INFORME DIAGNOSTICO Y ANALISIS PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

OFICINA DE PLANEACION INSTITUCIONAL

INTRODUCCIÓN

La seguridad de la información es un aspecto fundamental para cualquier organización en la era digital actual. Con la creciente dependencia de la tecnología y la proliferación de amenazas cibernéticas, es imperativo que las entidades implementen medidas efectivas para proteger la confidencialidad, integridad y disponibilidad de sus datos.

El presente documento contiene el diagnostico y analisis del Tratamiento de Riesgos de Seguridad de la Información se encuentra fundamentado en la norma ISO/IEC 27005:2018, la cual proporciona directrices detalladas para establecer, implementar, mantener y mejorar continuamente un proceso de gestión de riesgo de seguridad de la información dentro de una organización.

El objetivo principal de este plan es identificar, evaluar y tratar los riesgos de seguridad de la información de manera eficiente y efectiva, con el fin de proteger los activos de información críticos y garantizar la continuidad de las operaciones comerciales.

Al seguir los principios y procesos establecidos en la norma ISO/IEC 27005:2018, INDEPORTES CAUCA tendrá la potestad de:

- Identificar y comprender los riesgos de seguridad de la información a los que está expuesta.
- Evaluar la probabilidad y el impacto de dichos riesgos en función de los activos de la información y los objetivos de negocio.
- Seleccionar y aplicar medidas de control adecuadas para mitigar o reducir los riesgos a un nivel aceptable.
- Monitorear y revisar periódicamente el entorno de seguridad de la información para adaptarse a cambios en el panorama de amenazas y en las necesidades de la organización.

Este documento proporcionará un marco estructurado y coherente para la gestión de riesgos de seguridad de la información, alineado con las mejores prácticas internacionales y las recomendaciones de la norma ISO/IEC 27005:2018. Al adoptar este enfoque, INDEPORTES CAUCA fortalecera su postura de seguridad y contara con la confianza de sus partes interesadas en tema de la protección de la información.

OBJETIVOS

Objetivo General

- Reducir riesgos de la información en INDEPORTES – CAUCA apoyándonos con la norma ISO/IEC 27005. Gestión de riesgos de la Seguridad de la Información.

Objetivos Específicos

- Establecer un inventario completo de los activos de información de la organización, identificando aquellos que son críticos para el funcionamiento del negocio y requieren una protección especial.
- Realizar evaluaciones de riesgos periódicas para identificar las amenazas potenciales evaluando la probabilidad e impacto en los activos de información, clasificándolos según su nivel de criticidad.
- Proporcionar programas de capacitación y concientización en seguridad de la información para todo el personal, asegurando que estén familiarizados con las políticas, procedimientos y mejores prácticas de seguridad de la información.

ALCANCE

El alcance para este análisis y diagnostico del tratamiento de riesgos de seguridad y privacidad de la información es determinar qué riesgos específicos se tratan, como se abordan y quien será responsable de implementar las medidas de mitigación. Asegurar los sistemas de información físicos como hardware; equipos de cómputo, servidores y lógicos como software; bases de datos, aplicativos, sistemas operativos, etc. El objetivo es garantizar la protección adecuada de la información sensible y crítica de una organización aplicando la normativa en materia de auditoría de seguridad y seguridad informática para implementar planes estratégicos en busca de enfrentar los riesgos de INDEPORTES – CAUCA, se decidió que la información generada por esta entidad en cualquiera de estos soportes físicos y lógicos será utilizada en la forma prescrita por la normativa de seguridad informática de la empresa. Es por lo que se radica en aplicar la metodología PHVA (Planear, Hacer, Verificar y Actuar) relevante para mejorar procesos e implementar cambios como estrategia interactiva de resolución de problemas con una acción eficiente de los usuarios.

IDENTIFICACIÓN DEL RIESGO

La identificación de riesgos es fundamental para la gestión efectiva de los mismos en la entidad, ya que proporciona una base sólida para desarrollar estrategias de mitigación y gestión de riesgos, así como para tomar decisiones informadas sobre cómo asignar recursos y priorizar esfuerzos para proteger y fortalecer la entidad contra posibles adversidades.

El propósito principal es permitir a una entidad anticipar, comprender y gestionar los eventos y su capacidad para alcanzarlos.

Riesgos	Causas	Efectos
Posibilidad de pérdida, robo o fuga de Información	• Fallas en el proceso del respaldo de la información o restauración de esta. • Falta de control en el acceso de red a equipos no autorizados. • Falta de sistemas de seguridad informática (Firewall). • Falta de software actualizado y licenciado. • Falta de capacitación al personal sobre el uso de tecnologías. • Falta de políticas en el manejo de la	• Fugas de información. • Vulnerabilidades en los sistemas. • Malware. • Escalamiento de Privilegios. • Daño, eliminación o manipulación en información. • Ataques de denegación de servicios. • Menos control del tráfico de red. • Pérdida de imagen reputacional. • Costos financieros. • Incumplimiento de normativas.

	información de los empleados.	
Posibilidad de recepción de correos electrónicos no seguros.	• Falla en los filtros de seguridad o mala configuración del servidor. • Desconocimiento de los riesgos al acceder a correos falsos. • Falta de gestión en las contraseñas. • Falta de factor de doble autenticación.	• Ataques mediante troyanos. • Violación de privacidad. • Pérdida de datos y activos críticos. • Costos de mitigación y recuperación.
Posibilidad de daño en los equipos tecnológicos.	• Falta de mantenimiento. • Susceptibilidad a la humedad, el polvo y la suciedad. • Susceptibilidad a las variaciones de voltaje. • Mal uso de las herramientas tecnológicas. • Pérdida de archivos, documentos, bases de datos y configuraciones del sistema. • Los dispositivos dañados pueden representar riesgos de incendio.	• Fallas de hardware y software. • Ataques cibernéticos. • Robo y vandalismo.

	• Vulnerabilidad a ataques cibernéticos y violaciones de seguridad.	
Posibilidad de pérdida de conexión.	• Pérdida de datos no guardados. • Pérdidas de ingreso debido a la incapacidad de realizar transacciones. • Imposibilidad de acceder a sistemas remotos. • Incapacidad de enviar o recibir correos electrónicos. • Interrupción de sistemas de gestión empresarial y herramientas de seguimiento. • Desperdicio de tiempo y recursos.	• Problemas de hardware y software. • Interferencias electromagnéticas. • Mantenimiento o actualizaciones. • Red wifi inestable (Falta de red cableada). • Ancho de banda limitado.
Posibilidad de ataques cibernéticos.	• Robo de información financiera. • Espionaje industrial y robo de propiedad intelectual. • Espionaje gubernamental.	• Pérdida de datos confidenciales. • Pérdida de imagen reputacional. • Robo de identidad y fraude financiero. • Daño a la infraestructura crítica.

IDENTIFICACIÓN DE LAS AMENAZAS:

La identificación de amenazas es el proceso de reconocer y documentar todos los eventos potenciales o circunstancias que podrían causar daño o perjuicio a un sistema, activo, proceso o entidad. En el contexto de la seguridad de la información, la identificación de

amenazas implica identificar los diversos eventos o situaciones que podrían comprometer la confidencialidad, integridad o disponibilidad de los datos.

A continuación, se enlistan las posibles amenazas que podrían afectar la seguridad de la información:

Tipo de amenaza	Amenazas
Daños físicos	● Fuego ● Daños por agua ● Polución ● Destrucción de equipos o medios ● Polvo, corrosión, congelamiento
Eventos naturales	● Fenómeno climático ● Fenómeno sísmico ● Inundación
Pérdida de servicios esenciales	● Falla de energía eléctrica ● Falla de suministro de agua ● Falla de equipo de comunicaciones
Información comprometida	● Interceptación de señal ● Espionaje remoto ● Espionaje telefónico ● Robo de medios ● Robo de documentos, equipos, medios
Fallas técnicas	● Falla de equipo ● Funcionamiento deficiente de equipos ● Saturación de sistema ● Falla en el mantenimiento de sistema ● Funcionamiento deficiente de software
Acciones no autorizadas	● Uso no autorizado de equipo

	• Copia fraudulenta de software y de datos • Corrupción de datos • Procesamiento ilegal de datos
Compromiso de funciones	• Error en uso • Abuso de privilegios • Olvido de privilegios • Denegación de acciones • Brecha en disponibilidad de personal (Pérdida de acceso a los datos originales)
Amenaza informática humana	• Hacker • Cibercrimen • Espionaje industrial • Infiltrados

ANÁLISIS DE RIESGOS

El análisis de riesgos en el tratamiento de la seguridad de la información es fundamental para identificar, evaluar y mitigar las posibles amenazas y vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de los datos de una organización. Se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R1)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Pérdida, robo o fuga de Información.	5	5	Disponibilidad, confidencialidad e integridad de la informacion.	Extremo	implementacion de Firewall. Licenciamiento de Software.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R2)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Correos electronicos no seguros	3	4	confidencialidad de la informacion.	Alto	Capacitacion al personal del uso correcto del correo electronico.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R3)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Daño en los equipos tecnologicos	4	4	Disponibilidad de la informacion.	Alto	Mantenimientos preventivos. Actualizacion de software.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R4)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Perdida de conexión	3	3	Disponibilidad de la informacion.	Alto	Mejora en la infraestructura de red. Mantenimientos preventivos. Actualizacion de software.

ANALISIS DEL RIESGO					
	CLASIFICACION			EVALUACION	
RIESGO (R5)	PROBABILIDAD	IMPACTO	TIPO DE IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Ataques Ciberneticos	3	5	Disponibilidad, confidencialidad e integridad de la informacion.	Alto	Implementacion de herramientas de seguridad de la informacion.

MAPA DE CALOR:

Con el fin de visualizar de manera clara y concisa los riesgos que se tienen dentro de INDEPORTES CAUCA, se realiza el mapa de calor obteniendo información sobre las áreas afectadas y en que zona de impacto y posibilidad se encuentran establecidos, facilitando la toma de decisiones sobre las acciones a tomar referente al análisis ya realizado.

		IMPACTO				
		INSIGNIFICANTE(1)	MENOR (2)	DAÑINO (3)	CRITICO (4)	EXTREMO (5)
PROBABILIDAD	CASI SEGURO (5)	M(5)	A(10)	A(15)	E(20)	R1 E(25)
	PROBABLE (4)	M(4)	M(8)	A(12)	R3 A(16)	E(20)
	POSIBLE (3)	M(3)	M(6)	R4 A(9)	R2 A(12)	R5 A(15)
	IMPROBABLE (2)	B(2)	M(4)	M(6)	M(8)	A(10)
	RARO (1)	B(1)	B(2)	M(3)	M(4)	M(5)

IDENTIFICACIÓN DE VULNERABILIDADES:

Es un proceso clave dentro de la gestión de la seguridad de la información. Consiste en identificar y evaluar las debilidades o fallos en los sistemas, redes, aplicaciones y datos que podrían ser explotados por amenazas internas o externas para comprometer la seguridad de la información o interrumpir las operaciones comerciales.

TIPO	VULNERABILIDAD	AMENAZAS
Hardware	• Mantenimiento insuficiente.	• Incumplimiento en el mantenimiento del sistema del sistema de información.
	• Susceptibilidad a la humedad, polvo y a la suciedad.	• Polvo, corrosión y congelamiento.
	• Susceptibilidad a las variaciones de voltaje.	• Pérdida del suministro de energía.
	• Almacenamiento sin protección.	• Hurtos medios o documentos.

	• Falta de cuidado en la disposición final.	• Hurtos medios o documentos.
Software	• Ausencia o insuficiencia de pruebas de software. • Ausencia de terminación de sesión cuando se abandona la estación de trabajo. • Ausencia de documentación. • Fechas incorrectas. • Descarga y uso no controlado de software.	• Abuso de derechos. • Abuso de derechos. • Dificulta la comprensión de los activos de información y los procesos de negocio de la entidad. • Errores de sincronización de datos entre sistemas y aplicaciones. • Riesgo de infectar los sistemas con malware y software malicioso.

	• Ausencia en la protección física de la edificación, puertas y ventanas.	• Robo de activos físicos y equipos.
Red	• Conexión deficiente de los cables. • Líneas de comunicación sin protección. • Tráfico sensible sin protección. • Punto único de fallas.	• Fallas del sistema de telecomunicaciones. • Intercepción de datos. • Robo de información. • Interrupción del servicio.
Personal	• Ausencia del personal. • Procedimientos inadecuados de contratación. • Uso incorrecto de software y hardware. • Trabajo no supervisado del personal externo o de limpieza.	• Incumplimiento en la disponibilidad del personal. • Riesgo de empleados no calificados. • Vulnerabilidades de seguridad. • Acceso no autorizado a áreas sensibles.

Lugar	• Uso inadecuado de los controles de acceso al edificio. • Áreas susceptibles a inundación. • Red eléctrica inestable. • Ausencia de protección en puertas o ventanas.	• Violaciones de seguridad física. • Pérdida de datos y documentación. • Daño a equipos electrónicos. • Acceso no autorizado a información y activos.
Organización	• Ausencia de políticas sobre el uso de correo electrónico. • Ausencia de procesos para supervisión de derechos de acceso. • Ausencia de control de activos que se encuentran fuera de las instalaciones. • Ausencia de revisiones regulares por parte de la gerencia.	• Fugas de información confidencial. • Presenta amenaza interna para la seguridad de la entidad. • Pérdida o robo de activos. • Falta de detección temprana de problemas operativos, financieros, de seguridad o de cumplimiento.

IDENTIFICACIÓN DE CONTROLES EXISTENTES

La evaluación de riesgos se lleva a cabo cualitativamente mediante comparaciones. Como resultado, se analiza la probabilidad de ocurrencia del riesgo y su impacto y se crea una matriz denominada matriz de calificación, evaluación y respuesta a los 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 años

TABLA DE IMPACTO

En la cual se definen los niveles, descriptor y la descripción de cada uno de estos con el fin de tener claridad la importancia del impacto de cada uno de los riesgos analizados para este diagnostico.

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimo 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	Crítico	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Extremo	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

IDENTIFICACIÓN DE LAS CONSECUENCIAS:

Un escenario de riesgo describe un evento relacionado con Tecnologías de la Información que puede llevar a un impacto en la entidad. Para que los escenarios de riesgo sean completos y se puedan utilizar en análisis de riesgos, deben contener los siguientes componentes:

Escenario del riesgo	**Actor**	➢ Interno ➢ Externo
	Tipo de amenaza	➢ Malicioso ➢ Accidental ➢ Fracaso ➢ Natural
	Acción	➢ Divulgación ➢ Interrupción ➢ Modificación ➢ Robo ➢ Destrucción ➢ Diseño ineficaz ➢ Ejecución ineficaz ➢ Regulación ➢ Uso inadecuado
	Activo / Recurso	➢ Personas ➢ Ministerio ➢ Procesos ➢ Infraestructura ➢ Arquitectura de Componentes Institucionales