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

EMCANDELARIA

CON EXPERIENCIA AVANZAMOS

ALCALDÍA DE CANDELARIA

Carrera 11 No 10 – 55 Esquina Villagorgona (Candelria Valle) – Teléfono: (+57 2) 260 0979 – Celular: 3187173259
www.emcandelaria.gov.co – E-mail: contactenos@emcandelaria.gov.co – gerencia@emcandelaria.gov.co

GLOSARIO

- **Seguridad informática:** Se ocupa de la implementación técnica y de la operación para la protección de la información.

- **Seguridad de la información:** Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.

- **Amenazas:** Cualquier evento, persona, situación o fenómeno que pueda causar daño.

- **Vulnerabilidades:** Falla o debilidad en un sistema que puede ser explotada por quien la conozca.

- **Riesgo:** Probabilidad de ocurrencia de una amenaza.

- **Controles:** Conjunto de mecanismos que regulan el funcionamiento de un sistema.

- **Activo de Información:** Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.

- **Análisis de brechas:** es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.

- **Análisis de Riesgo:** Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.

- **Gestión del Riesgo Informáticos:** Actividades empleadas para mitigar los riesgos informáticos.

- **Incidente de seguridad informática:** daño que puede comprometer las operaciones de la Empresa.

- **Información:** Conjunto de datos que tienen un significado.

INTRODUCCION

El proceso de administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos las Empresas en la ejecución de sus actividades, están propensas a desarrollar riesgos el cual pueden ocasionar fracasos en una gestión; por lo tanto, es necesario tomar las medidas anticipadas, para identificar las causas y consecuencias de la materialización de dichos riesgos, buscando prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información y así facilitar su identificación, definición de controles y dar lineamientos concisos para su adecuada gestión.

TABLA DE CONTENIDO

1. OBJETIVOS

1.1 OBJETIVO GENERAL

- Mitigar la materialización de los riesgos de seguridad de la información en La Empresa Regional De Servicio Publico Domiciliario EMCANDELARIA S.A.S E.S.P, propendiendo al aumento de confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

1.2 OBJETIVOS ESPECÍFICOS

- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos de información a proteger en la Entidad.
- Identificar los riesgos, amenazas y vulnerabilidades en la Empresa.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.

2. ALCANCE

Esta guía, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

3. ÁMBITO DE APLICACIÓN

Los lineamientos definidos en este plan, aplica para la gestión de los riesgos en la Empresa Regional De Servicio Publico Domiciliario EMCANDELARIA S.A.S E.S.P.

4. PLAN DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION

El Plan de Seguridad de la Información de EMCANDELARIA S.A.S E.S.P está encaminado a la detección de vulnerabilidades para una vez detectadas, tomar las medidas necesarias para prevenir inconvenientes de la ciberseguridad. Es por esto que se llevan a cabo cuatro (4) etapas para mitigación de riesgos informáticos así.

4.1 Identificación

Se denomina activo a aquello que tiene algún valor para la Empresa y por tanto debe protegerse. En esta etapa se realiza inventario de los activos de información pertenecientes a la empresa EMCANDELARIA S.A.S E.S.P. como base para la gestión de riesgos de seguridad de la información y determinar los niveles de protección requeridos.

Infraestructura de TI

- Oficinas
- Escritorios
- Archivadores
- Equipos de alarma
- Supresión contra incendio
- Otros dispositivos de seguridad

Hardware de TI

- Equipos de cómputo de escritorio
- Equipos de cómputo portátiles
- Servidor
- Impresoras
- Dispositivos de almacenamiento Backup
- Módems
- Planta telefónica
- Dispositivos de comunicación móvil
- Líneas de terminación de red

Software de TI

- Sistemas operativos
- Herramientas de office

- Antivirus
- Software contable
- Software de gestión documental

Activos de servicios de TI

- Servicios de red
- Servicios de monitoreo gps
- Correo electrónico
- Mensajería instantánea en red
- Servicios web
- Redes sociales institucionales
- Contratos de soporte
- Bases de datos

4.2 IDENTIFICADORES DE RIESGOS

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Perdida Robo o Fuga de Información	-Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma. -No contar con acuerdos de confidencialidad con los empleados y terceros -Falta de autorización para la extracción de información generada por requerimientos. -Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad -Ataques cibernéticos internos o externos -Empleados no capacitados en los temas de riesgos informáticos. -Prestar los equipos informáticos a personal no autorizado. -No cerrar sesión cuando se desplaza del puesto. -Acceso no autorizado a las dependencias. -Conectar dispositivos externos a los equipos.	-Afectación parcial o total de la continuidad de las operaciones de los servicios -Vulneración de los sistemas de seguridad operando actualmente -Mala imagen, multas, sanciones y pérdidas económicas -Generación de consultas, funcionalidades o reportes con información sensible de los clientes -Pérdida o fuga de información

	-Falta de implementación de la política escritorio limpio	
RIESGOS INFORMÁTICOS	**CAUSAS**	**EFECTO**
Correos electrónicos de extraña procedencia	-Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - Falta de Filtros en el Servidor de Correo - Programas de DLP (Data Lost Prevention) - Falta de instalación de EndPoint (programa seguridad punto final) en las estaciones de trabajo.	-Cifrado de la información. - Captura de las pulsaciones del teclado. - Monitoreo de las actividades realizadas en el equipo. - Ataque remoto mediante un troyano o gusano. - Robo de contraseñas. - Robo de documentos y/o archivos.
Daño en los equipos tecnológicos	- Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas - Falta de equipos regulatorios de electricidad - Fallas por defectos de fabrica - Humedad - Falta de ambiente adecuado para los equipos - Desconocimiento del cuidado de los equipos	-Perdida de información -Perdidas de los quipos informáticos - Indisponibilidad del Servicio - Limitaciones en los procesos
Dumpsterdiving (buceo en la basura)	-Desconocimiento del riesgo. -Falta de capacitación y conciencia.	-Creación de perfil de ataque -Captura de información privilegiada
Perdida de conectividad	-Daño externo del ISP (Internet service provider)	- Acceso a la red - Acceso a información y archivos - Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios)
Ataques Informáticos	- Insiders -Estimulo o Reto personal -Ánimo de lucro -Espionaje	-Daño en los equipos tecnológicos - Incidente en la confidencialidad, integridad y disponibilidad de la información -Denegación de servicios -Secuestro de la información -Divulgación ilegal de la información -Suplantación de identidad -Destrucción de la información

		-Soborno de la información

4.3 IDENTIFICADOR DE AMENAZAS	
AMENAZA	**TIPO**
Polvo, Corrosión	Evento Natural
Inundación	Evento Natural
Incendios	Evento Natural
Fenómenos Sísmicos	Evento Natural
Fenómenos Térmicos	Evento Natural y Daño físico
Perdida en el suministro de energía	Daño Físico
Espionaje remoto	Acciones no autorizadas
Ingeniería Social	Acciones no autorizadas
Intrusión	Acciones no autorizadas
Accesos forzado al sistema	Acciones no autorizadas

4.4 IDENTIFICACIÓN DE VULNERABILIDADES	
VULNERABILIDADES	**DESCRIPCIÓN**
Fácil acceso a las áreas de trabajo	No existe un control para el acceso de las personas no autorizadas a las áreas de trabajo de la empresa
Falta de dispositivos de seguridad biométrica para acceso a las áreas de alto riesgo.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.
Falta de Política de escritorio Limpio.	La política de escritorio limpio, es implementada para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente.
Falta de máquina trituradora de papel	La máquina trituradora de papel , evita que las personas arrojen documentos importantes con información personal a la

	basura, y que puedan ser usados para crear perfiles de ataque.
Falta de Capacitación de los empleados responsables de temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los empleados, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos.
Falta de equipos electrónicos para copias de respaldo.	El no contar con un HDD externo, impide a los empleados realizar copias de respaldo o Back ups
Falta de equipos empresariales.	El no contar con suficientes equipos empresariales, lleva a los empleados a traer equipo personal que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente promueve el compartir cuentas de usuarios y calves que pueden afectar al prestador
Equipos clonados.	Los equipos clonados no cuentan con software legal que pueden infectar la red o traer problemas legales

4.5 IDENTIFICACIÓN DE CONTROLES EXISTENTES

La identificación de los controles existentes permite realizar la evaluación de riesgos. Lo controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros. Dada la importancia de los controles, con que cuenta la Empresa EMCANDELARIA S.A.S E.S.P, no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

5. Evaluación De Riesgos

En esta etapa se establecen las situaciones que ponen en peligro los activos anteriores el cual la Empresa está propensa a solventar

Infraestructura de TI

- Fuego
- Daños por agua
- Daños eléctricos
- Otros desastres naturales.

Hardware de TI

- Perdida Robo o Fuga de Información
- Manipulación de la configuración
- Suplantación de la identidad del usuario
- Abuso de privilegios de acceso
- Eliminación de copias de seguridad

Software de TI y Activos de servicios de TI

- Virus
- Malware
- Control de acceso a internet
- Cambios regulatorios
- Contraseñas de acceso irregulares
- Introducción de falsa información
- Ausencia de capacitación al personal en seguridad informática
- Correos electrónicos de extraña procedencia

Para la evaluación de riesgos se realiza una comparación entre, la probabilidad de ocurrencia del riesgo con el impacto del mismo. Se emplea una matriz llamada "Matriz de Calificación, Evaluación y respuesta a los Riesgos".

TABLA DE PROBABILIAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	probable	El evento probablemente ocurra en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

PROBABILIDAD	IMPACTO				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrófico(5)
Raro(1)	B	B	M	A	A
Improbable(2)	B	B	M	A	E
Posible(3)	B	M	A	E	E
Probable(4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B:Zona de Riesgo Baja: Asumir el Riesgo
M:Zona de Riesgo Moderada: Asumir el Riesgo, Reducir el Riesgo

A:Zona de Riesgo Alta: Reducir ,Evitar, Compartir o Transferir
E:Zona de Riesgo extrema: Reducir El Riesgo, Evitar Compartir o Transferir

RIESGO	CALIFICACIÓN		TIPO DE IMPACTO	EVALUACION ZONA DE RIESGO	MEDIDA DE RESPUESTA
	PROBABILIDAD	IMPACTO			
Perdida Robo o Fuga de Información	3	3	Confidencialidad, integridad, disponibilidad de la información.	ALTO	Reducir ,Evitar, Compartir o Transferir
Correos eléctronicos de extraña procedencia	1	2	Confidencialidad, integridad, disponibilidad de la información.	BAJO	Asumir el Riesgo
Daño en los equipos tecnologicos	4	1	Disponibilidad de la Información	MODERADO	Asumir el Riesgo, Reducir el Riesgo
Dumpsterdiving (Beseo en la Basura)	1	2	Confidencialidad	BAJO	Asumir el Riesgo
Perdida de Conectividad	5	2	Disponibilidad de la Información	ALTO	Reducir ,Evitar, Compartir o Transferir
Ataques Informaticos	1	5	Confidencialidad, integridad, disponibilidad de la información.	EXTREMO	Reducir El Riesgo, Evitar Compartir o Transferir

6. PRIORIZACIÓN DE PROTECCIÓN Y TOMA DE DECISIONES – TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Diseñar e implementar un programa anual de capacitación y sensibilización en seguridad de la información para empleados.

2. Implementar y celebrar cláusulas de confidencialidad, integridad y seguridad de la información en contratos con empleados y proveedores que prestan servicios a la Empresa.

3. Establecer e implementar una política de copias de respaldo para salvaguardar la información crítica.

4. Continuar implementando la política de almacenamiento en disco interno del equipo de computo "D, E o F".

5. Denegar acceso a páginas desconocidas con contenido gratuito como mp3, radio y redes sociales.

6. Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT).

7. Implementar soluciones de seguridad que permiten tener total auditoría y control sobre la infraestructura contratada en el dominio empresarial.

8. Asegurar el uso y apropiación de las redes Sociales corporativas

9. Realizar copias de seguridad semanales de información institucional

10. Instalar actualizaciones de software periódicamente

11. Implementar cambio de contraseñas periódicamente

12. Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se contrataron están siendo implementados, operados y mantenidos.

La Gestión del Riesgo en la seguridad de la información debe de contribuir a:

- Identificación de los Riesgos
- La valoración de los Riesgos en términos de sus consecuencias y la probabilidad de su ocurrencia
- La comunicación y el entendimiento de la probabilidad y las consecuencias de estos Riesgo
- El establecimiento del orden por prioridad para el tratamiento de los riesgos
- La priorización de las acciones para reducir la ocurrencia de los riesgos
- La participación de los interesados cuando se tomen las decisiones sobre la gestión del riesgo y mantenerlos informados sobre el estado de la gestión de riesgos.
- La eficacia del monitoreo de la gestión del riesgo
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos
- La captura de información para mejorar el enfoque de la gestión de riesgos
- La socialización a los secretarios y al personal acerca de los riesgos y las acciones que se toman para mitigarlos.

El reto es continuar con la implementación de acciones que garanticen la seguridad y privacidad de la información de la Empresa y avanzar hacia la adopción de métodos más seguros y efectivos, mediante la destinación de recursos y gestión de conocimiento de empresas similares, experiencias compartidas.

RECOMENDACIONES

• Concientizar constantemente a los funcionarios de la Empresa EMCANDELARIA S.A.S E.S.P, sobre la importancia de cumplir con la política de seguridad de la información.

• Aplicar correctivos o sanciones a los funcionarios que no cumplan con la política de seguridad de la información establecida.

• Mantener actualizada la política de seguridad de la información

• Realizar Auditorías periódicas de Seguridad Informática.

• Capacitar frecuentemente a los funcionarios de la EMCANDELARIA S.A.S E.S.P en temas de seguridad informática.

• Establecer un responsable de la seguridad informática en cada departamento o dependencia.

7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De manera genérica a continuación se entrega un texto guía para la elaboración de la política general de seguridad de la información, este puede ser base del desarrollo de dicho documento ya que contempla los principios básicos a tener en cuenta en su elaboración dentro de la planeación del sistema de gestión de seguridad de la información en una entidad.

La dirección de EMCANDELARIA S.A.S E.S.P entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para EMCANDELARIA S.A.S E.S.P, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de EMCANDELARIA S.A.S E.S.P
- Garantizar la continuidad del negocio frente a incidentes.

- EMCANDELARIA S.A.S E.S.P ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
- Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de EMCANDELARIA S.A.S E.S.P

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

• EMCANDELARIA S.A.S E.S.P protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

• EMCANDELARIA S.A.S E.S.P protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• EMCANDELARIA S.A.S E.S.P protegerá su información de las amenazas originadas por parte del personal.

• EMCANDELARIA S.A.S E.S.P protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• EMCANDELARIA S.A.S E.S.P controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• EMCANDELARIA S.A.S E.S.P implementará control de acceso a la información, sistemas y recursos de red.

• EMCANDELARIA S.A.S E.S.P garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• EMCANDELARIA S.A.S E.S.P garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• EMCANDELARIA S.A.S E.S.P garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• EMCANDELARIA S.A.S E.S.P garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.