entidad.

#### 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 esta (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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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).

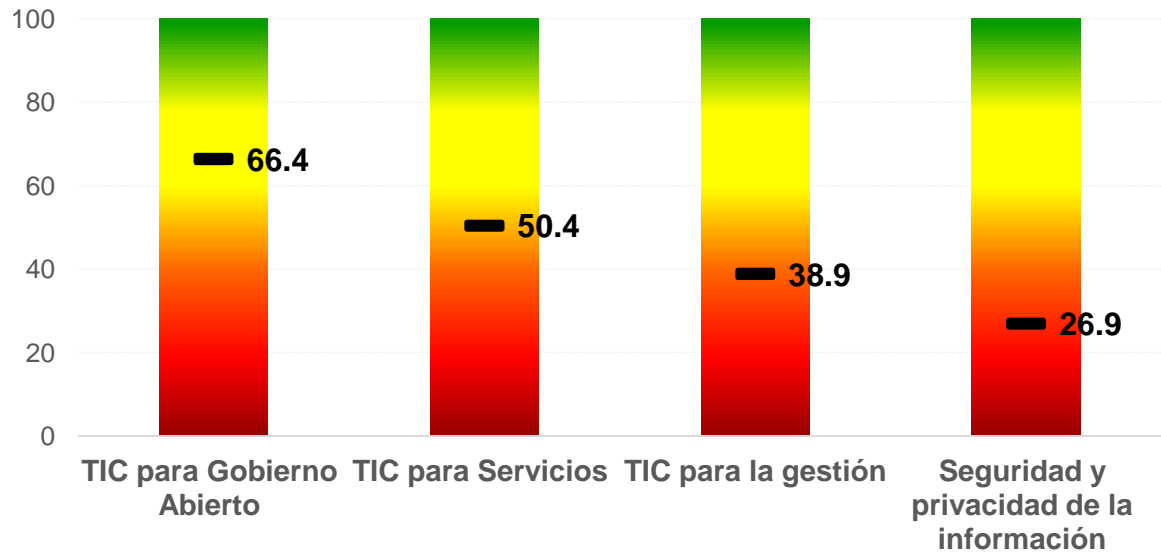
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **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. (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)
- **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 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/IEC 27000).

## DIAGNOSTICO

En el mes de Noviembre se realizó el auto diagnóstico determinado por el DAFP y gobierno digital del ministerio de tecnologías de la información, y como resultado se obtuvieron los siguientes puntajes por componente:



Luego de realizar la medición se llegó a las siguientes conclusiones:

- Existe un procedimiento de administración del riesgo en la plataforma que administra el sistema integrado de gestión de la entidad **SIG "F-GGR-07 ADMINISTRACION DEL RIESGO"**, pero no especifica claramente los pasos para administrar riesgos de seguridad de la información
- A la fecha no existe un inventario de activos de información y no existe una metodología clara sobre su identificación
- No existe un seguimiento a dichos riesgos de seguridad y privacidad de la información.
- Existen algunas buenas prácticas en materia de seguridad de la información efectuadas por la oficina de sistemas de la entidad

## ACTIVIDADES DEL PLAN

### ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- **Alta Dirección:** aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.
- **Proceso Administración del Sistema Integrado de Gestión:** Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

- **Responsables de los procesos:** Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.
- **Servidores públicos y contratistas:** ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.
- **Control Interno:** debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

## **POLITICA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES**

Con el fin de cumplir con este plan EMPODUITMA se compromete a el cumplimiento de los siguientes puntos, por parte de todos los integrantes del equipo de trabajo de la entidad.

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- f) Actualizar la información dentro de los cinco (5) días hábiles contados a partir de su recibo, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
- g) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.
- h) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
- i) Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley.

- j) Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- k) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- l) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- m) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
- n) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- o) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
- p) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.
- q) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- r) Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley.
- s) Informar a solicitud del Titular sobre el uso dado a sus datos.
- t) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
- u) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Para el cumplimiento de los puntos anteriores la dirección debe destinar los recursos necesarios en cuanto a los recursos humanos, financieros y tecnológicos, y garantizar el plan de seguimiento y evaluación.

#### **CRONOGRAMA DE ADMINISTRACION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

<b>ACTIVIDAD</b>	<b>Ene</b>	<b>Feb</b>	<b>Mar</b>	<b>Abr</b>	<b>May</b>	<b>Jun</b>	<b>Jul</b>	<b>Ago</b>	<b>Sep</b>	<b>Oct</b>	<b>Nov</b>	<b>Dic</b>
Realizar Autodiagnóstico												
Actualizar procedimiento de administración de riesgos												
Identificar, valorar, determinar controles, seguimiento y evaluar controles												





Identificar riesgos residuales y definir opciones de manejo													
Hacer seguimiento a riesgos													

## RIESGOS

- Identificación errónea de los riesgos
- Incumplimiento del cronograma, políticas, roles.
- No aplicación de controles definidos

## LINEAMIENTOS GENERALES DEL PLAN

1. Cualquier cambio al cronograma deberá ser aprobado por el comité institucional de gestión y desempeño.
2. Se hará seguimiento a las actividades en los 10 días calendario después de cada trimestre
3. El profesional especializado de sistemas deberá establecer mecanismos para hacer el seguimiento de estas actividades y verificar que se hayan cumplido adecuadamente

## SOCIALIZACIÓN

El presente Plan será socializado a funcionarios y usuarios de EMPODUITAMA S.A. E.S.P y Publicado en la página web de la entidad antes del 31 de Enero del 2019.

## ANEXOS

SIG "F-GGR-07 ADMINISTRACION DEL RIESGO"

Versión 1- Copia controlada: La versión de este documento reposa en el SIG de la entidad 31-01-2019-Si el documento se encuentra impreso no se garantiza su vigencia