PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2024

CONTROL DE CAMBIOS

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Elaboración y emisión de diagnostico	16/05/2022
05	Actualización	30/01/2024

	ELABORÓ	REVISÓ	APROBÓ
FECHA	30/01/2024	30/01/2024	30/01/2024
FIRMAS	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL
NOMBRE	YEILER EDUARDO BERNAL GUTIERREZ	OSCAR DARIO SOLER MORALES	DIEGO FERNANDO FUQUEN F.
CARGO	Líder de Gestión de la Tecnología	Asesor de planeación	Subgerente Administrativo y Financiero

INTRODUCCIÓN

El HOSPITAL REGIONAL DE SOGAMOSO E.S.E instaura el plan de tratamiento de riesgos de seguridad de la información como medida para mitigar los riesgos presentes en la institución los cuales se pueden clasificar como: perdida de la información, perdida de confidencialidad, integridad y disponibilidad de datos, evitando de esta manera la interrupción de los procesos de la entidad. Teniendo en cuenta que uno de los activos más importantes del HRS es la información, en base a lo anterior se genera la necesidad de mejorar las prácticas y normativas en la planificación, implementación, gestión y mejoramiento continuo de seguridad y privacidad en la información.

Este plan define el tratamiento del riesgo con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, de igual manera establece los lineamientos y respuestas para atender en forma oportuna, ante la posible pérdida, destrucción o robo de la información. Tanto el Hardware como el Software están expuestos a diversos Factores de Riesgo Humano y Físico. Pueden originarse pérdidas de información catastróficas, bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que pueden producir daño físico irreparable.

Las siguientes medidas se definen teniendo en cuenta la información suministrada mediante el análisis de los riesgos establecidos, y las necesidades del proceso de Gestión de la información y tecnología del HOSPITAL REGIONAL DE SOGAMOSO E.S.E, en cuanto a la seguridad de la información y proporciona las herramientas necesarias para identificar las medidas de corrección de riesgos y su ejecución en la institución.

2. OBJETIVOS

2.1. General

Identificar y establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, para preservar la confidencialidad, integridad y disponibilidad de la información, El plan de tratamiento de riesgos de la seguridad y privacidad de la información integra una estrategia con el fin de puntualizar y aplicar los lineamientos para manejar de forma integral los riesgos de seguridad digital que el HRS pueda estar expuesto.

2.2. Específicos

1. Actualizar e implementar las políticas de seguridad y privacidad del Hospital.
2. Promover el uso de mejores prácticas de seguridad de la información en la Institución.
3. Optimizar la gestión de la seguridad de la información al interior de la Institución.
4. Evaluar, analizar, prevenir y solucionar los riesgos de seguridad informática que se presentan en el HOSPITAL REGIONAL DE SOGAMOSO E.S.E.
5. Implementar un plan para orientar y planificar el monitoreo, gestión e implementación de los riesgos en seguridad y privacidad de la información.
6. Sensibilizar y capacitar a todos los funcionarios de la Institución en la formulación e implementación de controles y acciones encaminadas a prevenir los riesgos de la seguridad y privacidad de la información.
7. Fortalecer la cultura de seguridad y privacidad de la información en los funcionarios, personal en misión, usuarios externos.
8. Garantizar la seguridad y la privacidad de la información.

3. ALCANCE

La política de seguridad establecida por el HOSPITAL REGIONAL DE SOGAMOSO E.S.E aplica a toda la institución, sus colaboradores, contratistas y practicantes, que tengan acceso a la información del mismo, a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación del ente.

4. NORMATIVIDAD

4.1. 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: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.
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/IEC27000)
Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo (ISO/IEC27000)
Auditoria: 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)
Criterios del riesgo: Termino de referencia frente a los cuales la importancia de un riesgo se evalúa.
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.

Confidencialidad: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

Datos abiertos: Son todos aquellos datos primarios o con 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 a que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, 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)

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

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.

Evaluación del riesgo: Proceso de comparación de los resultados del análisis de riesgo, para evaluar, y determinar su magnitud o si son aceptables o tolerables.

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).

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la información pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorias de los sistemas integrados de gestión.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimizarían o cifrado.
Nivel del riesgo: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la clasificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
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).
Política de la seguridad de la información: Es el componente principal para la puesta en marcha del modelo de seguridad y privacidad de la información, y unos de los requisitos del Sistema de Gestión de Seguridad de la Información, es el documento que contiene objetivo, aplicabilidad, alcance, principios, nivel de cumplimiento, fundamentos, roles y responsabilidades que se requieren como requisito para la implementación del sistema de gestión de la seguridad de la información.
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.
Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a tratamiento que operan en el país (Ley 1581 de 2012, art 25).
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 2700).
Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

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).

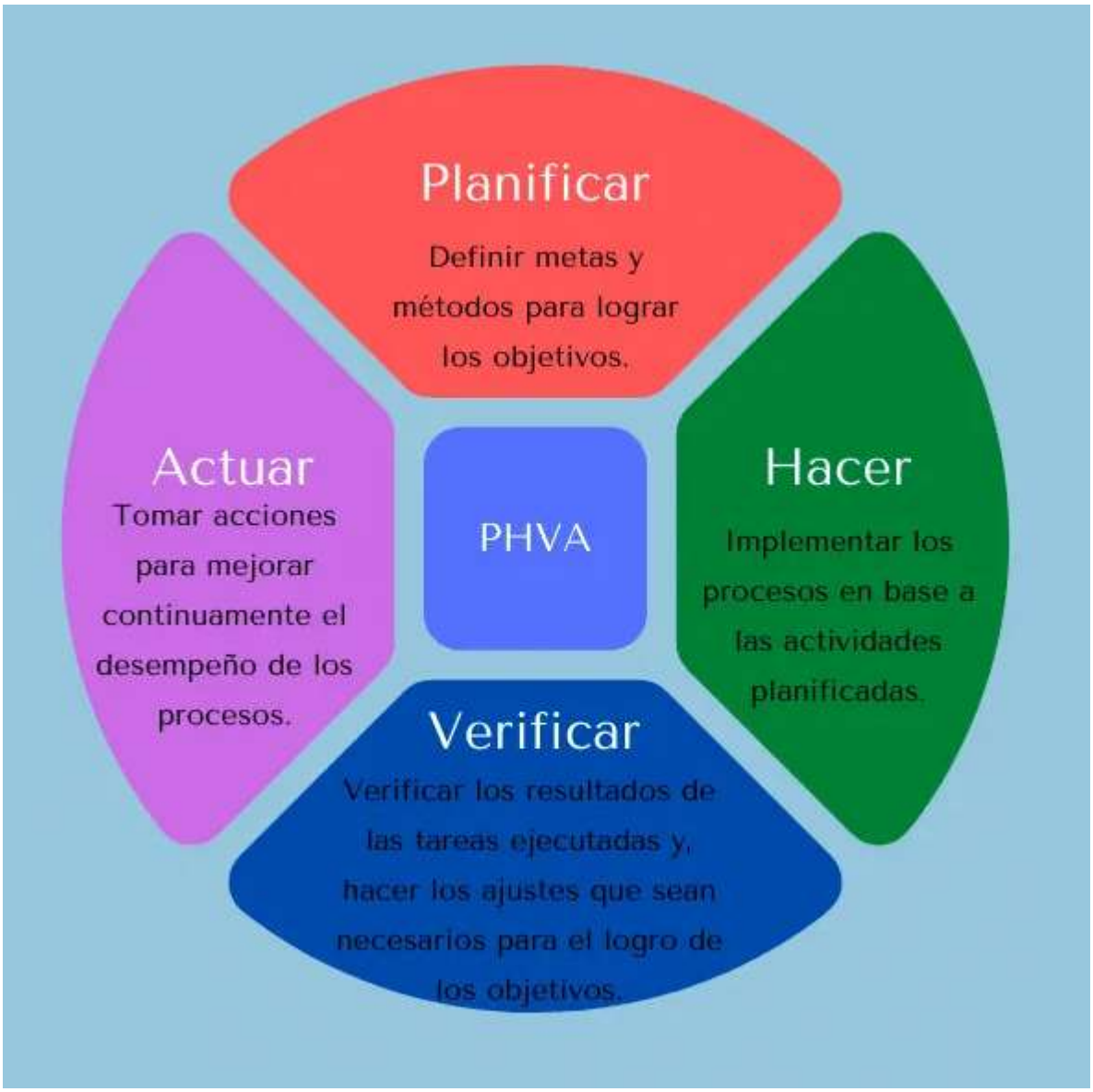
Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000).

4.2. MARCO NORMATIVO

- Resolución 3564 de 2015, reglamenta aspectos relacionados con la Ley de Transparencia y acceso a la información pública.
- Decreto reglamentario único 1081 de 2015, reglamento sobre la gestión de la información pública.
- Decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.
- Ley 1712 de 2014, Ley de transparencia y acceso a la información pública.
- Acuerdo 03 de 2015 del Archivo General de la nación, lineamientos generales sobre la gestión de documentos electrónicos.
- Ley Estatutaria 1581 de 2012, protección de datos personales.
- Ley 1266 de 2008, disposiciones generales de habeas data y se regula el manejo de la información.

5. DESARROLLO DEL PLAN O PROGRAMA

La implementación del sistema de gestión de seguridad y privacidad de la información, toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar), el modelo MSPI del Ministerio de Tecnologías de la información y las Comunicaciones, el modelo integrado de planeación y gestión MIPG y la norma ISO 27001:2013.



Fase de Diagnostico:

Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
Determinar el nivel de madurez de los controles de seguridad de la información.

Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
Identificación del uso de buenas prácticas en ciberseguridad.

Fase de planificación:

De acuerdo a los resultados de la etapa anterior, se procede a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la Institución, con el propósito de definir acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.
El alcance del MSPI permite al Hospital Regional de Sogamoso E.S.E definir los límites sobre los cuales se implementará la seguridad y privacidad. Este enfoque es por procesos y debe extenderse a toda la institución. Para desarrollar el alcance y los límites del modelo se deben tener en cuenta las siguientes recomendaciones: procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo de procesos.

Fase de implementación:

Esta fase le permitirá al Hospital, llevar a cabo la implementación de la planificación realizada en fase anterior del MSPI.

Fase de evaluación de desempeño:

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Fase de mejora continua:

En esta fase el Hospital debe consolidar los resultados obtenidos de la fase de la evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

Proyectos vigencia 2024

Para la vigencia 2024 se llevarán a cabo la ejecución de los siguientes proyectos de seguridad de la información dentro del Hospital Regional de Sogamoso.

NOMBRE	IMPLEMENTAR EL PROGRAMA DE CAPACITACION Y SENSIBILIZACION EN SEGURIDAD DE LA INFORMACION
DESCRPCION	Se busca capacitar al 100 por ciento de funcionarios y colaboradores del HOSPITAL REGIONAL DE SOGAMOSO en las políticas de seguridad y privacidad de la información, buenas prácticas, amenazas y controles en un entorno físico y digital
FECHA INICIO	MAYO - OCTUBRE 2024

NOMBRE	IMPLEMENTACION SEGURIDAD PERIMETRAL
DESCRPCION	Tiene como objetivo la protección informática de los sistemas y dispositivos conectados a la red de ataques y así poder controlar el tráfico de internet externo e interno en el Hospital Regional de Sogamoso.
FECHA INICIO	FEBRERO 2024

NOMBRE	ANTIVIRUS
DESCRPCION	Tiene como objetivo proteger a los equipos de computo de ataques de software malicioso complementando el proyecto de seguridad perimetral creando un sistema de seguridad informática robusto y seguro.
FECHA INICIO	FEBRERO 2024

NOMBRE	PAGINA WEB
DESCRPCION	Tiene como objetivo mantener informado a la comunidad y usuarios de la institución de todas las novedades y políticas que el hospital presenta
FECHA INICIO	MARZO 2024

6. Líneas de estrategias del plan e indicaciones.

Fortalecer a un nivel optimizado, controles del sistema de gestión de la información.

- Componente GEL: TIC para la gestión.
- Dominios del marco TI: Servicios tecnológicos, uso y apropiación.
- Objetivo estratégico institucional: Garantizar un sistema de información integral, eficiente y eficaz.

Implementar estrategias de sensibilización en seguridad de la información.

- Componente GEL: TIC para la gestión.
- Dominios del marco TI: Servicios tecnológicos, uso y apropiación.
- Objetivo estratégico institucional: Garantizar un sistema de información integral, eficiente y eficaz.

Proponer por la comunidad, funcionamiento, disponibilidad de los sistemas de la información misionales y de apoyo.

- Componente GEL: TIC para la gestión.
- Dominios del marco TI: Sistema de información, servicios tecnológicos, gestión de la información, uso y apropiación.

- Objetivo estratégico institucional: Garantizar un sistema de información integral, eficiente y eficaz.

Indicadores:

Porcentaje de ejecución de las actividades de ejecución del plan de la vigencia.
Formula: (N° de actividades ejecutadas / N° de actividades programadas) * 100.
Frecuencia de medición: Semestral

7. Plan de seguimiento.

El seguimiento del presente plan será verificado semestral, de tal manera que se haga el respectivo monitoreo y actualización según se determine la necesida

8. Oportunidad de mejora:

Los riesgos que se identifiquen durante la ejecución del plan deberán ser mitigados y monitoreados constantemente, además se deberán actualizar los recursos tecnológicos de la entidad de manera regular siempre y cuando la demanda lo requiera.

	HOSPITAL REGIONAL DE SOGAMOSO E.S.E	CÓDIGO: D-PI-FT-001
	PLAN OPERATIVO ANUAL	VERSIÓN: 02
	FORMATO	FECHA: 30/12/2020
		PÁGINA:

Nombre del Proceso: Gestión de Recursos Informáticos

Objetivo del Proceso: Planificar el desarrollo institucional del Hospital Regional de Sogamoso E.S.E. en el corto, mediano y largo plazo, mediante la formulación, ejecución, seguimiento, monitoreo y evaluación de planes, programas y proyectos, con el fin de garantizar el cumplimiento de objetivos y metas establecidas.

Líder del Proceso: Yeiler Eduardo Bernal Gutiérrez | **Fecha de Elaboración:** | **30/01/2024**

ÍTEM	OBJETIVO	META	ACTIVIDAD	INDICADOR	EJECUCIÓN	RESPONSABLE DE LA ACTIVIDAD	EVIDENCIA DE LA ACTIVIDAD	INCLUIDO EN EL PAA		PRESUPUESTO
					ENERO (sem 1–4) · FEBRERO (sem 1–4) · MARZO (sem 1–4) · ABRIL (sem 1–4) · MAYO (sem 1–4) · JUNIO (sem 1–4) · JULIO (sem 1–4) · AGOSTO (sem 1–4) · SEPTIEMBRE (sem 1–4) · OCTUBRE (sem 1–4) · NOVIEMBRE (sem 1–4) · DICIEMBRE (sem 1–4)			SI	NO	
1	Administrar el nivel de seguridad y privacidad y definir las accionesa implementar en el Hospital Regional de Sogamoso	Fortalecer y Proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada	Actualizar la política de seguridad y privacidad de la información	Resolución política Actualizada		**Líder Gestión de Recursos informáticos**	Documento manual de políticas de seguridad y privacidad informática		X	
			Actualizar el inventario de activos de información	numero de dependencias a los que se le identifico activos de información/ total de dependencias de la entidad * 100		**Líder Gestión de Recursos informáticos**	Documento metodología de gestión de activos de información		X	
			Realizar el diagnostico e implementación estrategia de transición de IPv4 A IPv6	Documento de diagnostico e implementación del protocolo de internet IPV6		**Líder Gestión de Recursos informáticos**	Documento del plan de diagnostico y estrategia de transición de IPv4 a IPv6	X		**$ 70.000.000**
			sensibilización y capacitación en lo referente a seguridad y privacidad de la información	Numero de personas a las que se evaluó la política de seguridad y privacidad de la información/ total de personas que laboran en misión en la institución		**Líder Gestión de Recursos informáticos**	Listado de asistencia a la sensibilización y capacitación en lo referente a seguridad y privacidad de la información		X	
			Realizar la renovación tecnológica del sistema de seguridad perimetral de la institución.	Documento de renovación del sistema de seguridad perimetral de la institución.		Líder de Gestión de Recurso Informático	Justificación técnica y Contrato.	X		**$ 50.000.000**
			Actualización COLCERT e intercambio de información de seguridad.	Reporte de envió de información al COLCERT		Líder de Gestión de Recurso Informático	Documento COLCERT e intercambio de información de seguridad.		X	

Elaboró

FIRMADO EN ORIGINAL

Yeiler Eduardo Bernal Gutierrez
Líder Oficina de sistemas

Revisó

FIRMADO EN ORIGINAL

Oscar Dario Soler Morales
Líder de Planeación

FIRMADO EN ORIGINAL

Sheyla Fanory Caicedo Rincón
Gerente