1. INTRODUCCIÓN:

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

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 de la Empresa 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 sobre cualquier proceso de la EMPOCALDAS S.A. E.S.P., a cualquier sistema de información o aspecto 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 gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la empresa de Obras Sanitarias de Caldas EMPOCALDAS S.A. E.S.P.

3.1.1. OBJETIVOS ESPECÍFICOS:

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la 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.
- Proponer soluciones para minimizar 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 gestión 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 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”.

5.2.1. VISIÓN GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

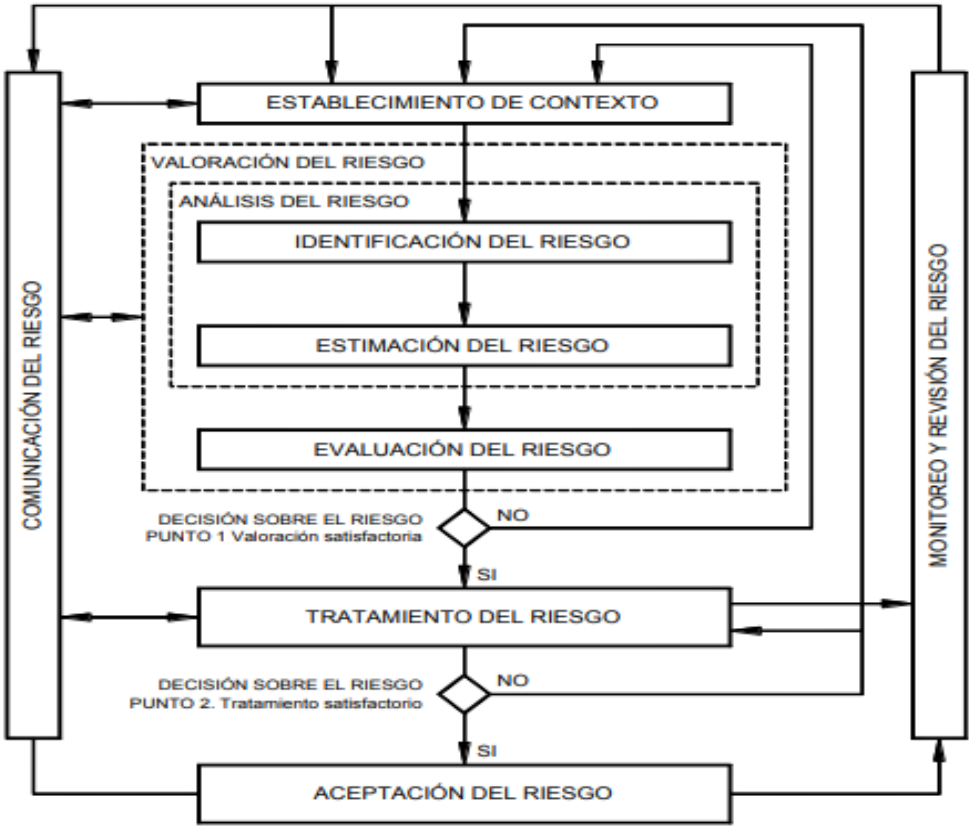


Figura 1. Proceso para la administración del riesgo.

5.2.2. IDENTIFICACIÓN DEL RIESGO

Riesgo Estratégico: Se asocia con la forma en que se administra la Empresa. 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 Empresa 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: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la Empresa y de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la Empresa 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 Empresa 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 Empresa para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

5.3. SITUACIÓN NO DESEADA

- 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

6. ORIGEN DEL PLAN DE GESTIÓN

EMPOCALDAS S.A. E.S.P. actualmente tiene su infraestructura tecnológica para atender todas las sedes a nivel departamental con sus servicios de acueducto y alcantarillado, también con la facturación del servicio de Aseo en su factura; se hace necesario la creación de un plan de gestión de riesgos de seguridad de la información que permita proteger los activos más valiosos de la Empresa.

6.1. 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.

6.2. 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 en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

6.2.1. 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.

6.2.2. CRITERIOS DE IMPACTO.

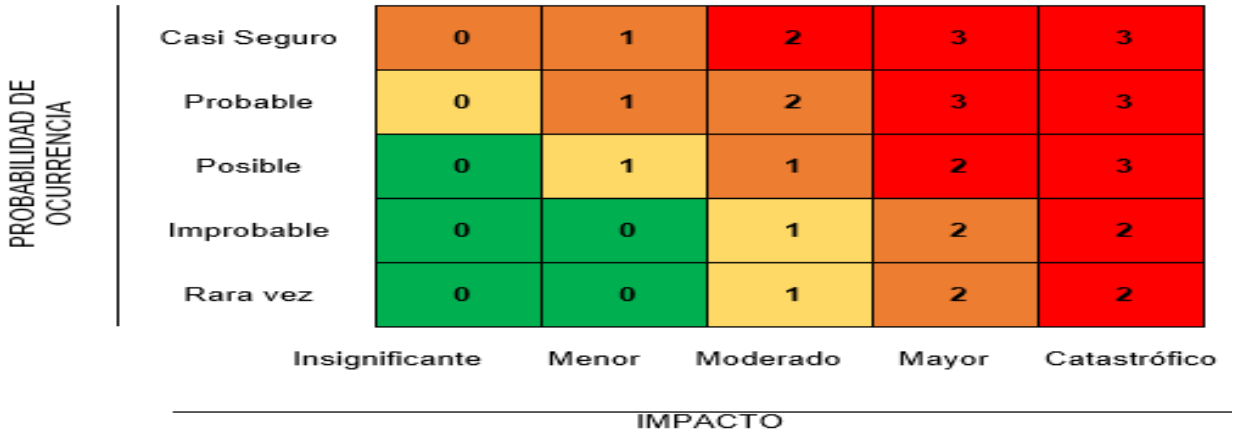
Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Empresa, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados.
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (afectación a partes internas o terceras partes).
- Pérdida del negocio y del valor financiero.
- Alteración de planes o fechas límites.
- Daños en la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

6.2.3. CRITERIOS DE ACEPTACIÓN

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de EMPOCALDAS S.A. E.S.P. y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información.

6.3. VALORACIÓN



Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Empresa, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo.
- Identificación de los riesgos.
- Estimación del riesgo.
- Evaluación del riesgo.

6.3.1. IDENTIFICACIÓN DEL RIESGO

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información.

Los activos de información se clasifican en dos tipos:

a) Primarios:

- Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

- Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) De Soporte

- Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.).
- Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, responsables, etc.)
- Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- Estructura organizativa: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de

las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Finalmente se identifican las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

6.3.2. ESTIMACIÓN DEL RIESGO

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- Probabilidad: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- Impacto: Hace referencia a las consecuencias que puede ocasionar a la Agencia la materialización del riesgo; se refiere a la magnitud de sus efectos.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deben analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

6.4. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo se obtiene una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

6.5. 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.

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

Ver documento adjunto Riesgos_SegInfo_2022.xlsx

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

NOMBRE DEL PROYECTO	AÑO 2022												COSTO PROYECTO
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembr	Octubre	Noviembr	Diciembre	
Mejoramiento Servidores de almacenamiento actual - Plan de Continuidad del Negocio													$ 50.000.000
Planes de Transición IPV4 - IPV6 - Adquisición Pool de direccionamiento IPV6													$ 15.000.000
Mantenimiento preventivo y correctivo UPS Manizales - Dorada - Chinchiná (BATERIAS)													$ 1.440.000
Extensión Garantía Servidores													$ 10.500.000
Adquisición licencia suscripción anual Firewall													$ 29.400.000
Plataforma correo e integración - Office 365 - Licenciamiento Power BI													$ 65.614.920
Renovación 3 Licencias Civil 3D por suscripción anual													$ 29.749.285
Renovación Licencia adobe creative Cloud para el área de comunicaciones													$ 4.636.000
Mantenimiento equipos de cómputo seccionales													$ 15.000.000
Adquisición licencias VEEMBackup para copias de seguridad correo electrónico y Sharepoint													$ 25.000.000
2 Personas soporte técnico - Mesa de ayuda (Helpdesk) - Mantenimiento preventivo a equipos													$ 56.146.896
Actualización marco documental y procedimental Gobierno Digital													$ 0
Portal Web - Intranet - Redes - Desarrollos orientados a la web e Intranet													$ 40.000.000
Mantenimiento infraestructura, comunicaciones y seguridad perimetral													$ 50.000.000
Implementación Data center alterno - Plan de recuperación de desastres.													$ 150.000.000
Cintas para Backups (15)													$ 4.500.000
Pentesting aplicativos web Hacking Etico - Infraestrutura													$ 18.000.000
Sistema de detección de incendios													$ 5.500.000

ACTIVIDAD	RECURSOS	Fecha Iniciación	Fecha Terminación	Responsable
Mejoramiento Servidores de almacenamiento actual - Plan de Continuidad del Negocio	$ 50.000.000	1/04/2022	31/12/2022	Sección Sistemas
Planes de Transición IPV4 - IPV6 - Adquisición Pool de direccionamiento IPV6	$ 15.000.000	1/04/2022	31/10/2022	Sección Sistemas
Mantenimiento preventivo y correctivo UPS Manizales - Dorada - Chinchiná (BATERIAS)	$ 1.440.000	1/04/2022	31/07/2022	Sección Sistemas
Extensión Garantía Servidores	$ 10.500.000	1/07/2022	31/12/2022	Sección Sistemas
Adquisición licencia suscripción anual Firewall	$ 29.400.000	1/03/2022	30/04/2022	Sección Sistemas
Plataforma correo e integración - Office 365 - Licenciamiento Power BI	$ 65.614.920	1/04/2022	31/03/2023	Sección Sistemas
Renovación 3 Licencias Civil 3D por suscripción anual	$ 29.749.285	1/04/2022	31/05/2022	Sección Sistemas
Renovación Licencia adobe creative Cloud para el área de comunicaciones	$ 4.636.000	1/09/2022	31/10/2022	Sección Sistemas
Mantenimiento equipos de cómputo seccionales	$ 15.000.000	1/05/2022	31/12/2022	Sección Sistemas
Adquisición licencias VEEMBackup para copias de seguridad correo electrónico y Sharepoint	$ 25.000.000	1/02/2022	31/03/2022	Sección Sistemas
2 Personas soporte técnico - Mesa de ayuda (Helpdesk) - Mantenimiento preventivo a equipos	$ 56.146.896	20/01/2022	31/12/2022	Sección Sistemas
Actualización marco documental y procedimental Gobierno Digital	$ 0	1/01/2022	31/12/2022	Sección Sistemas
Portal Web - Intranet - Redes - Desarrollos orientados a la web e Intranet	$ 40.000.000	1/01/2022	31/12/2022	Sección Sistemas
Mantenimiento infraestructura, comunicaciones y seguridad perimetral	$ 50.000.000	1/01/2022	31/12/2022	Sección Sistemas
Implementación Data center alterno - Plan de recuperación de desastres.	$ 150.000.000	1/04/2022	30/11/2022	Sección Sistemas
Cintas para Backups (15)	$ 4.500.000	1/02/2022	31/05/2022	Sección Sistemas
Pentesting aplicativos web Hacking Etico - Infraestrutura	$ 18.000.000	1/02/2022	31/05/2022	Sección Sistemas
Sistema de detección de incendios	$ 5.500.000	1/01/2022	28/02/2022	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

Elaboró o Actualizó	Revisó	Aprobó
Jefe Sección Sistemas	(Acta 1 - 2022-01-27) COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	