1. OBJETIVO

La Seguridad de la Información hace parte de la política del SGC de SER AMBIENTAL S.A ESP, por tanto, una de sus funciones fundamentales es la gestión riesgos que puedanafectar los procesos críticos del negocio y sus activos de información y que representen una amenaza para los principios de seguridad, Confidencialidad, Integridad y Disponibilidad. El propósito del análisis de riesgo es:

- Establecer los diferentes valores de los activos de información de cada proceso de la organización, los niveles de riesgos y el nivel aceptable de los mismos.
- Identificar las posibles vulnerabilidades y amenazas con su probabilidad de ocurrencia sobre los activos de cada proceso.
- Evaluar los riesgos inherentes y residuales, que afectan la pérdida de confidencialidad, integridad o disponibilidad en los activos de cada proceso.
- Establecer los niveles de riesgo que requerirán un plan de tratamiento de riesgos para los activos en estudio donde se evidencie que los riesgos residuales estén fuera de los niveles aceptables definidos.

2. ALCANCE

Los activos de información identificados en los procesos y sub procesos de SER AMBIENTAL S.A. ESP, clasificados como críticos (4) o importantes (3) de acuerdo a la calificación de criterios por confidencialidad, integridad y disponibilidad serán tenidos en cuenta para realizar la etapa de identificación y valoración de amenazas y vulnerabilidades,de igual forma se realizará la identificación de controles existentes junto con su respectivavaloración de efectividad.

3. NORMAS GENERALES

3.1. Perspectiva ISO

- ISO 9001 de 2015: Sistema de gestión de calidad.
- OHSAS 18001 de 2007: Sistema de gestión en seguridad y salud ocupacional.
- ISO 27001 de 2013: Sistema de seguridad de la información.
- ISO 14001 de 2015: Sistema de gestión ambiental.

3.2. Reglamento legal

Ver matriz legal

4. DEFINICIONES

4.1. **Acuerdo de Confidencialidad**: Es un convenio que crea obligaciones a una o aambas partes que intervienen, con respecto al uso, manejo y divulgación de la información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la misma, como parte de una relación contractual o comercial.

4.2. **Activo**: Cualquier cosa que tenga un valor de importancia relevante para la organización. Entre los activos de una organización se encuentra hardware, software, documentos electrónicos o físicos, infraestructura, servicios, personal,entre otros. El término Activo es sinónimo de Activo de Información.

4.3. **Amenaza:** Es una fuente generadora de eventos o acciones que puede produciro causar un daño representativo al activo de información, generando un factor oescenario de riesgo que originaría a la organización pérdidas por riesgo de seguridad de la información. La amenaza es un contexto de seguridad de la información que se manifiesta a través de actos deliberados, intencionados o impredecibles y provocados por las personas, la tecnología, la infraestructura, acontecimientos externos, entre otros.

4.4. **Confidencialidad:** Propiedad de salvaguardar el activo de información depersonas, procesos o entidades no autorizados.

4.5. **Controles:** Medidas de protección o salvaguardas dispuestas para reducir el nivelde riesgo. Pueden ser políticas, procedimientos, directrices, prácticas, estructurasde la organización, soluciones tecnológicas, entre otros.

4.6. **Disponibilidad:** Propiedad de garantizar que el activo de información sea accesible y utilizable en el momento que se requiera, por parte de las personas, procesos o entidades autorizada.

4.7. **Equipamiento:** El equipamiento de procesamiento de la información incluye todotipo de elemento físico soportado para el para el desarrollo de las actividades diarias del negocio. Estos elementos pueden ser entre otros: computadores de escritorio o personales, organizadores físicos, teléfonos móviles, escáneres, impresoras, tóner, fotocopiadoras, dispositivos USB, discos removibles, medios de almacenamiento y papel.

4.8. **Evento de seguridad de la información:** Es la ocurrencia identificada de un estado del activo de información (sistema, servicio, red, entre otros) que indica un incumplimiento posible de la política de seguridad de la información, una falla de controles existentes, o una situación previamente desconocida que puede ser pertinente para la seguridad.

4.9. **Incidente de seguridad de la información:** Uno o una serie de eventos de seguridad de la información indeseados o inesperados que afecta un activo deinformación y que tienen una probabilidad significativa de comprometer las operaciones del negocio y/o amenazar la seguridad de la información asociadacon el mismo.

4.10. **Integridad:** Propiedad de salvaguardar la exactitud y estado completo delactivo de información, de acuerdo a los diferentes métodos de proceso a que seexponga.

4.11. **Privacidad de Información:** es un derecho fundamental de toda persona atener el control de aquellos datos que puedan identificarla personalmente (Datos Personales).

4.12. **Procesamiento de Información:** Es la capacidad que tiene un sistema deinformación de efectuar cálculos con base a una secuencia de operaciones preestablecidas y permitiendo la transformación de datos fuentes en informaciónpara ser utilizada en la toma de decisiones.

4.13. **Propietario:** Se refiere al dueño responsable del activo de información utilizado para el desarrollo y cumplimiento de sus funciones. Está encargado de garantizar la seguridad adecuada del mismo, con base a los principios básicos deseguridad a saber: confidencialidad, integridad y disponibilidad.

4.14. **Proteger la organización:** Reducción del riesgo a través de la implementación de

acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste ocurre.

4.15. Riesgo: Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas, legales o de imagen para la organización por deficiencias, fallas o al no adecuado uso y/o manejo del activo de información, a causa de amenazas o vulnerabilidades que le altere su correcto funcionamiento uoperatividad.

4.16. Seguridad de la información: Preservación fundamental de la confidencialidad, integridad y disponibilidad del activo de información, además de otros criterios o propiedades tales como la autenticidad, no repudio, confiablidad, propiedad y/o responsabilidad, entre otros.

4.17. Sistema de Información: Es una disposición de personas, actividades o procedimientos y recursos tecnológicos integrados entre sí, para apoyar y mejorarlas operaciones diarias de la organización, con la finalidad de satisfacer las necesidades de información en general y facilitar la toma de decisiones por partede los directivos de la organización. Ejemplos aplicados: sistemas de automatización de oficina, sistemas de procesamiento de transacciones y sistemas de información de gestión.

4.18. Software malicioso: Es una variedad de software o programas de códigoshostiles e intrusivos que tienen como objeto infiltrarse en o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

4.19. Tratamiento del riesgo: Proceso de selección e implementación de controles o acciones para ajustar el nivel de riesgo del activo a los niveles aceptables para la Organización.

4.20. Vulnerabilidad: Es la debilidad o incapacidad de resistencia de un activo de información frente a una amenaza.

5. CONDICIONES

5.1. Generales

La metodología de gestión de riesgos se diseña teniendo en cuenta el contexto de la organización, tanto interno como externo dimensionando las situaciones que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados planteados por los objetivos de su sistema de gestión de la seguridad de la información.

5.1.1. Metodología de gestión de riesgos

a. Identificar el proceso y subproceso

b. Tipificar los activos relevantes del proceso

c. Valorar y clasificar el activo en función de los criterios de seguridad de lainformación

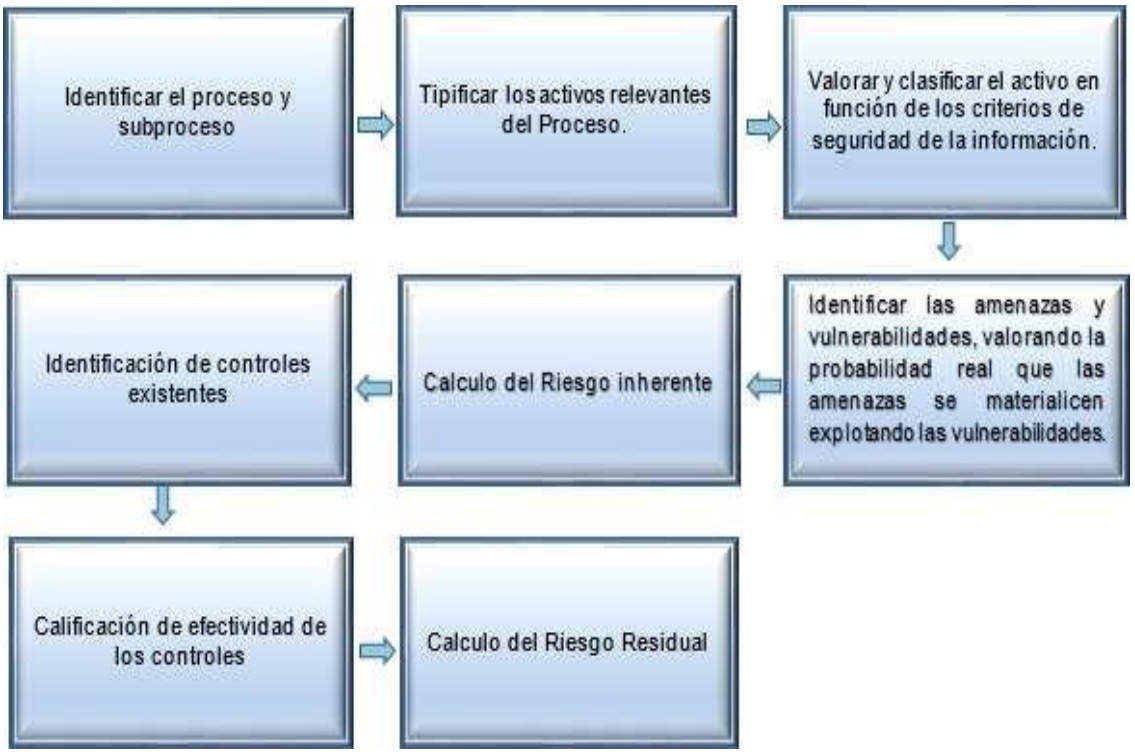
d. Identificar las amenazas y vulnerabilidades, valorando la probabilidad real que las amenazas se materialicen explotando las vulnerabilidades.

e. Cálculo del riesgo inherente

f. Identificación de controles existentes

g. Calificación de efectividad de los controles

h. Cálculo del riesgo residual



La metodología para la identificación, valoración de activos y gestión de riesgospara SER AMBIENTAL S.A. ESP, se encuentra apoyada en la matriz deriesgo, con el fin de brindar un informe detallado de los procesos; se ejecutará una matriz por cada proceso la cual deberá contemplar los siguientes campos:

5.1.2. Campos de la matriz de riesgos

PROPIEDADES DEL ACTIVO DE INFORMACIÓN	Nombre del Activo
	ID. Activo
	Proceso
	Subproceso
	Medio
	Dueño del Riesgo
CRITERIOS DE SEGURIDAD	Privacidad
	Justificación
	Confidencialidad
	Justificación
	Integridad
	Justificación
	Disponibilidad
	Justificación
VALORACIÓN DEL ACTIVO DE INFORMACIÓN	Valor del activo en decimal
	Valor del Activo
VALORACIÓN DEL RIESGOINHERENTE	Amenaza
	Valor de la Amenaza
	Probabilidad de que la amenaza se ejecute
	Promedio de las amenazas
	Valor del Impacto
	Nivel de Impacto sobre la operación
	Promedio del Nivel de Impacto
	Valor del Riesgo Inherente
VALORACIÓN DEL CONTROL	Controles
	Tipo de control
	Estado de documentación del control
	Efectividad del control
	Evaluación de cada control
	Calificación final de controles
RIESGO RESIDUAL	Riesgo residual por activo

Los anteriores campos son administrados a través de una matriz, con el objeto de realizar informes que permitan visualizar controles por proceso, por subprocesos, tipos de control y estado de los mismos.

5.1.3. Valoración de matriz de riesgos

5.1.3.1. Valoración por criterios de seguridad

- **Privacidad:** Valorando si el Activo de Información tiene o no datos personales.
- **Confidencialidad:** Valorando el impacto que tiene sobre SER AMBIENTAL S.A. ESP la divulgación no autorizada sobre el activo de información.
- **Integridad:** Valorando el impacto que puede ocasionar la perdida de la integridad del activo de información sobre las operaciones de SER AMBIENTAL S.A. ESP.
- **Disponibilidad:** Valorando el impacto que tiene sobre SER AMBIENTAL S.A. ESP, la falta de acceso oportuna al activo de información.

5.1.3.2. Tabla de valoración de los activos por Privacidad

Privacidad		
Muy Bajo	1	No tiene datos personales
Alto	4	Tiene datos Personales

5.1.3.3. Tabla de valoración de los activos por Confidencialidad

Confidencialidad		
Publica	1	Activo de información que por disposición de un proceso de Ser Ambiental S.A ESP o norma jurídica puede ser conocido y utilizado, sin que tengaincidencia alguna hacia las partes interesadas.
Uso Interno	2	Activo de información utilizado por personal o usuarios de Ser Ambiental S.A ESP, para realizar exclusivamente sus labores en los procesos relacionados y que no puede ser conocida por terceros sin la autorización del propietario del activo. En caso de ser divulgado, usado o modificado por personas o usuarios sin la debida autorización podría impactar de forma LEVEa los sistemas de información de información de Ser Ambiental S.A ESP o terceros relacionados.
Confidencial	3	Activo de información que sólo puede ser conocido y utilizado por un grupo LIMITADO de personas o usuarios autorizados, y cuya divulgación, uso o modificación de personas sin la debida autorización podría impactar de forma IMPORTANTE a los sistemas de información de Ser Ambiental S.A ESP o terceros relacionados.
Secreta	4	Activo de información con mayor nivel de sensibilidad que sólo puede ser conocido y utilizado por un grupo MUY REDUCIDO de personas o usuarios autorizados y generalmente de la alta dirección de Ser Ambiental S.A ESP o tercero relacionado. Su divulgación, uso o modificación de personas sin la debida autorizaciónpodría impactar de forma GRAVE a los sistemas de información de Ser Ambiental S.A ESP o terceros relacionados.
No Aplica	0	El Activo de información no tiene Confidencialidad sobre el proceso.

5.1.3.4. Valoración de los activos por Integridad.

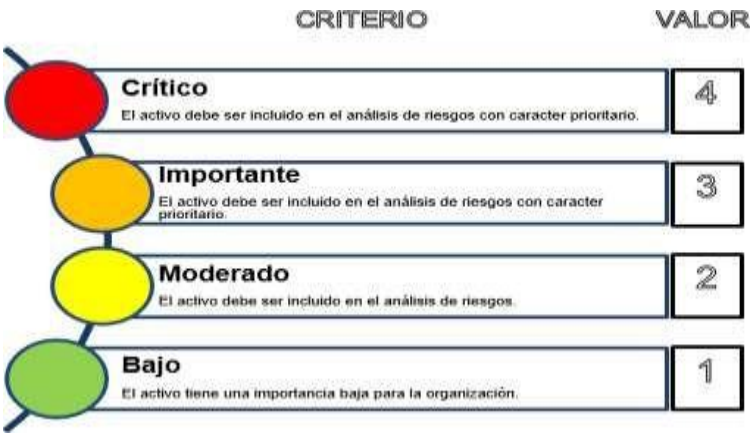
Integridad		
Muy Bajo	1	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos no tiene ningún impacto negativo en el proceso.
Bajo	2	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente de forma leve alproceso.
Medio	3	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente de forma importante al proceso.
Alto	4	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente de forma crítica al proceso.

5.1.3.5. Valoración de los activos por disponibilidad

Disponibilidad		
Muy Bajo	1	La falta del activo de información no tiene ningún impacto negativo enel proceso.
Bajo	2	Bajo La falta del activo de información impacta negativamente de forma leve al proceso.
Medio	3	La falta del activo de información impacta negativamente de forma importante al proceso.
Alto	4	La falta del activo de información impacta negativamente de forma crítica al proceso.

5.1.3.6. Valoración del activo

La valoración del activo de información se realizará de acuerdo a los valores establecidos para cada uno de los criterios de seguridad, de forma cualitativay del promedio de los mismos se obtendrá el valor del activo.



5.1.3.7. Valoración del riesgo

De acuerdo con lo establecido en la Norma ISO 27005:2009 se identifican las siguientes amenazas y vvulnerabilidades que le pueden ocurrir a un activo de información

TIPOS	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico.	Destrucción del equipo o los medios.Polvo, corrosión,
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Falta de "terminación de la sesión" cuando se abandona la estación detrabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borradoadecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos
	Distribución errada de los derechos de acceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación a los datos errados en términosde tiempo	Corrupción de datos
	Interfase de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autentificación, como la autentificación	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos

Software	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Falta de control eficaz del cambio	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Falta de copias de respaldo	Manipulación con software
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Falta de prueba del envío o la recepción de	Negación de acciones
	Líneas de comunicación sin protección	Escucha subrepticia
	Tráfico sensible sin protección	Escucha subrepticia
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Falta de identificación y autentificación de	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas autorizadas	Espionaje remoto
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos
	Falta de proceso formal para la revisión (supervisión) de los derechos deacceso	Abuso de los derechos
	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en loscontratos con los clientes y/o terceras partes	Abuso de los derechos
	Falta de procedimiento de monitoreo de los recursos de procesamientoinformación	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	Abuso de los derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos
	Falta de reportes sobre fallas incluidos en los registros de administradores yoperador	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información

	Falta de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Falta de procedimiento formal para el control de la documentación del SGC	Corrupción de datos

	Falta de procedimiento formal para la supervisión del registro del SGC	Corrupción de datos
Organización	Falta de procedimiento formal para la autorización de la informacióndisponible al público	Datos provenientes de fuentes no confiables
	Falta de asignación adecuada de responsabilidades en la seguridad de lainformación	Negación de acciones
	Falta de planes de continuidad	Falla del equipo
	Falta de políticas sobre el uso del correo	Error en el uso
	Falta de procedimientos para la introducción del software en los sistemasoperativos	Error en el uso
	Falta de registros en las bitácoras*(logs) de administrador y operario.	Error en el uso
	Falta de procedimientos para el manejo de información clasificada	Error en el uso
	Falta de responsabilidades en la seguridad de la información en ladescripción de los cargos	Error en el uso
	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Falta de procesos disciplinarios definidos en el caso de incidentes deseguridad de la información	Hurto de equipo
	Falta de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Falta de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Falta de mecanismos de monitoreo establecidos para las brechas en laseguridad	Hurto de medios o documentos
	Falta de revisiones regulares por parte de la	Uso no autorizado del equipo
	Falta de procedimientos para la presentación de informes sobre lasdebilidades en la seguridad	Uso no autorizado del equipo
	Falta de procedimientos del cumplimiento de las disposiciones con losderechos intelectuales	Uso de software falso o copiado
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos

	Falta de políticas para el uso correcto de los medios de telecomunicacionesy mensajería	Uso no autorizado del equipo

Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Falta de protección física de las puertas yventanas de la edificación	Hurto de equipo

5.1.3.8. Probabilidad de ocurrencia de las amenazas

Las amenazas deberán ser calificadas por probabilidad de ocurrencia de acuerdo con la siguiente escala

PROBABILIDAD DE OCURRENCIA	FRECUENCIA	VALOR
MUY BAJA	El evento puede ocurrir menos de 6 veces en el año	1
BAJA	El evento puede ocurrir entre 6 y 12 veces en el año	2
MEDIA	El evento puede ocurrir entre 12 y 24 veces en el año	3
ALTA	El evento puede ocurrir entre 24 y 48 veces en el año	4

5.1.3.9. Valoración del impacto operativo

La imagen institucional de SER AMBIENTAL S.A ESP engloba los productos,marcas, servicios y el resultado de la gestión de las operaciones de la organización, en consecuencia, el dueño del riesgo deberá valorar el nivel de impacto sobre la operación de acuerdo con los siguientes criterios:

IMPACTO	JUSTIFICACION	VALOR
MUY BAJA	Mínimo. La explotación de las vulnerabilidades puede ocasionar: (1) Daños menores a los activos o recursos tangibles. (2) afectación mínima de la misión, objetivos o intereses de la organización.	1
BAJA	Bajo. No afecta pérdida de ingresos o imagen de forma considerable.	2
MEDIA	Medio. La explotación de la vulnerabilidad puede ocasionar: (1) Pérdida financiera significativa, amenaza con pérdida de imagen de la Organización. (2) Costos por pérdidas de activos o recursos tangibles.	3
ALTA	Alto. La explotación de la vulnerabilidad puede ocasionar: (1) Altos costos por pérdida de activos o recursos tangibles. (2) Violencia significativa, daño o impedimento del logro de los objetivos de la organización, reputación o intereses. (3) Pérdida de vidas humanas o daños serios a la salud.	4

5.1.3.10. Cálculo del riesgo inherente

Dado que un activo posee más de una amenaza y una vulnerabilidad asociada, se tomará el valor de la probabilidad individual de ocurrencia de amenazas delictivo por el impacto, paralelamente se realizará el comparativocon el promedio de la probabilidad de ocurrencia de amenazas del activo paraevidenciar la efectividad real de los controles; lo cual permite estimar un cálculo de riesgo residual realista. El valor de riesgo inherente está definido por la siguiente formula:

RIESGO INHERENTE= PROBABILIDA x IMPACTO

5.1.2. Identificación y valoración de controles

Los controles, medidas de protección o salvaguardas dispuestas para reducir elnivel de riesgo, pueden ser políticas, lineamientos, procedimientos, directrices,prácticas, estructuras de la organización, soluciones tecnológicas, etc.

La efectividad de los controles se evalúa de acuerdo con los siguientes criterios:

TIPO	DOCUMENTACIÓN	EFECTIVIDAD
CORRECTIVO	NO DOCUMENTADO	NO ES EFECTIVO
DETECTIVO	DOCUMENTADO, PERO NO DIVULGADO	EFECTIVO OCASIONALMENTE
PREVENTIVO	DOCUMENTADO Y DIVULGADO	SIEMPRE ES EFECTIVO

Los controles tendrán una calificación máxima de efectividad del 90% bajo la premisa que ningún control es 100% efectivo. Se manejarán tres categorías decontrol:

a. Tipo: Correctivo, Detective y Preventivo
b. Documentación: No Documentado, Documentado No divulgado y Documentado Divulgado
c. Efectividad: No es efectivo, Efectivo ocasionalmente y Siempre funciona cada categoría tiene un valor máximo del 0,33 para un totaldel 100%.

5.1.3. Cálculo del riesgo inherente

Dado que un activo posee más de una amenaza y una vulnerabilidad asociada, se tomará el valor de la probabilidad individual de ocurrencia de amenazas del activo por el impacto, paralelamente se realizará el comparativocon el promedio de la probabilidad de ocurrencia de amenazas del activo paraevidenciar la efectividad real de los controles; lo cual permite estimar un cálculo de riesgo residual realista.

El valor de riesgo inherente está definido por la siguiente formula:

RIESGO RESIDUAL = Riesgo Inherente “RI” x % de Efectividad de los Controles “EC”

Después de aplicar esta fórmula el riesgo inherente puede permanecer igual o disminuir. En el caso que después de hacer esta evaluación el riesgo residual quede en un nivel de riesgo inaceptable, importante o moderado, se debe realizar un plan de tratamiento de los riesgos.

5.1.4. Niveles de aceptación del riesgo

De acuerdo con lo establecido en este documento y lo definido por el Comité de Calidad constituido por los dueños del riesgo, se definieron los siguientes valores como patrón para medición del Riesgo vs a los niveles de aceptaciónde riesgo.

Niveles de Riesgo:

VALORACIÓN	NIVEL DE ACEPTACIÓN	DESCRIPCIÓN
12 a 16	inaceptable	Requiere el establecimiento de acciones inmediatas, tomando las medidas necesarias para la mitigación del riesgo ubicado en este nivel.
8 a 11	Importante	Requiere el establecimiento de acciones urgentes, que permitan mitigar, tanto la probabilidad, como el impacto; incurriendo en costos para reducir, transferir o compartir los riesgos.
4 a 7	Moderado	Requiere del establecimiento de acciones al interior de la entidad, desarrollos tecnológicos que permitan evitar, reducir, transferir o compartir los riesgos; se requiere evaluar el costo/beneficio del plan para mitigar el riesgo.
1 a 3	Aceptable	Su gestión no es prioritaria, se establecen planes de acción sobre actividades de rutina, no implica grandes desarrollos tecnológicos.

5.1.5. Matriz de Niveles de Aceptación del Riesgo

		ZONAS DE RIESGO Y CALIFICACIÓN			
PROBABILIDAD DE OCURRENCIA	ALTA	4 y 7 Zona de riesgo moderado *Asumir el riesgo*	8 y 11 Zona de riesgo importante Reducir, *Evitar, Transferir o Compartir el riesgo*	12 y 16 Zona de riesgo intolerable Reducir, *Evitar, Transferir o Compartir el riesgo*	12 y 16 Zona de riesgo intolerable Reducir, *Evitar, Transferir o Compartir el riesgo*
	MEDIA	1 y 3 Zona de riesgo tolerable *Asumir el riesgo*	4 y 7 Zona de riesgo moderado *Asumir el riesgo*	8 y 11 Zona de riesgo importante Reducir, *Evitar, Transferir o Compartir el riesgo*	12 y 16 Zona de riesgo intolerable Reducir, *Evitar, Transferir o Compartir el riesgo*
	BAJA	1 y 3 Zona de riesgo tolerable *Asumir el riesgo*	4 y 7 Zona de riesgo moderado *Asumir el riesgo*	4 y 7 Zona de riesgo moderado *Asumir el riesgo*	8 y 11 Zona de riesgo importante Reducir, *Evitar, Transferir o Compartir el riesgo*
	MUY BAJA	1 y 3 Zona de riesgo tolerable *Asumir el riesgo*	1 y 3 Zona de riesgo tolerable *Asumir el riesgo*	1 y 3 Zona de riesgo tolerable *Asumir el riesgo*	4 y 7 Zona de riesgo moderado *Asumir el riesgo*
		LEVE	MODERADO	IMPORTANTE	CATASTRÓFICO
		IMPACTO			

5.1.6. Plan de tratamiento de riesgos a los activos de información

- El plan de tratamiento de los riesgos deberá ser definido entre el dueñodel riesgo y la Gerencia de TI de SER AMBIENTAL S.A. ESP.
- Se debe realizar un seguimiento periódico al plan de tratamiento de riesgos, con el fin de garantizar la adecuada ejecución del plan y la mitigación de los riesgos, de acuerdo a la prioridad y a los recursos asociados para su atención.
- Es importante incluir en el plan de tratamiento de riesgos, los planes de acción (recomendaciones para el tratamiento) y los posibles futuros controles que pueden mitigar los riesgos llevándolos a niveles aceptables por la organización.
- Estos controles que se apliquen a los riesgos deberán ser definidos deacuerdo a los establecidos en el Anexo A de la norma ISO 27001:2013.
- Se debe determinar quiénes son los responsables de implementar los controles definidos bajo la tutela del dueño del riesgo y establecer un tiempo límite de ejecución.
- En el plan de tratamiento de riesgos se pueden incluir planes de acciónadicionales a la gestión realizada con el dueño del riesgo impactado, como aquellos planes de acción con estrategias de seguridad que respondan a los requerimientos del negocio para el cumplimiento de requisitos legales o contractuales, definidos y establecidos por el Oficial de Seguridad de la Información y la alta dirección.

5.2. Seguridad y Salud en el trabajo

- Ajuste a su medida los elementos regulables del puesto de trabajo (sillas, pantalla y teclado), la espalda debe de quedar recta y apoyada en la silla ylos pies no deben de quedar colgando, deben de quedar apoyados en el suelo, las rodillas deben de hacer un Angulo de 90 grados. Mantenga organizado su puesto de trabajo.
- Evita encoger el hombro y/o cuello cuando hables por teléfono.
- Para desconectar un equipo tire siempre de la clavija, nunca del cable.
- Mantenga libre de obstáculos las salidas y zonas de paso.
- Realice pausas activas

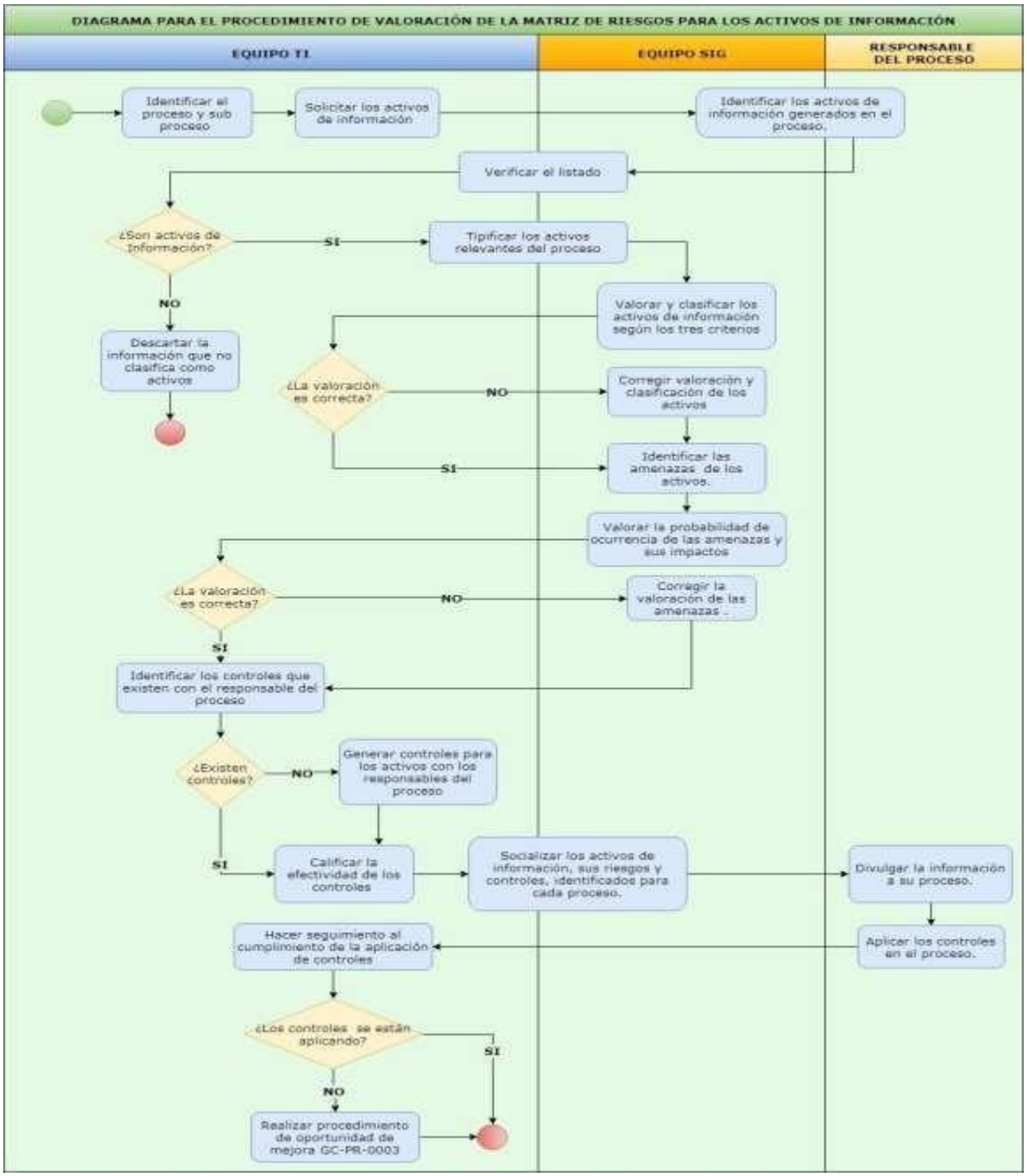
5.3. Ambiental

- Evite el desperdicio de papel corroborando que la información este correctaantes de su impresión.
- Cuando no se esté utilizando el computador ciérrelo o págalo.
- Apague las luminarias después de acabar su labor.
- Deposite los residuos dependiendo de su clasificación y características.
- Evite el desperdicio de agua, cierre las griferías después de utilizarlas.

5.4. Seguridad de la Información

Estos documentos están regidos bajo los parámetros de la ISO 27001.

6. DESCRIPCIÓN



7. DOCUMENTOS RELACIONADOS

Ítem	Proceso	Documento
1	Tecnología de la información	Diagrama Valoración y Gestión del Riesgo
2.	Tecnología de la información	Matriz SGC Activos de información

8. CONTROL DE CAMBIOS

Versión N°	Fecha	Elaborado/Modificado por	Descripción del cambio
01	27/07/2021	Coordinador de TI	Versión Original

9. RESPONSABLES

Elaboró: Coordinador de TI	**Revisó:** Director de TI
Aprobó: Gerente de TI	

COPIA CONTROLADA:	**SI:**	**NO**