E.S.E ALEJANDRO PRÓSPERO REVEREND

GUIA DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Santa Marta D.T.C.H - Magdalena

2024

TABLA DE CONTENIDO

INTRODUCCION

En la actualidad, la información se ha convertido en uno de los activos más valiosos para las organizaciones, siendo vital para la toma de decisiones, la operatividad y la calidad del servicio. En este sentido, la gestión efectiva de los riesgos de seguridad de la información se vuelve fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos sensibles y personales.

La E.S.E Alejandro Prospero Reverend, comprometida con la protección de la información y la eficiencia en la prestación de servicios de salud ha desarrollado esta guía con el propósito de brindar un marco de referencia específico y adaptado a las necesidades y desafíos que enfrenta en materia de seguridad de la información.

A lo largo de este documento, se planteará la metodología, herramientas y recomendaciones específicas para identificar, evaluar y gestionar los riesgos de seguridad de la información de manera integral y efectiva en la entidad. El propósito es el fortalecimiento de la seguridad de la información, la protección de los datos de los usuarios y la continuidad de los servicios de salud que se brindan.

OBJETIVO

Desarrollar e implementar un plan integral de gestión de riesgos de seguridad y privacidad de la información en la E.S.E Alejandro Prospero Reverend, que abarque la identificación, evaluación, tratamiento y monitoreo continuo de los riesgos asociados a la seguridad y privacidad de los datos

ALCANCE

Esta guía deberá ser utilizada como referencia para identificar, analizar, evaluar y monitorear los riesgos de seguridad y privacidad de la información.

La E.S.E. Alejandro Prospero Reverend ha establecido un proceso para la gestión de los riesgos relacionados con la seguridad y privacidad de la información, el cual abarca varias fases: la identificación de los riesgos asociados a los activos de información priorizados, el análisis de dichos riesgos, la valoración, la gestión de los mismos mediante estrategias de tratamiento, y el monitoreo y evaluación del riesgo residual. En caso de que un riesgo no se mitigue satisfactoriamente o persista en un nivel inaceptable, se vuelve a evaluar y se redefine su tratamiento.

MARCO DE REFERENCIA

Para la gestión de los riesgos y peligros en la E.S.E Alejandro Prospero Reverend se toman en cuenta los siguientes documentos:

- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”
- Ley 1523 de 2012. “Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones”
- 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 1072 de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo”
- Norma NTC ISO 22301: 2012 Sistema de Gestión de Continuidad de Negocio
- Norma NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información.
- Norma Técnica Colombiana NTC ISO 31000:2018. Gestión del Riesgo
- GTC 45 Guía Técnica Colombiana para la Identificación de los Peligros y la Valoración de los Riesgos en Seguridad y Salud Ocupacional - 2015
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Riesgos de Gestión, Corrupción y seguridad Digital – DAFP - octubre 2018.
- Modelo de Seguridad y Privacidad de la Información de MinTic – 2016.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

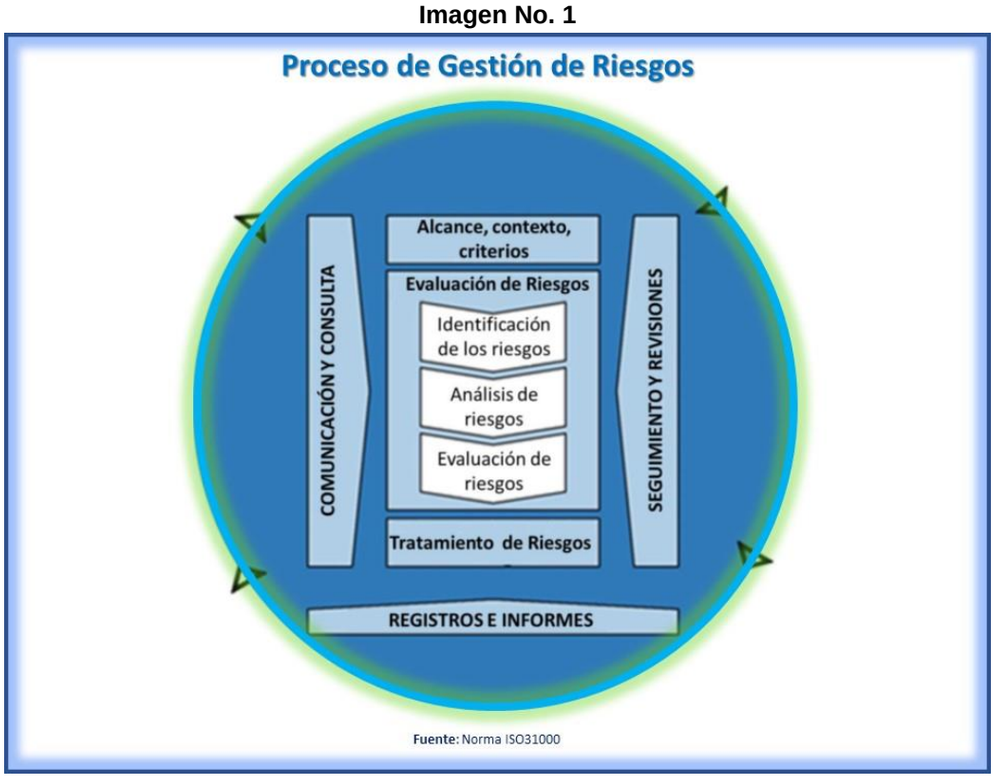
La gestión de riesgos de Seguridad y Privacidad de la Información le permite a la E.S.E Alejandro Prospero Reverend realizar una identificación, análisis y un tratamiento a los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones con el fin de prevenir la materialización de estos.

La gestión de riesgos de la E.S.E Alejandro Prospero Reverend se realiza con base en lo establecido en los siguientes documentos de referencia:

- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Departamento Administrativo de la Función Pública.
- Norma ISO/IEC 27001:2022
- Norma Técnica Colombiana NTC ISO 31000:2018. Gestión del Riesgo

Comprende las fases descritas en la siguiente imagen:

Imagen No. 1



Fuente: Norma ISO31000

DESCRIPCIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos de Seguridad de la Información se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”.

Para el riesgo identificado se deben asociar el grupo de activos o activos priorizados del proceso y sub-procesos y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

ESTABLECER EL CONTEXTO

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de la Entidad. A partir del contexto es posible establecer las causas de los riesgos a identificar.

Contexto Externo: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como:

CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4

Contexto Interno: Se determinan las características o aspectos esenciales del entorno en el cual la organización busca alcanzar sus objetivos. Se pueden considerar factores como:

CONTEXTO INTERNO	FINANCIEROS: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4

Contexto del Proceso: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo páginas 8 y 9.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4

IDENTIFICACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN PRIORIZADOS

Como primer paso para detectar los riesgos relacionados con la seguridad de la información, es esencial confirmar cuáles son los activos priorizados dentro del inventario de activos de información. Además, se requiere examinar diversos aspectos de la entidad, como su infraestructura física, espacios de trabajo y entorno en general, con el fin de identificar las posibles circunstancias que podrían amenazar la consecución de los objetivos establecidos para la organización.

Para facilitar el ejercicio de identificación, análisis, valoración y definición de las actividades de los planes de tratamiento se establece el Formato “Matriz de Riesgos de Seguridad de la Información” como herramienta de recolección de la información de los riesgos, la cual será usada para la generación del ID, desarrollar las mesas de trabajo en los casos que aplique y solicitudes para el registro de nuevos riesgos en el sistema de información.

Los activos de información priorizados son los que pasan a gestión de riesgos porque finalizada su identificación y valoración cumplen con alguna de las siguientes premisas:

- Cuando en alguno de los criterios de confidencialidad, integridad y disponibilidad su calificación sea igual a tres (3). En este caso, deberá construirse un riesgo del activo de información asociado con el principio que haya quedado con esa valoración.
- Todos los activos que hayan quedado con un nivel de importancia alta deberán pasar a identificación y evaluación de riesgos.

ROLES CON SUS RESPONSABILIDADES

Para iniciar la fase de identificación de riesgos como primera medida se establecen los siguientes roles con sus responsabilidades:

Gestor de riesgos de seguridad de la información:

- Proporcionar las políticas, procedimientos y controles de seguridad de la información.
- Liderar y supervisar la implementación del programa de gestión de riesgos de

seguridad de la información.
- Apoyar en la identificación, evaluación y tratamiento de los riesgos de seguridad de la información en la organización.

Equipo de Seguridad de la Información:

- Evaluar y gestionar los riesgos de seguridad de la información en las diferentes áreas de la organización.
- Apoyar en el diseño y en la implementación de las medidas de control necesarias para mitigar los riesgos identificados.
- Realizar seguimiento y monitoreo continuo de los riesgos y controles de seguridad de la información.

Responsables de Áreas:

- Identificar los activos de información críticos en sus respectivas áreas y los riesgos asociados.
- Implementar los controles de seguridad de la información recomendados por el equipo de gestión de riesgos.
- Reportar de manera oportuna cualquier incidente de seguridad de la información que se presente en su área.

Funcionarios y Contratistas de la E.S.E. Alejandro Prospero Reverend:

- Cumplir con las políticas y procedimientos de seguridad de la información establecidos.
- Participar en actividades de formación y concientización sobre seguridad de la información.
- Informar de manera inmediata cualquier incidente de seguridad o vulnerabilidad que identifiquen en su trabajo diario.

CODIFICACIÓN Y REDACCIÓN DE RIESGOS

Para realizar la codificación de los riesgos se utilizó como base el instructivo para la elaboración y control de documentos de la E.S.E Alejandro Prospero Reverend. A cada riesgo se le debe asignar un identificador de la siguiente forma:

- Dos últimas cifras del año de la identificación del riesgo.
- Sigla del tipo de Proceso
- Guion medio
- Sigla del Proceso
- Consecutivo del riesgo en tres cifras

Ejemplo:

Dos últimas cifras del Año	Guion	Sigla del Tipo de Proceso	Guion	Sigla del Proceso	Guion	Consecutivo del riesgo en tres cifras
24	-	A	-	SIT	-	1

Tabla No.1 - Abreviaturas para la identificación de procesos
ESE Alejandro Próspero Reverend

Tipo de Proceso	Sigla de Tipo de Proceso	Proceso	Sigla de Proceso
ESTRATÉGICO	E	Gerencia	GER

		Planeación estratégica	PLA
		Comunicaciones y Prensa	CYP
		Defensa y representación judicial	DYJ
		Control Interno Disciplinario	CID
		Contratación	CON
MISIONALES	M	Consultas: Medicina general, Enfermería, Odontología general, Optometría, Pediatría, Ginecología.	CMG
		Atención de la Ruta de Promoción y Mantenimiento de la Salud PYM	PYM
		Atención de la Ruta Materno Perinatal	RMP
		Atención en la Ruta de Atención de Grupos Especiales	RGE
		Hospitalización	HOS
		Urgencias	URG
		Medicina general	MEG
		Promoción y mantenimiento de la salud	PYM
		Transporte asistencial básico	TAB
		Servicio farmacéutico	FAR
		Imágenes diagnósticas: Rayos x, Ecografías	IRX
		Laboratorio citologías cérvico-uterinas	LAC
		Laboratorio clínico	LAB
		Terapia respiratoria	TER
		Información y orientación	IYO
		Gestión de PQRS	PQR
		Asociación de Usuarios	ADU
		Vigilancia epidemiológica	VEP
APOYO	A	Costos	CTS
		Administración del talento humano	THO
		Sistema de información y telecomunicaciones	SIT
		Mantenimiento	MNT
		Servicios generales	SGN
		Vigilancia	VIG
		Parque Automotor	PAM
		Almacén	ALM
		Gestión documental	GDM
		Pagos	PAG
		Facturación y cartera	FYC
		Presupuesto	PRE
		Contabilidad	CON
		Sistema de Gestión de la Seguridad y Salud en el trabajo	SST
		Gestión Ambiental	GAM
EVALUACIÓN	EV	Programa de auditoría para el mejoramiento de la calidad (PAMEC)	PMC
		Habilitación en plataforma REPS de novedades de servicio	RPS
		Sistemas de información para la calidad	SIC
		Relación con entes de control	REC

		Evaluación y seguimiento	EYS
		Liderazgo estratégico	LET
		Evaluación a la gestión del riesgo	EGR
		Enfoque hacia la prevención	EPR

Fuente: Oficina Asesora de Planeación, ESE Alejandro Próspero Reverend.

IDENTIFICACIÓN DE AMENAZAS:

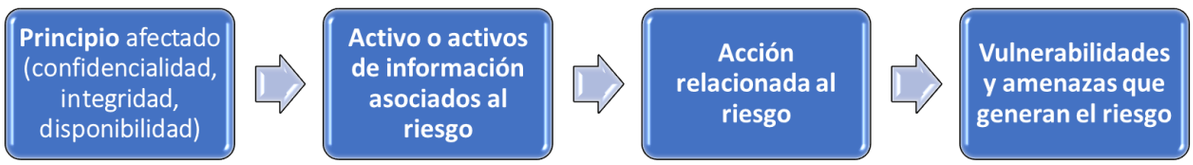
Las amenazas representan situaciones potenciales que pueden causar daños a los activos de la organización, incluyendo la información, los procesos y los sistemas. Estas amenazas pueden ser de origen natural o humano, y pueden ser tanto accidentales como deliberadas. Es recomendable identificar todas las posibles fuentes de amenazas, tanto accidentales como intencionales. Algunas categorías comunes de amenazas incluyen acciones no autorizadas, daño físico, fallas técnicas, desastres naturales, entre otras. Es importante identificar las amenazas de manera genérica y por tipo, para comprender mejor los riesgos a los que la organización está expuesta.

IDENTIFICACIÓN DE VULNERABILIDADES:

Las vulnerabilidades son debilidades o fallos en los activos de la organización que podrían ser explotados por las amenazas para causar daños. Para identificar correctamente las vulnerabilidades, es necesario conocer las amenazas comunes, tener un inventario de activos y conocer los controles existentes. Las vulnerabilidades pueden encontrarse en diversas áreas, como la organización, los procesos y procedimientos, el personal, el ambiente físico, la configuración del sistema de información, el hardware, el software, los equipos de comunicaciones y la dependencia de partes externas. Es importante recordar que la presencia de una vulnerabilidad no causa daños por sí misma; se requiere la presencia de una amenaza para explotarla.

Para la redacción de un riesgo se debe tener en cuenta la siguiente estructura:

Imagen No. 2: Estructura de redacción de un riesgo de seguridad y privacidad de la información, seguridad digital y continuidad del negocio



Ejemplos:

- Pérdida de **integridad** de (activo o activos de información), debido a (actividad/situación + vulnerabilidades y amenazas)

  Pérdida de integridad de la base de datos de nómina, debido a la modificación de información sin autorización por la falta de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil.

- Pérdida de **confidencialidad** de (activo o activos de información relacionados en elriesgo), debido a (actividad/situación+ vulnerabilidades y amenazas).

  Pérdida de confidencialidad de las historias clínicas, debido al acceso no autorizado a los computadores desatendidos por los funcionarios, por la falta de

Políticas de Seguridad de la Información, Bloqueo de equipos, escritorios limpios y a la falta de conciencia o conocimiento de los funcionarios

- Pérdida de **disponibilidad** del (activo o activos de información), debido a (actividad/situación+vulnerabilidades y amenazas).

Pérdida de disponibilidad y confidencialidad de los computadores y portátiles, por fallas en alguno de sus componentes debido al uso incorrecto de hardware y software, falta de apropiación, nivel de obsolescencia del parque computacional, red energética inestable y daños accidentales

La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (incidente), por lo que es preciso identificar lo siguiente:

- Proceso
- Dueño o responsable del riesgo
- Activos y/o servicios
- Riesgo
- Clasificación del riesgo
- Fuentes, Causas, Amenazas y vulnerabilidades

Una vez descrito el riesgo, se deberá asociar de acuerdo a la siguiente clasificación:

- ***Riesgos de Seguridad Digital***: Los riesgos de seguridad digital se refieren a las vulnerabilidades en los sistemas y aplicaciones de una organización que pueden ser explotadas por ciberdelincuentes para acceder, modificar o destruir información crítica. Estos riesgos incluyen la presencia de fallas en la protección de datos, como contraseñas débiles o falta de cifrado, así como la exposición a diversos tipos de ataques cibernéticos, como malware, phishing y ransomware, que pueden comprometer la seguridad de los activos digitales de la organización.

- ***Riesgos de Seguridad de la Información***: Los riesgos de seguridad de la información se centran en la confidencialidad, integridad y disponibilidad de los datos de una organización. La confidencialidad comprometida puede resultar en la divulgación de información sensible a personas no autorizadas, mientras que la integridad de la información afectada puede llevar a la alteración no autorizada de datos, comprometiendo su veracidad. Por otro lado, la disponibilidad de sistemas comprometida puede ocasionar que los sistemas no estén disponibles cuando se necesiten, debido a fallas técnicas o ataques que afecten su funcionamiento.

- ***Riesgos de Continuidad de la Operación***: Los riesgos de continuidad de la Operación se relacionan con la capacidad de una organización para mantener sus operaciones en situaciones adversas. Estos riesgos incluyen la posibilidad de interrupciones en las operaciones debido a eventos como desastres naturales, ciberataques o pandemias, que pueden afectar la capacidad de la organización para funcionar de manera eficiente. Asimismo, la pérdida de datos críticos y el incumplimiento de regulaciones legales también representan riesgos significativos que pueden impactar la continuidad y la reputación de la organización.

CONSECUENCIAS POSITIVAS Y NEGATIVAS

Se deben considerar las consecuencias positivas y negativas, teniendo en cuenta la estandarización que se relaciona a continuación.

Consecuencias Negativas

- ***Pérdida financiera***: La materialización de un riesgo puede resultar en pérdidas financieras para la organización, incluyendo multas, sanciones o costos de recuperación.
- ***Daño a la reputación***: Los riesgos materializados pueden dañar la reputación de la organización, afectando la confianza de los clientes, proveedores y otras partes interesadas.
- ***Interrupción del Servicio***: Algunos riesgos pueden provocar la interrupción de los servicios, lo que resulta en pérdida de productividad y posibles incumplimientos.
- ***Incumplimiento de normativas y regulaciones***: La materialización de ciertos riesgos puede llevar al incumplimiento de normativas, leyes y regulaciones, lo que puede resultar en multas, sanciones y pérdida de licencias comerciales.
- ***Daños a la Infraestructura Física***: Riesgos como desastres naturales, incendios o actos de vandalismo pueden causar daños a la infraestructura física de la organización, incluyendo edificios, instalaciones y equipos.
- ***Impacto en la seguridad de la información***: La materialización de riesgos de seguridad de la información puede resultar en la pérdida, robo o divulgación no autorizada de datos sensibles, lo que pone en riesgo la confidencialidad e integridad de la información.
- ***Daños a la Infraestructura Tecnológica***: fallos de hardware o errores humanos pueden resultar en la pérdida de datos críticos para la organización, lo que afecta la integridad y disponibilidad de la información.
- ***Sanciones***: La materialización de riesgos relacionados con prácticas éticas o legales inapropiadas puede resultar en sanciones por parte de organismos de supervisión, lo que afecta la reputación y la credibilidad de la organización.
- ***Reprocesos***: La materialización de riesgos relacionados con errores en los procesos internos de la organización puede requerir reprocesos para corregir las fallas y garantizar la calidad de los productos o servicios.
- ***Llamados de Atención***: Los llamados de atención son advertencias formales emitidas a Funcionarios y Contratistas o equipos dentro de la organización como resultado de la violación de políticas y procedimientos de seguridad de la Información

Consecuencias Positivas:

- ***Mejora en los procesos***: La identificación de un riesgo puede llevar a una revisión y mejora de los procesos existentes para hacerlos más eficientes y efectivos.
- ***Mayor conciencia de riesgos***: La materialización de un riesgo puede aumentar la conciencia de los riesgos en la organización y promover una cultura de gestión de riesgos más sólida.
- ***Oportunidades de aprendizaje***: La gestión de un riesgo puede proporcionar oportunidades de aprendizaje y desarrollo de capacidades para el personal involucrado.

- ***Optimización de la estructura organizativa***: La gestión de riesgos permite identificar las necesidades de personal y asignar recursos de manera más eficiente, lo que mejora la productividad y la colaboración entre los equipos.
- ***Mejora de la eficiencia operativa***: Identificar y mitigar los riesgos relacionados con la tecnología puede permitir a la organización optimizar el uso de sus recursos tecnológicos, mejorando la eficiencia de los procesos y reduciendo los tiempos de inactividad.

ANÁLISIS DEL RIESGO

El análisis de riesgos es un proceso cuantitativo y cualitativo donde se pretende determinar la probabilidad de ocurrencia de una eventualidad y el impacto que pueda causar la

materialización del riesgo.

- La Probabilidad representa el número de veces que el riesgo se ha presentado opuede presentarse en un determinado tiempo.

- El impacto hace referencia a magnitud de sus efectos en caso de materialización.

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Este proceso se hace partiendo de la experiencia de los funcionarios y el acompañamiento metodológico del Gestor de Riesgos de Seguridad de Información. Se puede realizar el análisis de riesgos utilizando una o varias de las siguientes técnicas:

- Entrevistas
- Cuestionarios
- Listas de chequeo
- Tormenta de ideas
- Grupo de expertos
- Opinión de expertos

Aunque inicialmente la mayoría de los riesgos serán analizados de forma cualitativa a medida que el proceso de gestión de riesgos madura se tendrán datos relevantes que permitirá hacer un análisis cuantitativo y así se obtendrá un mayor nivel de exactitud en la calificación de probabilidad, impacto y eficacia de controles.

A continuación, se mencionan 4 aspectos que se deben tener en cuenta para realizar un adecuado análisis de riesgo:

- Inventario de activos de información en el cual se hayan asignado por cada principio (confidencialidad, integridad y disponibilidad) un valor conforme a su importancia.
- Identificar cada uno de los activos priorizados y tener una relación de las amenazas y vulnerabilidades que le pueden afectar.
- Determinar las actividades o situaciones que conllevan a la materialización de riesgos y determinar cuántas veces se puede ejecutar o presentar esta en el año.
- Determinar el potencial de afectación que tendría un riesgo sobre la entidad en caso dematerializase.

El análisis de riesgos tiene como objeto priorizar los riesgos identificados de acuerdo con el nivel inherente (criticidad) obtenido, evaluando y determinando la probabilidad, el impacto de acuerdo con las vulnerabilidades y amenazas identificadas sin tener en cuenta los controles existentes.

ANÁLISIS DE LA PROBABILIDAD

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Los datos estadísticos que pueden servir como base para valorar la probabilidad pueden ser:

- Datos Internos (incidentes presentados con el riesgo o experticia y/o conocimiento

del dueño del riesgo).

- Datos Externos (Datos oficiales reportados por entes regulatorios y competentes quese relacionen con riesgos que afecten el contexto externo).

Tabla No. 2: Probabilidad

PROBABILIDAD	CONCEPTO	FRECUENCIA DE LA ACTIVIDAD
100%	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 101 veces por año
80%	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 51 veces al año y máximo 100 veces por año.
60%	Media	*La actividad que conlleva el riesgo se ejecuta de 24 a 50 veces por año*
40%	Baja	*La actividad que conlleva el riesgo se ejecuta de 3 a 23 veces por año*
20%	Muy baja	*La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.*

ANÁLISIS DEL IMPACTO

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Tabla No. 3: Impacto

Impacto	Afectación Económica	Reputacional
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país
Alto 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.

MAPA DE CALOR

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

La siguiente imagen corresponde al mapa de calor, para establecer el nivel del riesgo, se toma la calificación de probabilidad resultante de la tabla 1 y se ubica verticalmente, después la calificación de impacto de la Tabla 2 y se ubica de forma horizontal, luego se establece el punto de intersección entre las dos y este punto corresponderá al nivel de riesgo.

Imagen No. 3: Análisis del Riesgo Inherente - Probabilidad por Impacto

Probabilidad	Impacto: Leve 20%	Menor 40%	Moderado 60%	Alto 80%	Catastrófico 100%
Muy Alta 100%	Alto (Muy alta - Leve)	Alto (Muy Alta - Menor)	Alto (Muy Alta - Moderado)	Alto (Muy Alta - Mayor)	Extremo (Muy Alta - Catastrófico)
Alta 80%	Moderado (Alta - Leve)	Moderado (Alta - Menor)	Alto (Alta - Moderado)	Alto (Alta - Mayor)	Extremo (Alta - Catastrófico)
Media 60%	Moderado (Media - Leve)	Moderado (Media - Menor)	Moderado (Media - Moderado)	Alto (Media - Mayor)	Extremo (Media - Catastrófico)
Baja 40%	Bajo (Baja - Leve)	Moderado (Baja - Menor)	Moderado (Baja - Moderado)	Alto (Baja - Mayor)	Extremo (Baja - Catastrófico)
Muy Baja 20%	Bajo (Muy Baja - Leve)	Bajo (Muy Baja - Menor)	Moderado (Muy Baja - Moderador)	Alto (Muy Baja - Mayor)	Extremo (Muy Baja - Catastrófico)

Escala de valoración:	Extremo	Alto	Moderado	Bajo

VALORACIÓN DEL RIESGO

La fase de valoración permite evaluar la efectividad de los controles existentes para mitigar los riesgos identificados. En esta etapa, se analizan y se asignan puntajes a los controles implementados con el fin de determinar su capacidad para prevenir, detectar o corregir los riesgos que puedan afectar los objetivos de la organización.

ASPECTOS PARA TENER EN CUENTA EN LA VALORACIÓN DE CONTROLES:

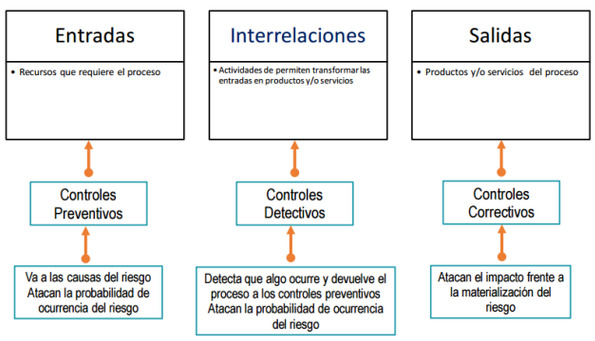
- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo

TIPOLOGÍAS DE CONTROLES:

- ***Control Preventivo***: Accionado en la entrada del proceso para establecer condiciones que aseguren el resultado final esperado.
- ***Control Detectivo***: Accionado durante la ejecución del proceso para detectar el riesgo, aunque puede generar reprocesos.
- ***Control Correctivo***: Accionado en la salida del proceso después de que se materializa el riesgo, con costos implícitos.

Para comprender esta estructura conceptual, en la figura 1 se consideran 3 fases globales del ciclo de un proceso as

Imagen No. 4: Ciclo del proceso y las tipologías de controles



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

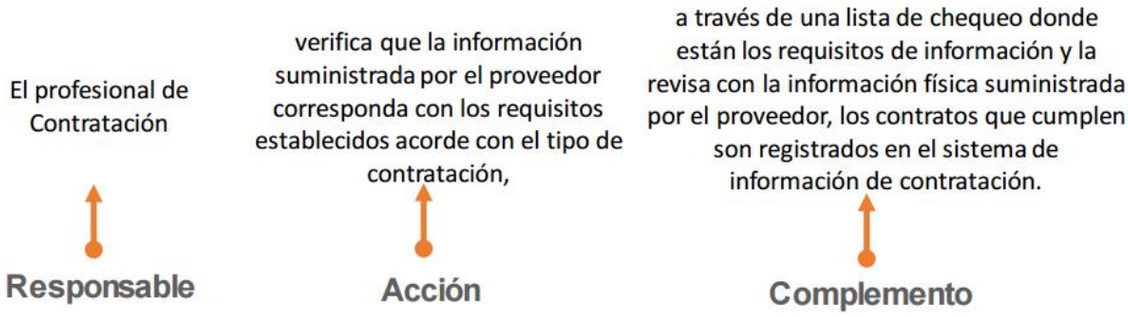
ESTRUCTURA DE LA VALORACIÓN DE CONTROLES:

para una adecuada redacción del control se propone una estructura que facilitará entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- ***Responsable de ejecutar el control***: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- ***Acción***: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- ***Complemento***: corresponde a los detalles que permiten identificar claramente el objeto del control.

En la siguiente figura se establece un ejemplo bajo esta estructura.

Imagen No. 5: Ejemplo aplicado bajo la estructura propuesta para la redacción del control



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

DISEÑO DEL CONTROL:

Los criterios de evaluación del control con relación al diseño son:

Tabla No. 4: Calificación diseño del control

	Calificación		
Criterios	**Fuerte (3)**	**Moderado (2)**	**Débil (1)**
¿Tiene Responsable asignado?	Cuando cumple con todos los criterios establecidos para evaluar el diseño del control	Cuando no cumple con uno o dos de los criterios establecidos para evaluar el diseño	Cuando no cumple con ninguno de los criterios establecidos para evaluar el diseño
¿Tiene Periodicidad definida?			
¿Está documentado?			

¿Existen evidencias de la ejecución?		del control	del control

EJECUCIÓN DEL CONTROL:

Los criterios de evaluación del control con relación a su ejecución son:

Tabla No. 5: Calificación ejecución del control

Calificación	Criterio
Fuerte (3)	El control se ejecuta de manera consistente conforme a la periodicidad definido y cuenta contodas las evidencias correspondientes.
Moderado (2)	El control se ejecuta algunas veces por parte del responsable y cuenta con algunas evidencias.
Débil (1)	El control no se ejecuta por parte del responsable y no se tiene evidencia del cumplimiento.

FORTALEZA DE LOS CONTROLES:

Para calcular la efectivad de los controles se realiza la multiplicación entre el valor dado al diseño del control por la ejecución de mismo, como se indica en la siguiente tabla:

Tabla No. 6: Calculo de diseño vs ejecución del control efectividad del control

Diseño		Ejecución		(Diseño x Ejecución)
Fuerte	3	Fuerte	3	9
Fuerte	3	Moderado	2	6
Fuerte	3	Débil	1	3
Moderado	2	Fuerte	3	6
Moderado	2	Moderado	2	4
Moderado	2	Débil	1	2
Débil	1	Fuerte	3	3
Débil	1	Moderado	2	2
Débil	1	Débil	1	1

De lo anterior se determina si un control es efectivo, moderadamente efectivo o poco efectivo como se muestra en las siguientes tablas:

Tabla No. 7: Efectividad de Controles

DISEÑO	**Fuerte (3)**	**Poco efectivo (3)**	**Moderadamente efectivo (6)**	**Efectivo (9)**
	Moderado (2)	**Poco efectivo (2)**	**Moderadamente efectivo (4)**	**Moderadamente efectivo (6)**
	Débil (1)	**Poco efectivo (1)**	**Poco efectivo (2)**	**Poco efectivo (3)**
		Débil (1)	**Moderado (2)**	**Fuerte (3)**

Ejecución

Tabla No. 8: Resultado de la valoración del control

Valoración del control	
Efectivo	9
Moderadamente efectivo	4 a 8
Poco efectivo	1 a 3

VALORACIÓN DEL RIESGO POSTERIOR A LA EVALUACIÓN DE LOS CONTROLES:

Para calcular la probabilidad e impacto conforme a la ejecución de los controles se debe aplicar lo definido en la siguiente tabla, con esto se obtendrá la calificación del riesgo posterior a la implementación de estos, la cual será la que se tenga en cuenta para establecer el manejo:

Tabla No. 9: Criterios de Evaluación de los Controles para Disminuir Probabilidad e Impacto

Valoración del control o conjunto de controles.	Los controles ayudan a disminuir la probabilidad	Los controles ayudan a disminuir el impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de impacto
Efectivo	Directamente	Directamente	2	2
Efectivo	Directamente	Indirectamente	2	1
Efectivo	Directamente	No disminuye	2	0
Efectivo	No disminuye	Directamente	0	2
Moderadamente efectivo	Directamente	Directamente	1	1
Moderadamente efectivo	Directamente	Indirectamente	1	0
Moderadamente efectivo	Directamente	No disminuye	1	0
Moderadamente efectivo	No disminuye	Directamente	0	1

Fuente: Guía para la Administración de los Riesgos de Gestión Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas.

MANEJO DEL RIESGO

Las opciones de tratamiento que se pueden aplicar a los riesgos identificados son las siguientes:

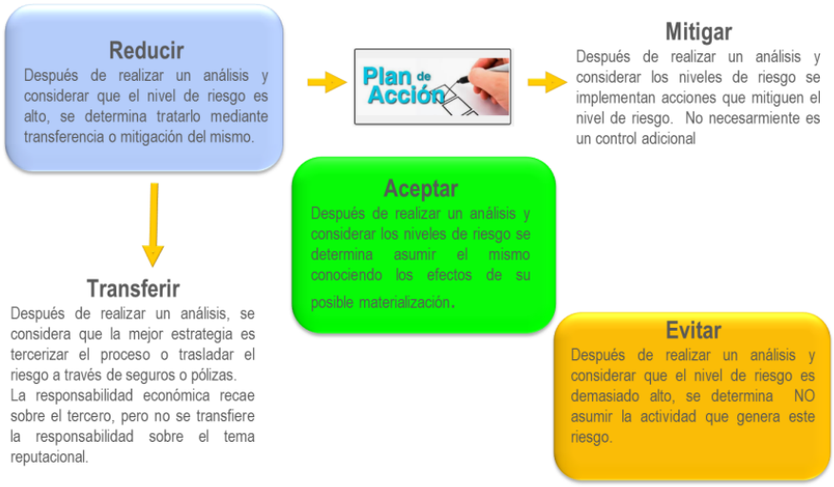
- ***Aceptar el riesgo:*** Consiste en reconocer la existencia del riesgo y decidir no tomar medidas adicionales para mitigarlo. Esta opción se elige cuando el riesgo es considerado aceptable y los costos de su tratamiento superan los beneficios esperados.

- ***Evitar el riesgo***: Implica tomar medidas para eliminar o reducir la exposición al riesgo, cancelando una actividad o un conjunto de actividades que puedan generar consecuencias no deseadas. Esta opción se aplica cuando los escenarios de riesgo identificados son considerados demasiado extremos y no pueden ser gestionados de manera efectiva.

- ***Compartir o transferir el riesgo***: Consiste en transferir parte del riesgo a terceros, como aseguradoras o socios comerciales, a través de contratos de seguros, acuerdos de responsabilidad compartida u otras formas de colaboración. Esta opción se utiliza para distribuir la responsabilidad del riesgo y reducir su impacto en la organización.

- ***Reducir el riesgo***: Implica implementar medidas para disminuir la probabilidad de ocurrencia o el impacto de un riesgo, a través de controles preventivos, detectivos o correctivos. Esta opción se aplica cuando el riesgo es considerado inaceptable y es necesario tomar acciones para mitigarlo.

Imagen No. 6: Opciones de Tratamiento para los riesgos identificados



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Al considerar estas opciones de tratamiento, la organización podrá seleccionar la estrategia más adecuada para gestionar sus riesgos de manera efectiva y proteger sus objetivos y activos frente a posibles amenazas.

Se puede aceptar el riesgo a decisión del dueño de los riesgos para aquellos que estén en nivel Bajo, que tengan identificados los controles existentes que se tienen implementados para que estén en ese nivel y que a su vez abarquen todas las causas.

La priorización del riesgo se determina de acuerdo con el tiempo de atención que implicará el plan de tratamiento y los controles a implementar:

Tabla No. 10: Priorización del riesgo

ORDEN DE PRIORIDAD	TIEMPO DE ATENCIÓN	TIEMPO SUGERIDO DE TRATAMIENTO
1	Corto plazo	Hasta 4 meses
2	Mediano plazo	De 4 a 8 meses
3	Largo plazo	De 8 meses en adelante

De acuerdo con los resultados obtenidos en la fase de identificación, análisis y valoración de riesgos, se definen los controles a implementar, estableciendo adicionalmente una serie de actividades a realizar con el propósito de mitigar los riesgos identificados.

Las actividades para implementar serán aquellas que el dueño del riesgo defina para tratar los riesgos aceptados, y debe estar asociado a los controles establecido en el anexo A de la norma ISO 27001/2013.

Para la definición de los planes de tratamiento es necesario tener en cuenta lo siguiente:

- **Control del Sistema de Gestión de Seguridad de la Información:** corresponde al nombre del control o controles descritos en el Anexo A de la ISO 27001/2013. Este debe estar relacionado con las actividades a implementar en el plan de tratamiento.

- **Actividades:** las actividades propuestas para el tratamiento deben impactar en la mitigación del riesgo (contrarrestar las vulnerabilidades y amenazas, principalmente las que no tienen un control asociado). Igualmente, debe estar relacionado con el control descrito en la opción “Nombre del control”. Su descripción debe iniciar con un verbo en infinitivo y establecer cómo se realiza, fecha de inicio, fecha de terminación y la evidencia del cumplimiento.

- **Responsable**: para cada actividad de tratamiento se debe definir el responsable de su ejecución.

MONITOREO

La fase de monitoreo es esencial en el proceso de gestión de riesgos de una entidad pública, ya que permite realizar un seguimiento continuo de la efectividad de las medidas de control implementadas y de la evolución de los riesgos identificados.

En esta etapa, se llevan a cabo actividades de supervisión y evaluación para garantizar que los controles sean eficaces y se ajusten a los cambios en el entorno organizacional.

El monitoreo se realizará a todos los riesgos identificados (bajo, moderado, alto y extremo) y en este se deberá indicar también si se ha materializado o no el riesgo.

EVALUACIÓN DEL RIESGO RESIDUAL

Una vez finalizado los planes de tratamiento, se procede a realizar la evaluación del nivel residual. La fase de evaluación del riesgo residual es crucial en el proceso de gestión de riesgos de una entidad pública, ya que permite determinar el nivel de riesgo que permanece después de la implementación de controles y medidas de mitigación.

RESULTADO

- Si el resultado de la evaluación del nivel residual es menor a la inherente, se concluyeque sus controles fueron adecuados y se pueden seguir implementando.
- Si el resultado de la evaluación del nivel residual es igual o superior a la evaluación inherente, se concluye que los controles no fueron adecuados por lo tanto se debe plantear un nuevo plan de tratamiento, hasta que el riesgo pueda mitigarse.
- La calificación del riesgo de esta fase será el insumo para iniciar la identificación de riesgos para la siguiente vigencia.

OPORTUNIDAD DE MEJORA

La oportunidad es la consecuencia positiva frente al resultado del tratamiento del Riesgo, lo anterior quiere decir que puede identificarse una oportunidad de mejora conforme a las consecuencias positivas.

MATERIALIZACIÓN

Cuando un riesgo se materializa, es fundamental seguir un plan de acción específico para gestionar la situación de manera efectiva y minimizar sus impactos negativos. A continuación, se presentan los pasos que se deben seguir en caso de que un riesgo se materialice:

- ***Identificación y Evaluación del Impacto***: En primer lugar, identificar y evaluar el impacto real del riesgo materializado en la entidad. Esto implica comprender la magnitud de las consecuencias y cómo afecta a los objetivos institucionales.

- ***Comunicación***: Es importante comunicar de manera oportuna y transparente la materialización del riesgo a todas las partes interesadas relevantes, incluidos los responsables de la toma de decisiones, el equipo de gestión de riesgos y otros involucrados.

- ***Activación del Plan de Contingencia***: Si la entidad cuenta con un plan de contingencia previamente establecido para el riesgo en cuestión, este debe ser activado de inmediato. El plan de contingencia proporcionará las acciones específicas a seguir para mitigar los impactos del riesgo materializado.

- ***Análisis de Causa Raíz***: Realizar un análisis de causa raíz para comprender las razones detrás de la materialización del riesgo. Identificar las causas subyacentes ayudará a implementar medidas preventivas para evitar que el riesgo se repita en el futuro.

- ***Implementación de Medidas Correctivas***: Basándose en el análisis de causa raíz, se deben implementar medidas correctivas para abordar las deficiencias identificadas y fortalecer los controles internos para prevenir la materialización del riesgo en el futuro.

- ***Monitoreo y Seguimiento***: Es fundamental monitorear de cerca la efectividad de las medidas correctivas implementadas y realizar un seguimiento continuo para asegurarse de que el riesgo materializado esté bajo control y no vuelva a ocurrir.

- ***Lecciones Aprendidas***: Finalmente, es importante documentar las lecciones aprendidas de la materialización del riesgo, para mejorar el proceso de gestión de riesgos y fortalecer la capacidad de la entidad para enfrentar situaciones similares en el futuro

CONCLUSIONES

La gestión efectiva de los riesgos de seguridad de la información es el pilar fundamental para salvaguardar la confidencialidad, integridad y disponibilidad de los datos en la E.S.E Alejandro Prospero Reverend.

La identificación y valoración de los riesgos de seguridad de la información nos capacita para implementar medidas preventivas que contrarresten posibles amenazas y resguarden la información crítica de la entidad.

Es fundamental establecer un marco de referencia específico y adaptado a las necesidades de la E.S.E Alejandro Prospero Reverend en el ámbito de la seguridad de la información, con el propósito de fortalecer la protección de los datos de los usuarios y asegurar la continuidad de los servicios de salud que se ofrecen.

Esta guía refleja la importancia de una gestión proactiva y eficiente de los riesgos de seguridad de la información en la E.S.E Alejandro Prospero Reverend, con el firme propósito de garantizar la protección de la información y la continuidad de nuestros servicios.