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

TABLA DE CONTENIDO

INTRODUCCIÓN

Es muy importante que la institución cuente con un Plan De Gestión de Riesgos para garantizar la continuidad del negocio. Por este motivo, se realizan las actualizaciones en análisis que tienen que ver con riesgos de seguridad de la información aplicados a la Empresa Social del Estado Región de Salud Soacha, donde se analiza la situación actual y se identifican los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir protecciones necesarias que podrían formar parte del Plan De Gestión De Riesgos en la Seguridad de la Información.

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del Negocio, le permite a la Empresa Social del Estado Región de Salud Soacha realizar la identificación, análisis y tratamiento a los riesgos que pueden comprometer el cumplimiento de los objetivos trazados a favor de todos los usuarios, contribuyendo en la toma de decisiones con el fin de prevenir la materialización de estos.

1 CAPÍTULO 1. GENERALIDADES

1.1 Objetivos

1.1.1 Objetivo general:

Desarrollar un Plan De Gestión De Seguridad y Privacidad De La Información, que permita minimizar los riesgos de pérdida de activos de la información en la Empresa Social de Estado Región Salud Soacha.

1.2 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.
- **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 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 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).

1.3 Alcances Y Limitaciones

1.3.1 Alcances

- Lograr el compromiso de la Empresa Social de Estado Región Salud Soacha para emprender la implementación del Plan De Gestión De Seguridad y Privacidad De La Información.
- Definir Roles y Responsabilidades para apoyar y asesorar el proceso de diseño e implementación del plan de gestión de seguridad y privacidad de la información, tomando como referencia la Guía No. 4 de MINTIC.
- Socializar al personal de la entidad en el proceso de Plan De Gestión De Seguridad y Privacidad De La Información.

1.3.2 Limitaciones

Los recursos económicos necesarios para apoyar la implementación del Plan De Gestión De Seguridad y Privacidad De La Información en la Empresa Social de Estado Región Salud Soacha.

1.4 Control De Cambios

FECHA	VERSIÓN	DESCRIPCIÓN
31/01/2023	00	Creación Documento
29/01/2024	01	Actualización

1.5 Gestión Del Riesgo

1.5.1 Importancia de la gestión del riesgo:

En el ámbito empresarial actual, se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas a nivel nacional e internacional.

La Empresa Social del Estado Región de Salud Soacha, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la Empresa Social de Estado Región Salud Soacha, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

1.5.2 Definición de la gestión del riesgo

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "**la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto cause daño a la organización**".

1.5.3 Identificación del riesgo

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento

de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- **Riesgos Operativos:** Comprende riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

1.5.4 Situaciones no deseadas

RIESGO TECNOLÓGICO	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	CALIFICACIÓN	EVALUACIÓN	MITIGACIÓN DEL RIESGO
Confidencialidad e Integridad de la información	Se promueve la campaña cero papel, sin embargo se han encontrado dentro del papel reutilizable información personal de algunos usuarios y/o funcionarios de la institución.	Exposición de datos personales en papel reutilizable.	Incumplimiento de confidencialidad e integridad de la información.	Riesgo de Información	60	Riesgo Alto	Socializar con los funcionarios de la entidad acerca de las políticas de seguridad y confidencialidad de la información.
Pérdida de información y/o deterioro físico	Los funcionarios no realizan copias de seguridad a la información producto de sus funciones. Equipos compartidos en algunas dependencias. Uso de memorias extraíbles y unidades extraíbles	No se realizan copias de seguridad. No existen cuentas de usuario individuales. No existe control de uso de memorias USB	Infección por Virus	Riesgo de Información Riesgo Tecnológico	60		Actualizar y socializar el proceso de copias de seguridad en equipos de cómputo a los funcionarios de la institución Adquirir un servidor para almacenar las copias de seguridad. Adquisición de una nube para almacenamiento de información.
Pérdida de información y/o deterioro físico	Pérdida de información y/o deterioro físico física está siendo archivada en sitios no adecuados para ello.	No se ha iniciado la ejecución de digitalización de información.	Daño de documentos y deterioro del papel.	Deterioro del papel.	40	Riesgo Importante	Iniciar la ejecución de la digitalización y almacenamiento de la información contenida en papel.
No hay respaldo de información en sistemas de información	No existe un proceso establecido de copias de seguridad dentro y fuera de la entidad para la información generada en los sistemas de información.	No hay procesos de copias de seguridad establecidos	Pérdida de información	Riesgo Tecnológico	60	Riesgo Importante	Crear procesos de copias de seguridad.
No hay respaldo de información en sistemas de información	No existe un sistema de información para la documentación sensible, como contratos y acuerdos.			Riesgo de información	60	Riesgo Importante	Invertir en un software o sistema de información para el almacenamiento y consulta de la documentación física existente en la institución.
Transición IPv4 a IPv6	No existen transición de protocolo de IP	No existen transición de protocolo de IP	No existen transición de protocolo de IP	Riesgo tecnológico	20	Riesgo Bajo	*establecer normas para la transición de IPv4 a IPv6 debido a que todos los equipos informáticos de la entidad soportan la nueva versión de IP

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión.
- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja cobertura de internet.
- Daño de equipos y de información
- Atrasos en la entrega de información
- Atrasos en asistencia técnica
- Fuga de información
- Manipulación indebida de información

1.5.5 Origen del plan de gestión

El Gobierno Nacional y el Ministerio de las TIC, han abandonado los proyectos de Gobierno en Línea, que permiten conocer el funcionamiento de las entidades públicas en el país, incluyendo las Empresas Sociales del Estado. Es por ello necesario que la Empresa Social de Estado Región Salud Soacha, cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a los usuarios y a los entes de control.

1.5.6 Propósito del Plan De Gestión De Riesgos De La Seguridad De La Información

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto o servicio.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

1.6 Análisis De Vulnerabilidades

1.6.1 Descripción de las vulnerabilidades

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Empresa Social de Estado Región Salud Soacha se encontraron otras amenazas e impactos como los siguientes:

- La red de internet implementada tanto en la sede principal como en centros y puestos de salud, no es la más adecuada teniendo en cuenta que la mayor parte de la red ha sido cableada en categoría 5 y 6, lo que hace que la señal se torne débil hacia algunas oficinas.
- Los puntos de red ubicados en cada oficina no son los suficientes y se han dispuesto nuevos según se va presentando la necesidad. No existe una estructura o protocolo fijo y establecido para la infraestructura física de la Empresa Social de Estado Región Salud Soacha.

- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada área, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada oportunamente.
- Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

  - Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.
  - En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
  - En algunas áreas de la Empresa Social de Estado Región Salud Soacha, no existen los equipos de cómputo suficientes para el uso de la totalidad del personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.
  - El Datacenter de la entidad requiere de algunas características importantes para cumplir con las normas de funcionamiento (alimentación eléctrica estabilizada e ininterrumpida, sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, piso falso entre otros).
  - La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.
  - No hay control para el uso de memorias portátiles en los equipos de la Empresa Social de Estado Región Salud Soacha, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
  - Se identificó un desconocimiento del tema de seguridad y privacidad de la información en la Empresa Social de Estado Región Salud Soacha.
  - No existe un Firewall para la red de la Empresa Social de Estado Región Salud Soacha, solo existe uno a través del PepLink, que es limitado para la cantidad de equipos y accesos de la institución.
  - No existe una herramienta tecnológica para el historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la E.S.E.
  - Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las áreas y servicios no son los adecuados.
  - Las copias de seguridad se están realizando únicamente en los equipos de cómputo priorizados y en el servidor institucional donde se manejan sistemas de Información DGH.NET.
  - Esta solución no es óptima, ya que existe riesgo de pérdida total de información en caso de ocurrir desastres naturales, incendios u otros que afecten las copias de respaldo almacenadas en el Servidor o Datacenter ubicado dentro de la misma entidad.
  - No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la entidad. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores).

- La Empresa Social de Estado Región Salud Soacha cuenta con una planta de energía que en la actualidad solo cubre la sede asistencial principal, en consecuencia, se presentan riesgos de pérdida de información por los cortes de energía en los procesos asistenciales y administrativos en las diferentes áreas.

1.7 Metodología de la implementación

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Empresa Social de Estado Región Salud Soacha, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos. De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

- Diagnosticar
- Planear
- Hacer
- Verificar
- Actuar

1.8 Actividades

- Realizar Diagnóstico.
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- Realizar la Identificación de los Riesgos con los líderes del Proceso.
  - Entrevistar con los líderes del Proceso.
- Valorar 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.

1.9 Cumplimiento de la implementación

De acuerdo a las fases mencionadas anteriormente, se describe a continuación las actividades que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el proceso de sistemas de la Empresa Social de Estado Región Salud Soacha.

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

1.10 Cronograma

ACTIVIDADES		TRIMESTRE I						TRIMESTRE II						TRIMESTRE III						TRIMESTRE IV					
		ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC	
ÁREA	ACTIVIDAD	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN	1, Plan de tratamiento de Riesgos SGSI (En cumplimiento al Plan 12 del Debreto 612 MIPG)	P																							
	2, Realizar el seguimiento o controles de funcioncionabilidad de herramienta implementada para la minimización del riesgo (Instructivo No. 1 - Instructivo Instrumento de Evaluación MSPI)							P						P						P				P	

ACTIVIDADES		Responsable	Evidencias
ÁREA	ACTIVIDAD		
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN	1, Plan de tratamiento de Riesgos SGSI (En cumplimiento al Plan 12 del Debreto 612 MIPG)	REFENTE TICS	Entrega del Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información
	2, Realizar el seguimiento o controles de funcioncionabilidad de herramienta implementada para la minimización del riesgo (Instructivo No. 1 - Instructivo Instrumento de Evaluación MSPI)	REFENTE TICS	Diligenciamiento de la herramienta de Diagnostico de Seguridad y Privacidad de la Información. Informe de Diagnostico en el que se identifican los riesgos de seguridad y privacidad de la información.
		REFENTE TICS	
		REFENTE TICS	