1. INTRODUCCIÓN:

En EMPOCALDAS S.A. E.S.P. se busca fomentar la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra la confidencialidad, integridad y disponibilidad, con la implementación de medidas de control de seguridad, que permitan gestionar y reducir los riesgos e impactos a que está expuesta para lograr el máximo retorno de las inversiones en las oportunidades de negocio.

Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

EMPOCALDAS S.A. E.S.P. decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad y privacidad de la información aprobada por el Comité Institucional de Gestión y Desempeño, y como medio o herramienta para el logro de los objetivos de mantener la información confidencial, integra y disponible, a través de su ciclo de vida, desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- ***Confidencialidad****:* Propiedad que la información sea concedida únicamente a quien esté autorizado.
- ***Integridad****:* Propiedad que la información se mantenga exacta y completa.
- ***Disponibilidad****:* propiedad que la información sea accesible y utilizable en el momento que se requiera.

2. ALCANCE

La gestión de Riesgos de Seguridad de la Información y su Tratamiento, será aplicada en todos los niveles sobre todos los procesos de EMPOCALDAS S.A. E.S.P., a cualquier activo de información como hardware, software, servicios, componentes de red, personas, instalaciones o cualquier otro aspecto en particular de control de la Empresa, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la

información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Desarrollar un plan de tratamiento de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad que permita garantizar la operación normal de la organización, minimizar la probabilidad e impacto de los riesgos, minimizar la materialización de los riesgos de seguridad de la información y la pérdida de activos de la información en la empresa de Obras Sanitarias de Caldas EMPOCALDAS S.A. E.S.P.

3.2. OBJETIVOS ESPECÍFICOS:

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación a que Empocaldas S.A. E.S.P. pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

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

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

- Definir los principales activos a proteger en EMPOCALDAS S.A. E.S.P.

- Identificar las principales amenazas que afectan a los activos.

- Aplicar controles que permitan minimizar la materialización de los riesgos a los que está expuesto cada activo.

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

4. TÉRMINOS Y DEFINICIONES

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo es evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

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

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

5. GESTIÓN DE RIESGOS

5.1. IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial 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 del mundo.

EMPOCALDAS S.A. E.S.P. sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno Digital que viene impulsando actividades dentro de las Empresas públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información.

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 Empresa sin un plan de tratamiento de riesgos está expuesta a perder su información.

El plan de tratamiento de riesgos y seguridad se implementa para identificar los posibles conflictos que podrían estar afectando 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 confidencialidad, disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

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 empresa.

5.2. DEFINICIÓN 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 causa daño a la organización”.

Para el tratamiento de los riesgos de seguridad de la información, tomando como referente la guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) de diciembre de 2020, se define la operatividad institucional para la administración del riesgo según la siguiente figura.

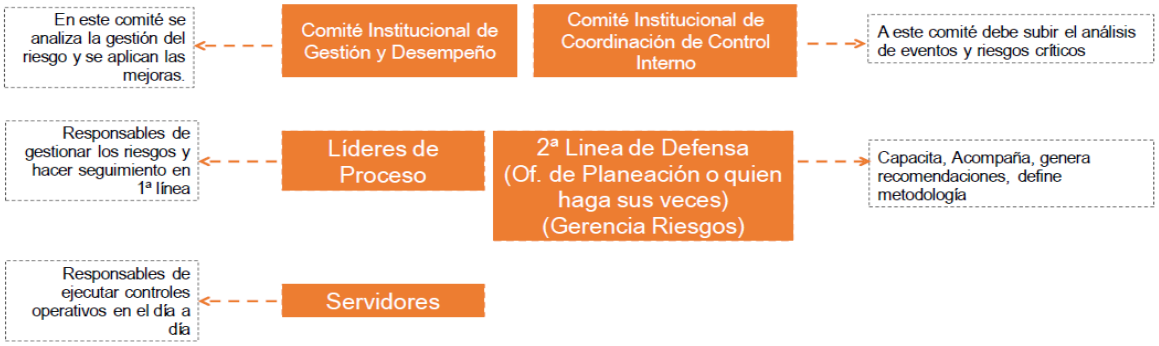

Figura 1: Operatividad Institucionalidad para la Administración del Riesgo - Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

5.3. PROPÓSITO DEL PLAN DE GESTIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dar soporte al modelo de seguridad de la información al interior de la Empresa.
- 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 un servicio o un mecanismo.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

5.4. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de EMPOCALDAS S.A. E.S.P. y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación y aplicación de controles en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

5.5. CRITERIOS DE EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Empresa.

6. ESTRUCTURA METODOLÓGICA

EMPOCALDAS S.A E.S.P siguiendo los lineamientos de la Guía para la Administración del Riesgo y Diseño de Controles en las entidades públicas emitida

por el DAFP en su versión 5 en diciembre del año 2020 aprobó el documento D-CG-09-POLITICAS DE GESTIÓN DEL RIESGO con el objeto de establecer disposiciones y criterios Institucionales que orienten a la Empresa de Obras Sanitaria de Caldas EMPOCALDAS S.A E.S.P., en la identificación, análisis, valoración y administración de los riesgos que puedan afectar el logro de los objetivos estratégicos y de proceso, impidiendo o retrasando el cumplimiento de la misión institucional..

La política de administración de riesgos es aplicable a todos los procesos de la entidad en todas sus seccionales, comprende los riesgos de gestión, de corrupción y de seguridad de la información.

7. ESTRATEGIAS PARA COMBATIR EL RIESGO

Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente. La decisión que se toma frente a un determinado nivel de riesgo puede ser aceptar, reducir o evitar.

Reducir: Después de realizar un análisis y considerar que e nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

Aceptar: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Evitar: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: responsable, fecha de implementación, y fecha de seguimiento.

8. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas • (3) cambios o aparición de nuevas vulnerabilidades • (4) aumento de las consecuencias o impactos, (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

9. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

9.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Como primer paso para la identificación de riesgos de seguridad de la información se identifican los activos de información del proceso. En el cual un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: Aplicaciones de la organización, Servicios web, Redes, Información física o digital, Tecnologías de información TI, Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital

La identificación y valoración de los activos de información será realizada por la primera línea de defensa (líderes de proceso), y para la generación de este inventario, Empocaldas S.A. E.S.P. tendrá en cuenta los siguientes pasos:

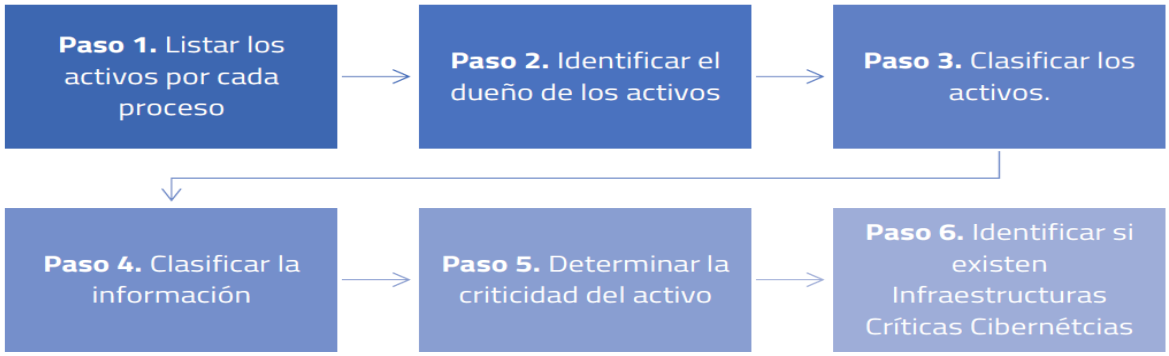

Figura 11: Pasos para la identificación y valoración del inventario de activos de información – Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Para la clasificación de los activos de información, estos pertenecerán a un determinado grupo de activos como son: información, software, hardware, servicios, intangibles, componentes de red, personas e instalaciones.

9.2. IDENTIFICACIÓN DEL RIESGO

Como lo indica la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" emitida por el DAFP, los tres tipos de riesgo inherentes de seguridad de la información son:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se asocia el grupo de activos, o activos específicos del proceso, y conjuntamente se analizan las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Según lo expuesto en la guía para la administración del riesgo y el diseño de controles en entidades públicas, "La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control."

9.3. VALORACION DEL RIESGO

Para esta etapa se toman las tablas de probabilidad e impacto definidas en la primera parte del presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.

Las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

9.4. CONTROLES ASOCIADOS A SEGURIDAD DE LA INFORMACIÓN

Empocaldas S.A. E.S.P. establece e implementa los controles asociados a la seguridad de la información empleando los controles del Anexo A de la ISO/IEC 27001:2013 y que se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”.

10. MATRIZ DE IDENTIFICACIÓN DE RIESGOS EMPOCALDAS S.A. E.S.P

Ver documento adjunto Riesgos_SegInfo_2023.xlsx

11. RUTA DE IMPLEMENTACIÓN PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

NOMBRE DEL PROYECTO	AÑO 2023												COSTO PROYECTO
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembr	Octubre	Noviembr	Diciembre	
ADQUISICIÓN DE CINTAS PARA BACKUPS CUSTODIA DE INFORMACIÓN, ADQUISICIÓN ELEMENTOS, ACCESORIOS Y KIT DE MANTENIMIENTO EQUIPOS SECCIONAL MANIZALES Y ACCESORIOS PARTES PARA LA PLATAFORMA TECNOLÓGICA, ELEMENTOS PARA REPOTENCIAR EQUIPOS													$ 39.000.000
GESTIONAR EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO UPS MANIZALES - DORADA - CHINCHINÁ - CAMBIO BATERÍAS UPS MANIZALES - ADQUISICION BATERIAS													$ 8.000.000
CONTRATAR LA PRESTACION SERVICIOS PARA LA REALZACION DE DOS (2) MANTENIMIENTOS PREVENTIVOS(5) AIRES ACONDICIONADOS DORADA Y ADQUISICIÓN 2 AIRES ACONDICIONADOS Y SENSOR DE HUMEDAD PARA LA SECCIONAL MANIZALES													$ 23.000.000
GESTIONAR LA RENOVACIÓN DE EXTENSIÓN DE GARANTÍAS PARA LOS EQUIPOS SERVIDORES DEL DATA CENTER.													$ 16.000.000
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO SUSCRIPCIÓN ANUAL FIREWALL - RENOVACIÓN FORTICLIENTE ENDPOINT - ADQUISICIÓN DNSSEC - RENOVACIÓN POOL DE LICENCIAS IPV6													$ 45.000.000
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO VEEAM BACKUP PARA OFFICE 365 POR SUSCRIPCIÓN A UN AÑO.													$ 21.000.000

ACTIVIDAD	RECURSOS	Fecha Iniciación	Fecha Terminación	Responsable
ADQUISICIÓN DE CINTAS PARA BACKUPS CUSTODIA DE INFORMACIÓN, ADQUISICIÓN ELEMENTOS, ACCESORIOS Y KIT DE MANTENIMIENTO EQUIPOS SECCIONAL MANIZALES Y ACCESORIOS PARTES PARA LA PLATAFORMA TECNOLÓGICA, ELEMENTOS PARA REPOTENCIAR EQUIPOS	$ 39.000.000	1/05/2023	30/12/2023	Sección Sistemas
GESTIONAR EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO UPS MANIZALES - DORADA - CHINCHINÁ - CAMBIO BATERÍAS UPS MANIZALES - ADQUISICION BATERIAS	$ 8.000.000	1/04/2023	31/12/2023	Sección Sistemas
CONTRATAR LA PRESTACION SERVICIOS PARA LA REALZACION DE DOS (2) MANTENIMIENTOS PREVENTIVOS(5) AIRES ACONDICIONADOS DORADA Y ADQUISICIÓN 2 AIRES ACONDICIONADOS Y SENSOR DE HUMEDAD PARA LA SECCIONAL MANIZALES	$ 23.000.000	1/04/2023	31/12/2023	Sección Sistemas
GESTIONAR LA RENOVACIÓN DE EXTENSIÓN DE GARANTÍAS PARA LOS EQUIPOS SERVIDORES DEL DATA CENTER.	$ 16.000.000	1/07/2023	31/10/2023	Sección Sistemas
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO SUSCRIPCIÓN ANUAL FIREWALL - RENOVACIÓN FORTICLIENTE ENDPOINT - ADQUISICIÓN DNSSEC - RENOVACIÓN POOL DE LICENCIAS IPV6	$ 45.000.000	1/02/2023	31/05/2023	Sección Sistemas
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO VEEAM BACKUP PARA OFFICE 365 POR SUSCRIPCIÓN A UN AÑO.	$ 21.000.000	1/03/2023	31/05/20223	Sección Sistemas

ACTIVIDADES RELACIONADAS
DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
IDENTIFICAR Y DEFINIR CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA REDUCIR Y/O MITIGAR LOS RIESGOS.
REALIZACIÓN COPIAS DE SEGURIDAD SISTEMAS DE INFORMACIÓN 2 COPIAS AL DÍA
COPIAS DE SEGURIDAD OFFICE 365
ENVIO A CUSTODIA COPIAS DE SEGURIDAD MENSUALES
REVISIÓN Y ANÁLISI DE INCIDENTES DE SEGURIDAD
BITACORA DE REVISIÓN LOGS
CAPACITAR A FUNCIONARIOS DE FORMA PERIÓDICA EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
ENVIO DE INFORMACIÓN Y TIPS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
SOCIALIZACIÓN GUIA DE CLASIFICACIÓN DE LA INFORMACIÓN
MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS A PLATAFORMA TECNOLÓGICA

Fecha	Versión	Asunto	Solicitado Por	Aprobado Por
Enero 2022	03	Actualización del Documento	Jefe Depto. Administrativo y Financiero	Jefe Depto. Administrativo y Financiero
2023-01-26	04	Se actualiza la ruta de implementación	Depto. Planeación y Proyectos	CIGD

Elaboró o Actualizó	Revisó y Aprobó
Jefe de Sistemas	(ACTA 2 – 2023-01-25) COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO