PLAN DE CONTROL DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información de la Empresa de Vivienda de Antioquia VIVA, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto organizacional, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos Misionales y el plan de desarrollo de la entidad. Es así que desde la Dirección Administrativa y Financiera se ha establecido una política clara de apoyo y compromiso frente a los temas relacionados con la Seguridad de la Información con el fin de garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad; lo cual se ve reflejado mediante la aprobación de la resolución 486 del 05 de septiembre de 2023.

2. OBJETIVO(S)

- Liderar la política de administración de riesgos de la entidad adoptando un enfoque en la gestión de riesgos mediante la adecuada identificación, análisis, valoración y tratamiento de los riesgos con el fin de prevenir su posible materialización; minimizar cualquier impacto y facilitar la toma de decisiones según el tipo de riesgo, a través de la aplicación del presente plan; y que a través de la implementación de controles adecuados se permita reducir, mitigar, transferir o eliminar los riesgos potenciales en los diferentes procesos.

- Fortalecer el comportamiento profesional y personal de los funcionarios de VIVA, generando toma de conciencia frente al pensamiento basado en riesgos incorporando en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones para prevenir eventos e incidentes de seguridad que puedan afectar el logro de los objetivos misionales de la entidad.

3. ALCANCE

La gestión de riesgos de seguridad y privacidad de la información, incluido su tratamiento será aplicado sobre todos los activos de información (Hardware, software y servicios tecnológicos) de la entidad identificados en cada uno de los procesos y que harán parte del Registro de Activos de Información; con base en las normas vigentes, la metodología definida por la organización

desde su Modelo de Gestión Organizacional (MGO) para la gestión del riesgo, así como las pautas, recomendaciones y/o requisitos previstos en la ISO 27001 para su seguimiento, monitoreo y evaluación con un enfoque de cumplimiento y mejoramiento continuo. Así mismo, el plan de tratamiento de riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles moderado, alto y extremo acorde con los lineamientos definidos por el Ministerio de TIC, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad. Ver tabla de referencia en la guía del MINTIC: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1. Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2. Niveles de Clasificación

A través de esta guía se busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP. Ayudar a que las Entidades logren vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información.

La gestión de riesgos de seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción) le permite a la Empresa de Vivienda de Antioquia VIVA, realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la Información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que se pueda aceptar o asumir desde la Alta Dirección.

4. POLÍTICA DE ADMINISTRACION Y GESTION DE RIESGOS

"Los procesos de la Empresa De Vivienda De Antioquia - VIVA, durante su accionar pueden presentar situaciones o eventos que generen desviaciones en la consecución de sus objetivos. Para ello, a través de su esquema de líneas de defensa establece y aplica herramientas de gestión de riesgos mediante la identificación, análisis, valoración y tratamiento, con el fin de reducir la probabilidad de ocurrencia y/o mitigación del impacto de la materialización de los mismos. Para lograrlo, establece actividades de prevención, sensibilización y control para el tratamiento de los riesgos que puedan afectar los objetivos y metas institucionales, aumentando la capacidad para lograr los resultados previstos, previniendo, reduciendo o eliminando los efectos indeseados".

5. RESPONSABLE(S)

El líder del proceso de Gestión de Tecnología de la Información es el responsable de la elaboración, actualización, divulgación, ejecución y seguimiento del presente plan de control de riesgos de seguridad y privacidad de la información con responsabilidad compartida entre los funcionarios, contratistas y aquellas personas o terceros que intervienen en calidad de participantes de la organización, sus áreas y procesos.

Roles: En la actualidad, la Empresa de Vivienda de Antioquia - VIVA, cuenta con una estructura organizacional de 5 personas en el equipo de Gestión de TI, adscritas a la Dirección Administrativa y Financiera; conformada por:

- ✓ Un profesional, cuyo perfil es de ingeniero de sistemas con especialización, encargado de coordinar el proceso de información y tecnología.
- ✓ Un profesional universitario, cuyo perfil es de ingeniero de sistemas o informática, encargado de la administración de la infraestructura entre otras funciones de analista y soporte de nivel 2 que estén a su alcance.
- ✓ Un auxiliar de apoyo técnico, cuyo perfil es de técnico en mantenimiento y reparación de computadores, encargado de prestar soporte de nivel 1 a los usuarios de la entidad, entre otras tareas asignadas que estén a su alcance.
- ✓ Un profesional de apoyo, con certificación en la norma ISO 27001 y cuyo perfil es de ingeniero de sistemas, encargado de todas las funciones propias del proceso de Gestión de TI que le sean asignadas.
- ✓ Un profesional de apoyo, cuyo perfil es de ingeniero de telecomunicaciones, encargado del análisis de los datos, diseño y construcción de tableros de información para facilitar la gestión de información propia de las áreas y procesos de la entidad.
- ✓ Un profesional de apoyo, cuyo perfil es de ingeniero de desarrollo de software, encargado del análisis, diseño y desarrollo de aplicaciones requeridas para resolver las necesidades particulares de VIVA y facilitar la gestión de información propia de las áreas y procesos de la entidad.

6. ESTRATEGIAS(S)

- Dar a conocer al personal de VIVA la Política de Seguridad y Privacidad de la Información aprobada mediante la resolución 486 del 05 de septiembre de 2023.

- Fortalecer el compromiso de la Empresa de Vivienda de Antioquia - VIVA, frente a la seguridad y privacidad de la información, a través de los lineamientos que deberán seguirse para proteger la información a través de la definición de procedimientos, protocolos, estándares y controles de seguridad al interior de la Empresa de Vivienda de Antioquia – VIVA.

- Dar a conocer los protocolos de seguridad como las reglas o normas diseñadas para garantizar la confidencialidad, la integridad y la disponibilidad de la información; evitando que personas no autorizadas puedan acceder a la información, manipularla o destruirla.

- Realizar un monitoreo permanente de los componentes de infraestructura tecnológica y tomar las acciones que sean necesarias para mitigar los posibles riesgos de seguridad.

- Dar a conocer al personal de VIVA la Matriz de Riesgos de Seguridad y Privacidad de la Información y garantizar su actualización.

- Realizar campañas de divulgación y sensibilización frente a posibles amenazas a la seguridad y privacidad de la información.

7. PROYECTO(S)

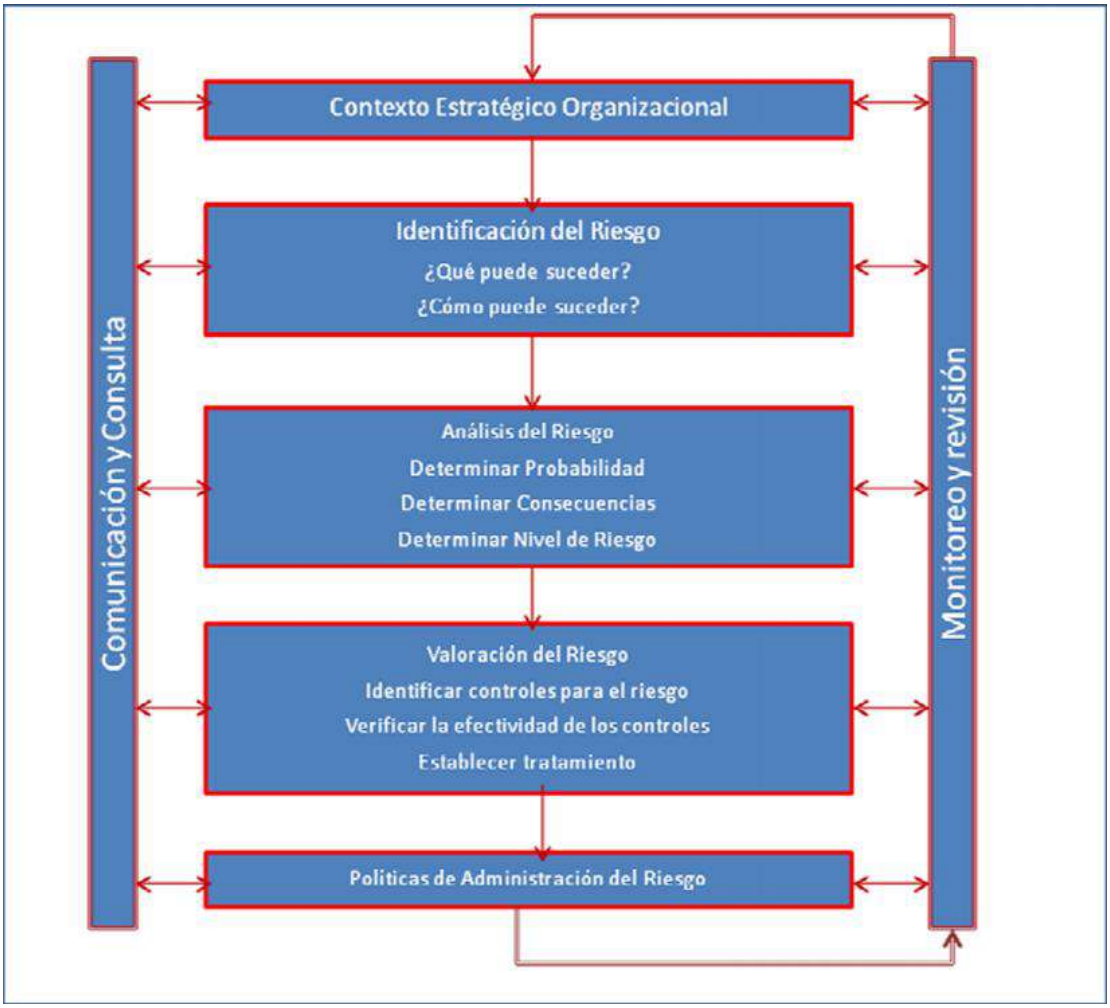
- Adquirir, desplegar y configurar nuevo licenciamiento de software antivirus.
- Adquirir e implementar nuevo dispositivo firewall de seguridad.
- Ampliar la cuota de almacenamiento de los dispositivos NAS para salvaguardar los respaldos de información.
- Asegurar la configuración IPv6 de comunicaciones para disponer la red de datos con mayor nivel de seguridad.

8. META(S)

Mejorar el nivel de protección de la información sensible de la organización, empleados y proveedores de la empresa, mediante la implementación de controles técnicos, administrativos y operativos, de acuerdo con las normas vigentes y las mejores prácticas en la materia.

9. ACCIONES DEL PLAN DE CONTROL DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con la guía del MINTIC, el proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para tomar las acciones correspondientes que permitan realizar la valoración del riesgo y posterior tratamiento:


Contexto Estratégico Organizacional
Identificación del Riesgo
¿Qué puede suceder?
¿Cómo puede suceder?
Análisis del Riesgo
Determinar Probabilidad
Determinar Consecuencias
Determinar Nivel de Riesgo
Valoración del Riesgo
Identificar controles para el riesgo
Verificar la efectividad de los controles
Establecer tratamiento
Politicas de Administración del Riesgo
Comunicación y Consulta
Monitoreo y revisión

- Proceso para la administración del riesgo en seguridad de la información

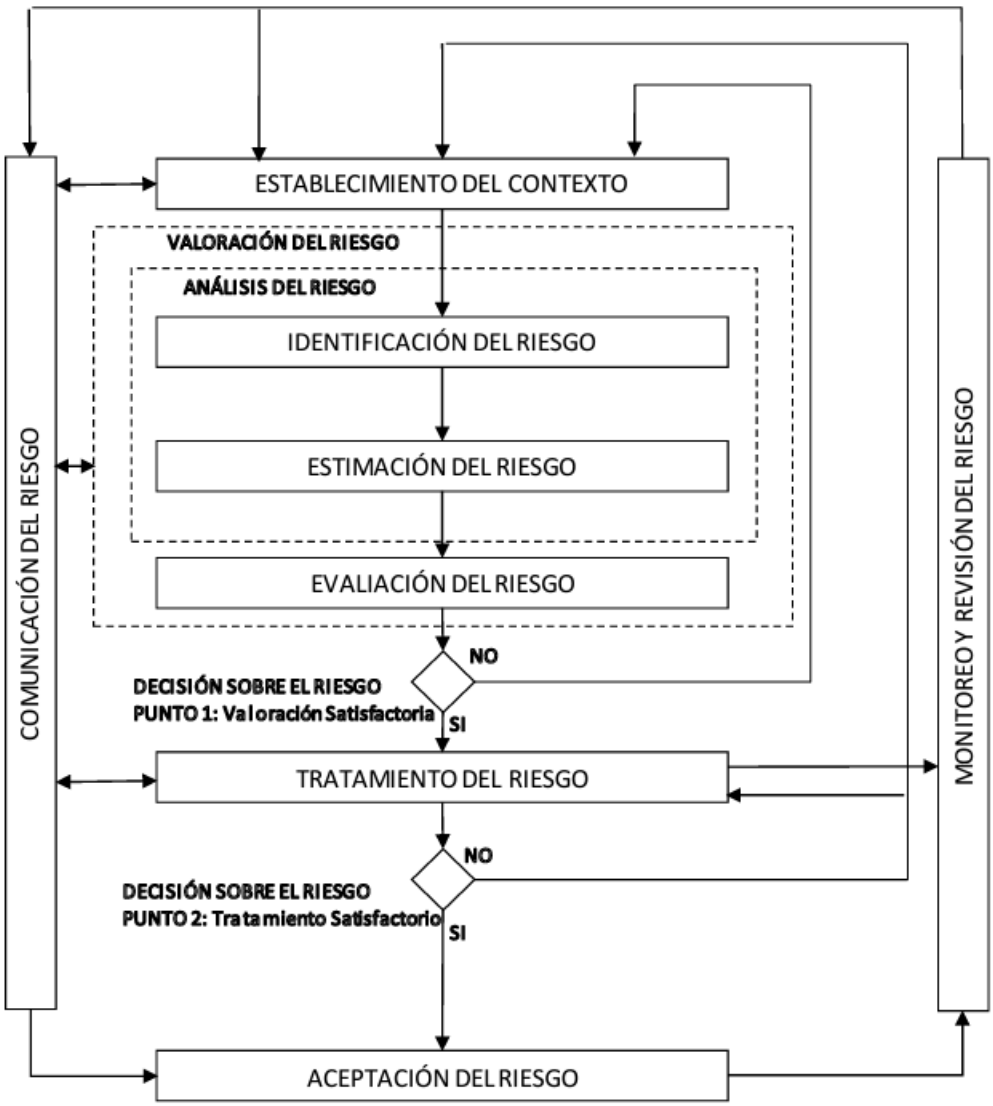


Imagen 2. Tomado de la NTC-ISO/IEC 27005

Ver referencia en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

10. PRODUCTO(S)

- Manual de Política de Seguridad y Privacidad de la Información.

- Seguimiento a implementación de Política de Seguridad y Privacidad de la Información.
- Matriz de riesgos de TI y tratamiento eficaz de los riesgos de seguridad.
- Implementación y configuración de seguridad a nivel de la Infraestructura tecnológica (Hardware y Software).
- Indicador de seguridad (Virus y amenazas) e informes de consola.
- Guía de atención de eventos e incidentes de seguridad.

11. CRONOGRAMA Y/O PLAN DE ACCIÓN PARA SU EJECUCIÓN

El plan de tratamiento de riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados y clasificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC):

Gestión	Actividades	Tareas	Responsable
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Gestión de información y tecnología
	Sensibilización	Socialización de lineamientos de la gestión de riesgos de seguridad y privacidad de la Información y Seguridad Digital	Gestión de información y tecnología
	Identificación de Riesgos de Seguridad y Privacidad de la Información, seguridad digital, disponibilidad y continuidad de la operación	Contexto, Identificación, Análisis y Evaluación de Riesgos	Gestión de información y tecnología
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	
		Seguimiento implementación de controles y planes de tratamiento de riesgos los	Gestión de información y tecnología

	Seguimiento Fase de Tratamiento	identificados (verificación de evidencias)	
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento	Gestión de información y tecnología
		Revisión y/o actualización de lineamientos de riesgos de seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	Gestión de información y tecnología

12. INDICADORES

Satisfacción:
(Suma de la cantidad de las calificaciones del nivel de satisfacción (Bueno y Muy bueno) / total de encuestas diligenciadas) *100

Obsolescencia:
(Se = Suma de los equipos tecnológicos con 60 meses o más de antigüedad /
Te = Total de equipos tecnológicos de la entidad) *100

Respaldos:
Eficacia en el Respaldo (ER) = (Respaldados ejecutados / respaldos programados) * 100

Virus:
Numero de equipos afectados por virus y/o amenazas / Número total de equipos conectados a la red *100

13. RIESGOS DEL PROCESO

A continuación, se describe los riesgos asociados al proceso, los cuales serán tratados según el presente plan de control de riesgos de seguridad y privacidad de la información:

RIESGO	DESCRIPCIÓN DEL RIESGO
Retraso en la ejecución de las actividades laborales de los funcionarios, por suspensión o falta de disponibilidad de los servicios tecnológicos del Proceso de TI	Suspensión y no disponibilidad de los servicios tecnológicos que son indispendables para la ejecución de las actividades de la empresa, tales como: Impresión, internet, almacenamiento, gestión documental (Mercurio), Xenco, dominio, control de acceso, antivirus, copias de seguridad, ERP (Sicof), correo y herramientas colaborativas (Office 365), red LAN, red inalámbrica; debido a fallas físicas, desconfiguraciones, desactualizaciones y pérdida de elementos por ausencia de controles y mantenimientos programados (Lógico, físico).
Pérdida de los activos de información de la empresa debido a la ausencia de respaldos y restauraciones	Inadecuado respaldo y restauración de los activos de información de la Empresa, debido a la falta de ejecución de actividades indispensables a nivel del Proceso y/o de un Sistema Especializado de Backups y restauraciones que permitan su aseguramiento Activo de información: Información indispensable en la que la empresa utilizó recursos para su construcción, modificación o ajuste, es decir todo proyecto, informe o producto que se tenga en formato digital y que esté almacenado en los servidores de la entidad
Posibilidad de vulnerar la seguridad de la información	Vulneración de la seguridad de la información, por falta de infraestructura, herramientas, políticas y procedimientos adecuados; debido a que no se ejecutan los controles necesarios y se desconocen las políticas de seguridad de la información.
Posibilidad de pérdida información de la página web de la entidad.	Pérdida de información de la página web de la entidad por fallas técnicas de infraestructura o manejo inadecuado de la información

Para la Gestión de los Riesgos de Seguridad de la Información se indica la metodología y/o enfoque organizacional descritos en el numeral de: “ACCIONES DEL PLAN DE CONTROL DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN”.

14. DESARROLLO DE LA TEMATICA A TRATAR

A través de la adecuada gestión de los posibles riesgos de seguridad identificados, se pretende fortalecer la confidencialidad, la integridad y disponibilidad de la información en la entidad VIVA, mediante procedimientos, lineamientos y herramientas tecnológicas que generen cumplimiento y apoyo a los demás procesos de la entidad, enfocando los esfuerzos en la generación de cultura y cuidado de la seguridad informática a través del presente plan de seguridad y privacidad de la información.

15. SIGLAS Y DEFINICIONES

Las siguientes definiciones son utilizadas en el contexto de la gestión de la seguridad de la información y aplican en todo momento durante 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 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.

Tratamiento del Riesgo: Proceso para modificar el riesgo” (Icontec Internacional, 2011).

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.

16. CONTROL DE DOCUMENTOS

ELABORÓ	APROBÓ	REVISÓ
Carlos Alberto Restrepo Buitrago Coordinador de TI	Luz Edilia López Vahos Directora Administrativa y Financiera	Gloria Estela Hernández Manrique Coordinadora de Gestión Organizacional