E.S.E. CAMU SANTA TERESITA

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

VIGENCIA 2025

Contenido

NORMOGRAMA

Ley 909 de 2004: “Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones”.

Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Ley 1712 de 2014: “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

Decreto Ministerial 1078 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Decreto Presidencial 1083 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

Decreto Presidencial 612 de 2018: “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”.

Decreto Presidencial 767 de 2022: “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Resolución Ministerial 00500 de 2021: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital”.

ISO/IEC 27001:2013: Tecnología de la información-Técnicas de seguridad-Sistemas de Gestión de la Seguridad de la Información (SGSI)- Requisitos.

ACUERDO N° 028 DEL 24 DE SEPTIEMBRE DE 1996: Emitido por el Concejo municipal de Santa Cruz de Lorica. "Por el cual se crea la E.S.E CAMU SANTA TERESITA"

ACUERDO N° 002 (11 DE MAYO DE 2020): "Por el cual se aprueba el plan de gestión gerencias 2020 — 2023 de la E.S.E CAMU SANTA TERESITA"

DEFINICIONES

- Activo: cualquier elemento que tenga valor para la organización.
- Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- Causa: Elemento específico que origina el evento.
- Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- Contexto interno: Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.
- Criterios de riesgos: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- Evaluación del Riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- Fuente: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- Identificación del riesgo: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos de este.
- Riesgo aceptable: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- Riesgo: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.
- Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

OBJETIVO

Establecer un plan de acción para el tratamiento de riesgos de seguridad y privacidad de la información, sobre los activos de información que soportan el cumplimiento de los objetivos organizacionales, conducentes a preservar la confidencialidad, integridad y disponibilidad de la información institucional, en atención al contexto organizacional de la E.S.E CAMU SANTA TERESITA, las capacidades y recursos disponibles, para fortalecer la confianza de los usuarios, y demás partes interesadas.

Específicos:

- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia y determinar su nivel de relevancia como incidente de seguridad de la información o no
- Identificar las principales amenazas que afectan los activos de información en la E.S.E CAMU SANTA TERESITA
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo de información.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.

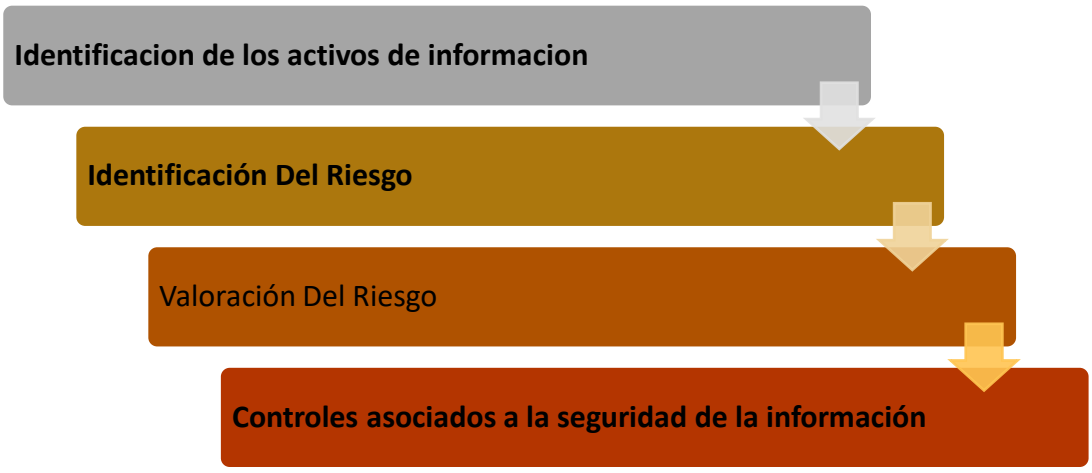
ALCANCE

La gestión de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información de la ESE CAMU SANTA TERESITA, identificados por cada uno de los procesos y que hacen parte del Registro de Activos de Información de la ENTIDAD; con base en las normas vigentes, la metodología definida por ella para la gestión del riesgo definida, las pautas y recomendaciones previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

DESARROLLO DEL PLAN

Identificación Y Valoración De Riesgos

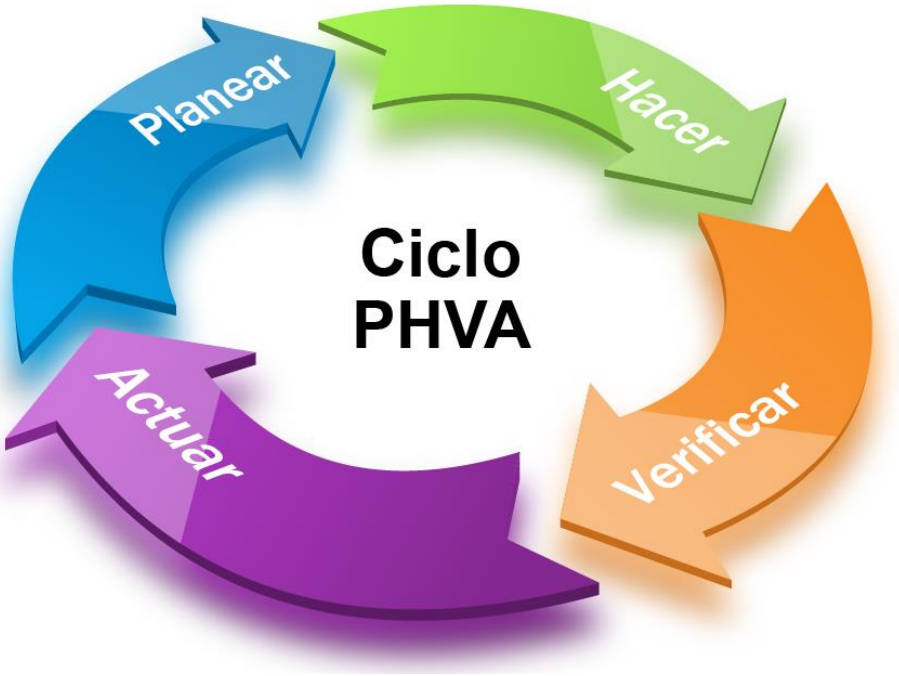
La técnica de análisis de riesgo para activos de información nos permite, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la entidad. Por ello se hace necesario contar con técnicas habituales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: Identificación de los activos de información, identificación del riesgo, valoración del riesgo y controles asociados a la seguridad de la información, en concordancia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6, emitida por el Departamento Administrativo de la Función Pública.



Diagonal 22 A N° 20-42 – B. Alto Kennedy – Telefonos: (064)7731763
Email: administrativa@esecamusantateresita.gov.co
Lorica – Córdoba
www.esecamusantateresita.gov.co

Metodología

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en adelante MSPI en la E.S.E CAMU SANTA TERESITA, toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, definiendo las siguientes fases de implementación del MSPI



De igual manera El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por los siguientes Hitos o actividades:

Programación y Agendamiento de Entrevistas

En esta fase se seleccionan los procesos incluidos en el alcance del SGSI de la ESAP y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.

Entrevista con los Líderes

Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

Identificación y Calificación de Riesgos

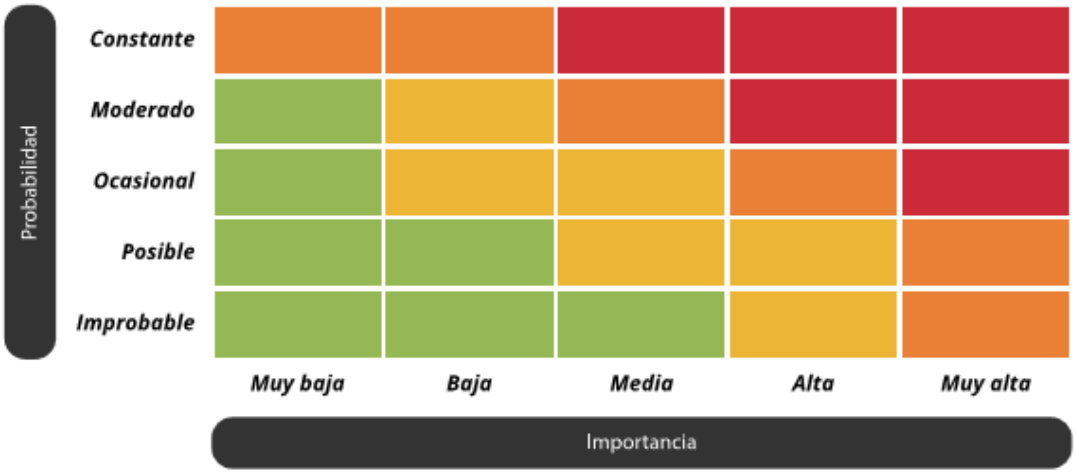
En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

Valoración del Riesgo Residual

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

Mapas De Calor Donde Se Ubican Los Riesgos

Luego se procede a ubicar los riesgos en un mapa de calor teniendo en cuenta probabilidad e importancia, para visualizar su comportamiento a medida que se van aplicando los controles.



Tratamiento De Riesgos De Seguridad De La Información

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones

aplicando el apetito de riesgos definido por la E.S.E CAMU SANTA TERESITA.

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos

identificados con el apoyo de la Oficina de sistemas e informática, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos.

Controles recomendados

Frente a los riesgos encontrados con estrategia de mitigación, para su gestión se proponen los controles de la norma ISO 27001

Seguimiento Y Control

El seguimiento y control se realiza de acuerdo con la GUÍA PARA LA ADMINISTRACIÓN DE RIESGO v6.

CRONOGRAMA

Los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control y las fechas para implementar dichos controles, la oficina de sistemas e informática apoyará el proceso de definición de los controles con los líderes de cada uno de los grupos o dependencias.

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN																								
ACTIVIDAD	DIC-23				ENE-24				FEB-24				MAR-24				ABR-24				MAY-24			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1. Realizar el Diagnostico																								
2.Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información																								
3.Realizar la Identificación de los Riesgos con los líderes del Proceso																								
4.Valorar del riesgo y del riesgo residual																								
5.Realizar Mapas de calor donde se ubican los riesgos																								
6.Plantear al plan de tratamiento de riego aprobado por los lideres																								
SEGUIMIENTO Y CONTROL																								

RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento. Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas bajo la responsabilidad de la Oficina de sistemas, los recursos de inversión serán socializados con el área gerencial de la entidad.

RESPONSABLES

1. Representante Legal de la Entidad y Comité de Gestión y Desempeño Institucional:

Aprobar los documentos de Alto Nivel

2. Coordinador Administrativo y Coordinador Operativo: Velar por la implementación de los planes.

3. Responsable de Seguridad Digital / CIO / Enlace TIC: Coordinar las actividades de implementación y apoyar en la definición de controles para mitigar los riesgos de seguridad.

APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado

conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Kathia Sánchez Peinado **Cargo:** Coordinadora área de Sistemas		