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

Vigencia 2024

Carerra 11 No 10 – 55 Esquina Villagorgona (Candelaria- Valle) – Teléfono: (+57 2) 260 0979 – Celular: 318 717 3259
www.emcandelaria.gov.co - E-mail: contactenos@emcandelaria.gov.co – gerencia@emcandelaria.gov.co

TABLA DE CONTENIDO

GLOSARIO

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la gestión de riesgos:

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.

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

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 generadoras 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 se evaluada.

Control: Medida que modifica el riesgo. 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.

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.

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.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

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.

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 con trol o las diferentes auditorías de los sistemas integrados de gestión.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Riesgo en la seguridad de la información: 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.

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.

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.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

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.

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

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

INTRODUCCIÓN

Las empresas hoy día, se encuentran inmersas en la denominada revolución digital, en donde se reconoce el protagonismo de la información en sus procesos productivos, por tanto la importancia de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo 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.

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 entidades. Una organización sin un plan de gestión de riesgos está expuesta a perder toda su información.

Son requisitos indispensables para la implementación del presente plan:

- ✓ Lograr el compromiso de la alta gerencia de EMCANDELARIA S.A.S E.S.P para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.

- ✓ Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

- ✓ Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

OBJETIVO GENERAL

Definir los lineamientos y metodología a seguir para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información.

OBJETIVOS ESPECÍFICOS

- ✓ Identificar durante el 2024 los riesgos en los procesos de la entidad, que puedan afectar la integridad, confidencialidad y disponibilidad de la información.
- ✓ Definir los principales activos a proteger en la entidad.
- ✓ Identificar las principales amenazas que afectan a los activos.
- ✓ identificar y analizar los Riesgos referentes a los temas de la Seguridad de la Información.

2. MARCO TEORICO

2.1. SEGURIDAD INFORMÁTICA

La seguridad Informática y la seguridad de la información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integridad y disponibilidad de la información.

Ilustración 1: Pilares de la seguridad Informática.

2.2. NORMA ISO 27001

La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

2.3. NORMA ISO 27005

La norma ISO 27005 es un soporte a la norma (ISO 27001) la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.

“Las secciones contenidas en la norma ISO 27005 son:

- Prefacio
- Introducción
- Referencias normativas
- Términos y definiciones
- Estructura
- Fondo
- Descripción general del proceso de ISRM
- Establecimiento de contexto
- Evaluación de riesgos de seguridad de la información (ISRA)
- Tratamiento de riesgos de seguridad de la información
- Seguridad de la información Aceptación del riesgo
- Seguridad de la información Comunicación de riesgos
- Seguridad de la información Monitoreo y revisión de riesgos

- Anexo A: Definición del alcance del proceso
- Anexo B: Valoración de activos y evaluación de impacto
- Anexo C: ejemplos de amenazas típicas
- Anexo D: Vulnerabilidades y métodos de evaluación de vulnerabilidad[1]
- Anexo E: enfoques ISRA"

En la siguiente figura se muestra el procedimiento de la guía 7 que propone el departamento administrativo de la función pública (DAFP) junto con el ministerio de la tecnología de información y comunicación (MinTIC) para la gestión de riesgos informáticos.

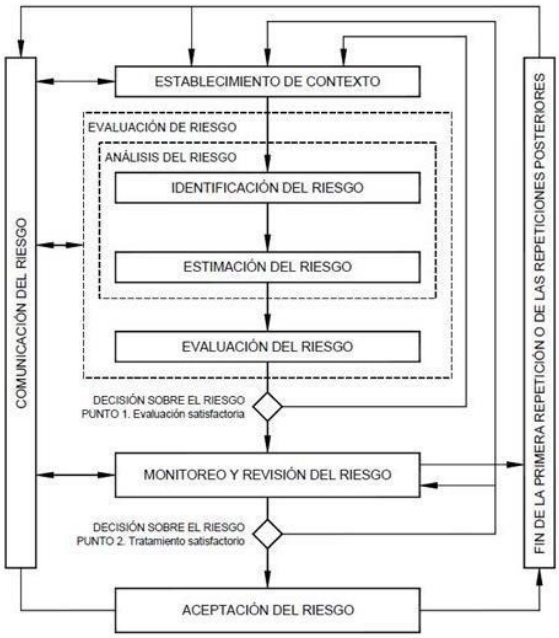


Ilustración 2: Tomada de NTC-ISO/IEC 27005 Gestión de Riesgos

2.4. ISO 27001. ORIGEN E HISTORIA

1901 – Nacen en Inglaterra las Normas “BS”: La British Standards Institution publica normas con el prefijo “BS” con carácter internacional.

1995- Se escribe la norma BS 7799-1:1995 por el Departamento de Comercio e Industria del Reino Unido (DTI), Mejores prácticas para la gestión de la seguridad de la información.

1998 –Se hace una revisión de la anterior norma BS 7799-2:1999 que establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.

2000 - La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios dando como resultado la norma ISO/IEC 17799:2000:

2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

2006 - BS 7799-3:2006 proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).

2007 –Se renombra la norma ISO 17799: y pasa a ser la ISO 27002:2005

2007 –Se publica la nueva versión de la norma ISO/IEC 27001:2007:

2008 – nace la guía para la Implantación (bajo desarrollo) ISO 27003:2008.[2]

2008 -ISO 27004:2008 Métricas e Indicadores (bajo desarrollo).

2008 –se crea la norma ISO 27005:2008 para la Gestión de Riesgos (BS 7799-3:2006)

2009 – Se publica un documento adicional de modificaciones llamadoISO

27001:2007/1M:2009.

2011 – ISO 27005:2011: Se publica la nueva versión.

En el año 2013 se publicado ya la nueva versión de la ISO 27001 que trae cambios significativos en su estructura, evaluación y tratamiento de los riesgos.

Cuadro. Familia de normas 27000

Norma ISO/IEC	Título
ISO 27000	Gestión de la Seguridad de la Información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para un **SGSI**.
ISO 27002	Código de Buenas Prácticas.
ISO 27003	Guía de Implantación de un **SGSI**.
ISO 27004	Sistema de Métricas e Indicadores.
ISO 27005	Guía de Análisis y Gestión de Riesgos.
ISO 27006	Especificaciones para Organismos Certificadores de **SGSI**.
ISO 27007	Guía para auditar un **SGSI**.

Tabla 1: Familia Norma ISO 27000

3. MARCO CONTEXTUAL

CORREGIMIENTO DE VILLAGORGONA

Villagorgona, no tiene un fundador conocido, aunque por sus tierras paso dos veces el Conquistador SEBASTIAN DE BELALCAZAR. En el año de 1953, según escritura

pública #196 realizada en la Notaría de Candelaria, (V), el Municipio compro en las inmediaciones de lo que hoy es Villagorgona, cinco plazas de terreno para parcelar entre las familias de escasos recursos económicos, y sin vivienda propia, la negociación se hizo por intermedio de la Alcaldía Municipal de Candelaria. Actualmente los pobladores se dedican al cultivo de caña, Producción Avícola y alfarería.

Desde sus comienzos ha sido un pueblo pacífico y laborioso, sus primeros pobladores fueron los indios Buchitolos, Gorgonios, y Gualies, quienes vivían de la pesca y del cultivo de maíz.

Actualmente, EMCANDELARIA S.A.S E.S.P cuenta con las Siguientes dependencia:

- Gerencia
- Oficina de Asesores
- Tesorería
- Dpto. Operativo y Mantenimiento
- Archivo
- Salud Ocupacional
- Almacén
- Recursos humanos
- Área jurídica y contratación
- Área comercial
- Área de facturación
- Ventanilla única y Servicio al Cliente

3.1. PRESENTACIÓN DE LA ORGANIZACIÓN

EMCANDELARIA S.A.S E.S.P es una empresa pública descentralizada de la Alcaldía Municipal de Candelaria, empresa Prestadora de Servicios públicos Domiciliarios de Acueducto, alcantarillado y tratamiento de aguas residuales con personería jurídica propia con plena autonomía administrativa, de capital y patrimonio independiente, cuya organización y funcionamiento se rige por el

ordenamiento establecido en la Ley 142 de 1994 y demás normas que la modifiquen o aclaren.

Las Empresas Públicas Municipales de Candelaria –EMCANDELARIA S.A.S E.S.P. dio inicio a sus labores en enero de 1993; creada mediante Decreto Extraordinario número 002 del 04 de noviembre 1991 expedido por la Alcaldía Municipal de Candelaria dando cumplimiento al Acuerdo Municipal número 007 de noviembre 14 de 1989, que facultaba al alcalde municipal para crear una empresa para la prestación de los servicios públicos domiciliarios, de conformidad con lo dispuesto en el artículo nacional número 77 de 1987.

La empresa en sus inicios prestaba los servicios de Aseo, Acueducto, Alcantarillado y Mantenimiento al Alumbrado público, en la trayectoria de la empresa se entregó para la operación y administración el servicio de Aseo a saber: en Contrato de Concesión para la prestación del servicio de aseo celebrado entre el Municipio de Candelaria y la Empresa “Urbaseo Candelaria S.A.E.S.P.”.

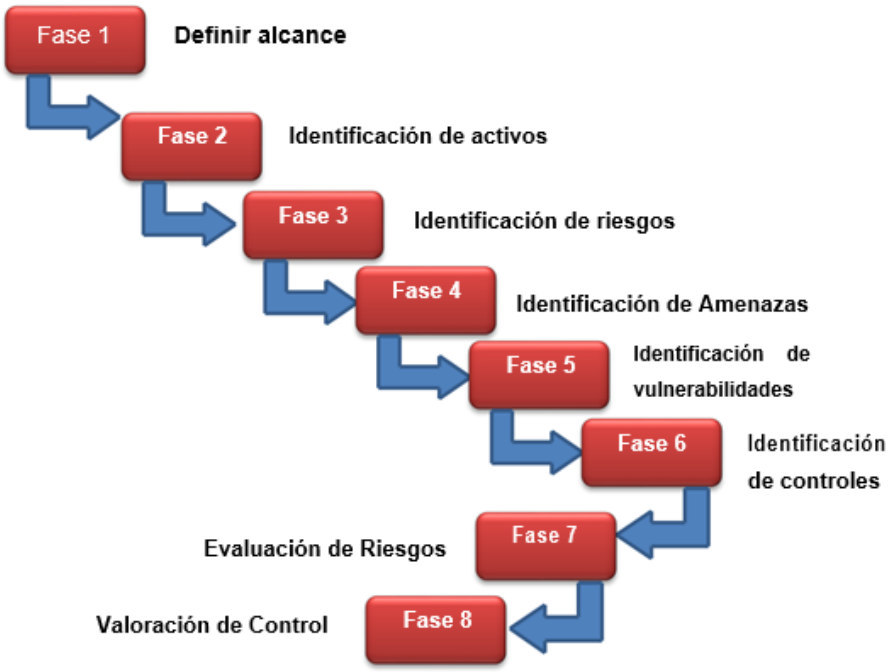
Entre los años 1998 y 1999 se fundó en el municipio la entidad Iluminaciones Candelaria, a la cual le fue cedido por el Alcalde de Turno el mantenimiento al Alumbrado Público, acciones que debilitaron la empresa; pero a pesar de las dificultades sostuvo su posición y permanencia.

Mediante Decreto numero 101 A de agosto 8 de 2002 Las Empresas Públicas Municipales de Candelaria adoptan los Estatutos de la Empresa y adopta su transformación como Empresa Industrial y Comercial del Estado.

Por medio del Acuerdo número 002 de mayo 21 de 2004 se expide el Estatuto de Contratación para Las Empresas Públicas Municipales de Candelaria EMCANDELARIA S.A.S. E.S.P.

A pesar de los esfuerzos por la sostenibilidad de la Empresa el 02 de enero de 2007 mediante Decreto 01 se ordena la liquidación de Las Empresas Públicas Municipales de Candelaria –EMCANDELARIA S.A.S. E.S.P.

4. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO DEL PROYECTO



4.1 ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso de la entidad, 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.

La identificación y tratamiento de los riesgos de seguridad de la información como lineamiento de la alta gerencia, será de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad; dicho tratamiento de riesgo debe involucrar a todos los procesos y actividades desarrolladas por la Entidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

4.2 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACION

El principal activo de una organización es la información en sí, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en Discos Duros Externos, Memorias USB o en forma digital, en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización.)

Se diseñó un formato de inventario de activos de información que contiene los siguientes campos:

Nombre del líder del proceso / Nombre del funcionario

Norma, función o proceso / Función que realiza el funcionario

TIPO DOCUMENTAL:

Nombre del activo de información / Nombre correspondiente al activo de información como Base de Datos, Actas, informes, Sistemas de información etc.

Descripción del activo de información

TIPOLOGÍA:

Software / el activo de información se encuentra en forma digital **Hardware/** el activo de información se encuentra en física

Servicios / el activo de información se emplea como servicio a terceros **Documentos físicos**

TIPO DE SOPORTE (medio de conservación y/o Soporte:

Análogo / Copia adicional del documento en forma física

Digital / Copia de seguridad en otro equipo, en correo electrónico o en la Nube.

Electrónico / Copia de seguridad en equipo electrónico como Disco Duro Externo USB.

Presentación de la información (formato o extensión) / en que aplicación se realiza el activo de información Ej: .PDF, DOC, XLS etc.

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN:

Nivel del Criterio

Confidencialidad / Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado o contratista de la entidad o no	Publico
1	Información que puede ser conocida y utilizada por todos los empleados de EMCANDELARIA S.A.S. E.S.P y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad, el Sector Público Nacional o terceros.	Reservada – Uso Interno
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la entidad o a terceros.	Reservada - Confidencial
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta gerencia de la entidad, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.	Reservada Secreta

Integridad / / Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Integridad
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación de EMCANDELARIA S.A.S E.S.P.
1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la Alcaldía o terceros
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Alcaldía o terceros.
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la Alcaldía o a terceros.

Disponibilidad / / Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operatoria de la entidad.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para la entidad o terceros.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la entidad o a terceros.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la entidad o a terceros.

4.3 IDENTIFICACIÓN DEL RIESGO

El objetivo de la identificación de riesgos es conocer lo incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento de EMCANDELARIA S.A.S E.S.P y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

La identificación de los riegos se realiza con observación directa, ingeniería social y con análisis a los equipos de seguridad perimetral. Por confidencialidad de la entidad se presenta la identificación de riesgos general.

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. -Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT -No contar con acuerdos de confidencialidad con los	-Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo -Vulneración de los sistemas de seguridad operando
	-Falta de autorización para la extracción de información generadas por requerimientos.	-Mala imagen multas, sanciones y Pérdidas económicas
	-Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad	-Generación de consultas, funcionalidades o reportes con información sensible de los clientes
	-Habilitación de puertos USB en modo lectura y escritura para almacenamiento	-Generación de consultas, funcionalidades o reportes con información sensible de los clientes

	-Ataques cibernéticos internos o externos	-Pérdida o fuga de información
	-Desconocimiento del riesgo.	
	-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. -Falta de implementación de la política escritorio limpio	
Correos electrónicos de extraña procedencia	-Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - No generar una Cultura de	-Cifrado de la información. - Captura de las pulsaciones del teclado. - Monitoreo de las actividades realizadas en el equipo. - Ataque remoto

	Seguridad de la Información - Falta de Filtros en Servidor de Correo con el SPAM - Programas de DLP (Data Lost Prevention) Falta de instalación EndPoint (programa seguridad punto final) en las estaciones de trabajo.	mediante un troyano o gusano. - Robo de contraseñas. - Robo de documentos y/o archivos. - Sistema con mal funcionamiento.
Daño en los equipos tecnológicos	-Manejo inadecuado de los equipos - Falta de mantenimiento o mala conexión de estos en las instalaciones eléctricas - Falta de equipos de potenciación -Fallas por defectos de fabrica - Derrame de líquido	-Perdida de Información -Perdidas de los equipos informáticos - Indisponibilidad del Servicio - Traumatismos en los procesos

	-Falta de ambiente adecuado para los equipos -Falta Educación a los usuarios en el manejo de los	
Ataques Informáticos	-Estimulo o Reto personal -Rebelión -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

4.4 IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño a los activos de la organización. Las amenazas pueden ser de origen Humano o Ambientales.

AMENAZA	TIPO
Polvo, Corrosión	Evento Naturales
Inundación	Evento Naturales
Incendios	Evento Naturales
Fenómenos Sísmicos	Evento Naturales
Fenómenos Térmicos	Evento Naturales y Daños físicos
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
Manipulación del Hardware	Acciones no autorizadas
Manipulación con Software	Acciones no autorizadas
Fallas del equipo	Fallas técnicas
Saturación del sistema de información	Fallas técnicas

4.5 IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información.

VULNERABILIDADES	DESCRIPCION
Fácil acceso a las dependencias o Secretarías.	No existe un control para el acceso de las personas no autorizadas a las diferentes áreas de la entidad.
Falta de dispositivos de seguridad biométrica para acceso a las dependencias de alto riesgo.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.

Escritorio Limpio.	implementada para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente.
Máquina trituradora de papel	La máquina trituradora de papel, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.
Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, 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 funcionarios realizar copias de respaldo o Back ups

Falta de equipos institucionales.	El no contar con suficientes equipos institucionales, lleva a los funcionarios 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
Equipo clon.	Los equipos clones, no cuentan con software legal que pueden infectar la red o traer problemas legales

Identificación de Vulnerabilidades

4.6 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 Alcaldía Municipal de Candelaria Valle no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

4.7 EVALUACIÓN DE RIESGO

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

EMCANDELARIA S.A.S E.S.P cuenta con un Sistema de Gestión Documental que realiza el análisis de riesgos con la información recolectada en el análisis de riesgos.

TABLA DE PROBABILIDAD

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

29

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)	Catastrofico(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

Matriz de calificación, evaluación y respuestas a los riesgos.

4.8 VALORACION DE CONTROLES

La valoración de controles evalúa los controles existentes en la organización y la efectividad para mitigar la exposición al riesgo.

Se emplea una tabla para la valoración de control donde se establecen 2 parámetros con 5 criterios, dependiendo del puntaje y si el control se ejecuta con la probabilidad, con el impacto o ambos, se genera un desplazamiento del valor del riesgo.

VALORACIÓN DE CONTROL		
PARAMETROS	**CRITERIOS**	**PUNTAJE**
HERRAMIENTAS PARA EJERCER EL CONTROL	Posee una herramienta para ejercer el control.	15
	Existen manuales, Instructivos o procedimientos para el manejo de la herramienta.	15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.	30
SEGUIMIENTO AL CONTROL	Están definidos los responsables de la ejecución del control y del seguimiento.	15
	La frecuencia de ejecución del control y seguimiento es adecuada.	25
TOTAL		100

	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO, DESPLAZA EN LA MATRIZ DE CALIFICACION,EVALUACION Y RESPUESTA A LOS RIESGOS	
ENTRE 0-50	0	0
ENTRE 51-75	1	1
ENTRE 76-100	2	2

4.9 SOCIALIZACIÓN DE LA IMPORTANCIA DE LA GESTIÓN DE RIESGOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN

Debido a que los funcionarios de una entidad, son el eslabón más débil de la seguridad informática, se realiza una presentación sobre seguridad informática y seguridad de la información que permite a los funcionarios, conocer la importancia de la gestión de riesgos informáticos y conocer los riesgos que enfrentan para poder mitigarlos.