CONTROL DE CAMBIOS

Versión	Descripción del cambio	Autor	Fecha
1.0	Versión Inicial	Rosa Gutiérrez	21/11/2022

Aprobación Documental

Elaboró: Rosa Gutiérrez Gutiérrez **Rol**: Gerente Experiencia del Cliente – Colombia **Fecha**: diciembre-2022	**Aprobó**: Rodrigo Baldecchi Quezada **Rol**: Director Corporativo Experiencia Cliente **Fecha:** diciembre-2022

TABLA DE CONTENDO

CONTENIDO DE TABLAS

CONTENIDO DE FIGURAS

1. OBJETIVO

Establecer la metodología para gestionar los riesgos de las diferentes líneas de servicio, áreas y proyectos de la corporación de forma centralizada y homogénea garantizando que se identifiquen, registren y gestionen los riesgos de forma correcta para evitar la materialización de estos.

2. ALCANCE

La metodología aplica en todos los países en donde la organización tiene presencia y para las unidades de negocio, áreas y/o procesos que hagan parte del alcance de alguna de las siguientes certificaciones: ISO 27001:2013, ISO 20000-1, ISO 90001:2015, ISO 14001:2015, 45001:2018 y gestión de riesgo integral de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT).

3. NORMATIVIDAD APLICABLE

ISO 31001:2018, MAGERIT, ISO 27005:2020

4. TERMINOLOGÍA

TERMINO	DEFINICIÓN
Riesgo:	Efecto de la incertidumbre sobre los objetivos. La probabilidad que una amenaza se materialice causando daño a uno o más activos de información, al medio ambiente y/o la salud de los trabajadores, efecto o consecuencia no deseada en datos personales o no previsto en los tratamientos de datos personales generando daños o perjuicios sobre los derechos o libertades de un individuo.
Fuentes de riesgos (causas):	Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
Consecuencia:	Es el resultado de un evento que afecta a un objetivo de forma negativa o positiva.
Activo de información:	Recurso que almacena información o digital de la organización.
Control:	Medida que mantiene o modifica el nivel de un riesgo.
Medio Ambiente:	Es el espacio en el que se desarrolla la vida de los diferentes organismos.
Probabilidad:	Posibilidad de que ocurra un evento
Impacto:	Resultado en caso que se llegue a materializar el riesgo.
Riesgo Residual:	Riesgo remanente después aplicar los controles para reducir el riesgo derivado de cada una de las fuentes de riesgo.
Riesgo Intrínseco o inherente:	Es el nivel de riesgo evaluado sin la implantación de medidas y garantas para reducir el riesgo.
Vulnerabilidad:	Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Gestión de Riesgos:	Permite adecuar las medidas a los riesgos que se definieron.
SGSI:	Sistema de Gestión de Seguridad de la Información.
SGA:	Sistema Gestión Ambiental.
SST:	Sistema seguridad y salud en el trabajo.
SAGRILAFT:	Sistema de autocontrol y gestión del riesgo de LA/FT/FPADM, conforme lo

	establece el capítulo X de la Circular básica jurídica de la Superintendencia de Sociedades.
Oportunidad o riesgo positivo:	Es el evento o conjunto de eventos que pueden generar que la organización, lance nuevos productos, abra nuevos mercados, capte más clientes, utilice nuevas tecnologías, entre otros.
Disponibilidad:	Propiedad de un activo de ser accesible y usable por una entidad autorizada.
Interrupción:	Suspensión temporal de la ejecución de un proceso.
Tratamiento de Riesgo:	Es definir e implementar controles (medidas) que disminuyan el nivel del riesgo o la eliminación de este.
Dato personal:	
PTEE:	Programa de Transparencia y Ética Empresarial
Categoría especial de datos personales:	Son datos personales relacionados con: Origen étnico, Origen racial, Opiniones políticas, Convicciones religiosas, Convicciones filosóficas, Afiliación sindical, Datos relativos a la salud, Datos relativos a la vida sexual, Datos relativos a las orientaciones sexuales y datos relativos a condenas e infracciones penales.
Reversible:	Puede volver a su situación previa.
Metodología:	Es una serie de técnicas, métodos y estrategias, que implementadas sistemáticamente aseguran un resultado válido y confiable.
Sistema de Gestión:	Conjunto de elementos interrelacionados o que interactúan para establecer políticas, objetivos y procesos.
Valor de menor cuantía:	cuando el monto no supere los 40 SMLMV
SMLMV:	Salarios mínimos legales mensuales Vigentes.
Mapa de calor:	Es una herramienta de visualización para mostrar los niveles de riesgos que enfrenta una organización y ayuda a priorizar los riesgos.
Calidad:	Capacidad de la organización para cumplir a cabalidad los requisitos legales, normativos y contractuales
Continuidad:	Es la capacidad de la organización para mantener sus servicios y negocio a lo largo del tiempo.
Disponibilidad:	Es la capacidad de la organización para mantener accesibles sus servicios de acuerdo con lo acordado.
Riesgo emergente:	Un nuevo peligro identificado, que pueda originar un riesgo.
Activos de información:	Son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que la organización funcione de forma adecuada y logre los objetivos propuestos por la alta dirección.
DOFA:	DOFA: La sigla DOFA es. Debilidades, Oportunidades, Fortalezas y Amenazas. Es un tipo de análisis que se utilizar para determinar el contexto de una organización, situación actual.

Tabla 1 - Terminología

5. TIPOS DE RIESGOS

La organización definió los tipos de riesgos que se describen en la tabla 2, la clasificación se deberá realizar utilizando los criterios descritos y la nomenclatura se usará para el registro en la herramienta de gestión, lo anterior para facilitar las consultas por tipo de riesgo.

TIPO DE RIESGO	NOMENCLATURA	DESCRIPCIÓN
Riesgo estratégico:	EST	Son los que pueden generar una disrupción en el corazón de la estrategia de la organización incluso impidiendo el logro de esta. Son aquellos que se derivan de la toma de decisiones de negocio fallidos.
Riesgo natural:	NAT	Riesgo que no es provocado por la acción humana, por ejemplo: climático (tornados, tormentas), biológico (epidemia causada por virus) y/o geológico (terremotos, volcanes), es decir, son riesgos que no se pueden controlar.
Riesgo operacional:	OPE	Son riesgos relacionados a los procesos, actividades u operaciones que se realiza.
Riesgo Operativo:	OPR	Riesgo que puede generar pérdidas económicas derivadas de un uso inadecuado de los sistemas de información y las tecnologías inherentes en los procesos de la organización.
Riesgo tecnológico:	TEC	Está relacionado con cualquier perdida financiera, interrupción de las operaciones o daño a la reputación de una organización originada por un fallo o problema de sus sistemas de tecnología de la información.
Riesgo financiero:	FIN	Es el que se produce por pérdida financieras en una empresa.
Riesgo legal:	LEG	Es el que afronta una empresa por el marco normativo al que está sujeta, es la posibilidad de sufrir pérdidas económicas por el incumplimiento o modificación de las leyes.
Riesgo reputacional:	REP	Posibilidad de pérdida o disminución en la reputación de una organización de forma que afecte de forma negativa a la percepción que el entorno social tiene sobre la misma.
Riesgo de contagio:	CON	Posibilidad de pérdida que puede sufrir la Empresa de forma directa o indirecta por el accionar de una contraparte.
Riesgo de proveedor:	PRO	Son los riesgos que se pueden originar por los servicios prestados por un proveedor.
Riesgo ambiental:	AMB	Es la posibilidad que se materialice un evento de orden catastrófico en el medio ambiente debido a un fenómeno natural y/o acción humana causando daños en las personas u otros seres vivos.
Riesgo laboral:	LAB	Es todo lo que expone a un trabajador ante una situación de peligro en el trabajo que puede causarle una lesión, una enfermedad e incluso la muerte.
Riesgo físico:	FIS	son los más habituales y son originados por diversas causas, como, por ejemplo: ruidos excesivos, iluminación, temperatura, humedad, radiaciones, manipulación de maquinaria pesada y/o trabajar en alturas.

TIPO DE RIESGO	NOMENCLATURA	DESCRIPCIÓN
Riesgo ergonómico:	ERG	Estos riesgos son los originados por posturas incorrectas en los puestos de trabajo, levantamiento de peso excesivo o movimientos repetitivos que pueden provocar daños físicos, que con el tiempo pueden convertirse en crónicos.
Riesgo psicosocial:	PSI	Son los asociados con el estrés, la monotonía y/o la fatiga.
Riesgo mecánico:	MEC	Son los asociados con trabajos en altura, uso incorrecto de herramientas o equipos defectuosos.
Riesgo de datos personales:	PER	Son los Riesgos asociados a datos personales

Tabla 2 - Tipos de Riesgos

6. NIVEL DE PROBABILIDAD

La organización estableció 5 niveles de probabilidad y para cada uno se definieron criterios que faciliten la selección del nivel más adecuado para cada riesgo.

MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
Si algo sucede cada 2 años su probabilidad es **MUY BAJA**	Si algo sucede 01 vez en un año su probabilidad es **BAJA**	Si algo sucede 02 veces en el semestre su probabilidad es **MEDIA**	Si algo sucede 01 vez a la semana su probabilidad es **ALTA**	Si algo sucede 01 vez al día su probabilidad es **MUY ALTA**
Si algo sucede cada 3 años su probabilidad es **MUY BAJA**	Si algo sucede más de 2 veces en 2 años su probabilidad es **BAJA**	Si algo sucede 03 o más veces en el semestre su probabilidad es **MEDIA**	Si algo sucede 02 o más veces al mes su probabilidad es **ALTA**	Si algo sucede 02 veces al día su probabilidad es **MUY ALTA**
Si algo sucede cada 5 años o superior su probabilidad es **MUY BAJA**	-	Si algo sucede 01 vez en el semestre su probabilidad es **MEDIA**	Si algo sucede 01 vez al mes su probabilidad es **ALTA**	Si algo sucede 02 o más veces a la semana su probabilidad es **MUY ALTA**

Tabla 3 - Niveles de Probabilidad

7. NIVEL DE IMPACTO

Para el impacto también se definieron 5 niveles y los criterios para cada nivel se dividieron por ambiro de aplicación. En la tabla 4 se muestran los criterios para: Calidad, Medio Ambiente, Seguridad y Salud en el Trabajo y Seguridad de la Información.

	CALIDAD	MEDIO AMBIENTE	SEGURIDAD Y SALUD	SEGURIDAD DE LA INFORMACIÓN
MUY ALTO	Incumplimiento transversal de acuerdos contractuales, requisitos legales o normativos (a más de un cliente).	Muertes múltiples de colaboradores o especies naturales, zona inhabitable, daño irreparable al ecosistema.	Accidentes mortales (Pérdida de vida de colaboradores).	Incidente prolongado que afecta el acceso a información crítica o sensible con consecuencias económicas o administrativas graves para la organización.
ALTO	Incumplimiento individual de acuerdos contractuales, requisitos legales o normativos.	Afectación del medio ambiente y/o salud de los colaboradores reversible.	Incapacidad total o permanente Daño a la salud permanente de los colaboradores.	Interrupción del acceso a la información con consecuencias económicas o administrativas importantes.
MEDIO	Incumplimientos contemplados dentro del contrato asociados a penalidades.	Aumento de consumo de recursos no renovables como el agua y la energía.	Incapacidad temporal (mayor a 16 días y menor a 6 meses). Daño a la salud reversible.	Incidente de gravedad moderada que afecta la información con bajas consecuencias económicas o administrativas.
BAJO	Debilidad en los procesos y/o requisitos de la norma o contratos	incumplimiento o debilidad de los requisitos de la norma por clasificación incorrecta de residuos ordinarios.	Incapacidades de 1 a 15 días.	Situación de baja gravedad con interrupción controlada en la operación en la cual se afectan datos poco significativos, con mínimas consecuencias económicas o administrativas.
MUY BAJO	–	No hay contaminación y/o afectación a personas y/o al medio ambiente.	Evento sin incapacidad, lesiones superficiales.	Evento de mínima gravedad en la operación en la que no se ve afectada la información ni tampoco existen consecuencias económicas o administrativas

Tabla 4 - Parte I – Criterios de impacto

En la tabla 5 se muestran los criterios para: Disponibilidad, Datos personales, continuidad, Ética y Compliance.

IMPACTO	DISPONIBILIDAD	DATOS PERSONALES	CONTINUIDAD	ETICA Y COMPLIANCE
MUY ALTO	Servicios completamente inaccesibles e inusables incumpliendo los niveles de disponibilidad planificados.	Daño o perjuicio material y/o moral para las personas afectadas, imposible de reparar o que las puede privar totalmente de sus derechos o libertades.	Interrupción prolongada superior a los niveles definidos en la operación en la que se ven afectados procesos críticos con consecuencias económicas o administrativas relevantes para la organización.	Extinción de dominio (declaración de titularidad de los bienes a favor del estado) – Colombia Ser incluido en listas restrictivas y el reporte de empresas sancionadas por lavado de activos, corrupción y/o soborno trasnacional.
ALTO	Servicios completamente inaccesibles e inusables dentro de los niveles de disponibilidad planificados.	Daño o perjuicio material y/o moral para las personas afectadas, difícil de reparar o que las puede privar totalmente de sus derechos o libertades.	Interrupción de corto de tiempo en la operación de los procesos críticos con consecuencias económicas o administrativas importantes.	Que la organización sea vinculada a investigaciones por LA/FTFAMDM (lavado de activos, financiación del terrorismo y financiación de armas de destrucción masiva, corrupción y/o soborno trasnacional.
MEDIO	Servicio intermitente o degradado perceptible para el cliente.	Daño o perjuicio material o moral para las personas afectadas, difícil de reparar o que las puede privar de manera parcial de sus derechos o libertades.	Interrupción leve en la operación de los procesos críticos o en sus componentes con bajas consecuencias económicas o administrativas	Multas superiores a la mínima cuantía.

IMPACTO	DISPONIBILIDAD	DATOS PERSONALES	CONTINUIDAD	ETICA Y COMPLIANCE
BAJO	Servicio intermitente o degradado sin afectación al cliente (imperceptible)	No genera daño o perjuicio material y/o moral para las personas afectadas, ni se las priva de sus derechos o libertades.	Situación con interrupción controlada en la operación de los procesos críticos o en sus componentes con mínimas consecuencias económicas o administrativas.	Multas de mínima cuantía.
MUY BAJO	Falla o degradación de un componente que podría afectar la disponibilidad del servicio.	No genera daño o perjuicio material o moral para las personas afectadas, ni se les priva de sus derechos o libertades.	Evento en la operación en la que no se ven afectados sus procesos críticos y sin consecuencias económicas o administrativas.	–

Tabla 5 - Parte II – Criterios de impacto

8. MATRIZ DE PROBABILIDAD E IMPACTO (MAPA DE CALOR)

De la combinación de la probabilidad e impacto se origina el mapa de calor y a su vez esto determinará el nivel del riesgo. El nivel del riesgo se calcula de la siguiente manera:

NIVEL DE RIESGO = (VALOR IMPACTO) * (VALOR PROBABILIDAD)

			PROBABILIDAD				
			Muy Baja	Baja	Media	Alta	Muy Alta
			1	**2**	**3**	**4**	**5**
IMPACTO	**10**	Muy Alto	10	20	30	40	50
	8	Alto	8	16	24	32	40
	6	Medio	6	12	18	24	30
	4	Bajo	4	8	12	16	20
	2	Muy bajo	2	4	6	8	10

Tabla 6 - Mapa de calor

9. DESCRIPCIÓN NIVELES DE RIESGO

La organización definió 5 niveles de riesgo y el intervalo de cada nivel es el que muestra la tabla 7

NILVEL	PUNTUACIÓN	SISTEMA	DESCRIPCIÓN
NIVEL 1 MUY BAJO	2 - 4	Calidad	-
		Medio Ambiente	* No hay contaminación y/o afectación a personas y/o al medio ambiente.
		Seguridad y Salud en el trabajo	* Evento sin incapacidad, lesiones superficiales.
		Seguridad de la información	* Evento de mínima gravedad en la operación en la que no se ve afectada la información ni tampoco existen consecuencias económicas o administrativas
		Disponibilidad	* Falla o degradación de un componente que podría afectar la disponibilidad del servicio.
		Datos Personales	* No genera daño o perjuicio material o moral para las personas afectadas, ni se les priva de sus derechos o libertades.
		Continuidad	* Evento en la operación en la que no se ven afectados sus procesos críticos y sin consecuencias económicas o administrativas.
		Ética y Compliance	-
NIVEL 2 BAJO	6 - 8	Calidad	* Debilidad en los procesos y/o requisitos de la norma o contratos
		Medio Ambiente	* Incumplimiento o debilidad de los requisitos de la norma por clasificación incorrecta de residuos ordinarios.
		Seguridad y Salud en el trabajo	* Incapacidades de 1 a 15 días.

NILVEL	PUNTUACIÓN	SISTEMA	DESCRIPCIÓN
		Seguridad de la información	* Situación de baja gravedad con interrupción controlada en la operación en la cual se afectan datos poco significativos, con mínimas consecuencias económicas o administrativas.
		Disponibilidad	* Servicio intermitente o degradado sin afectación al cliente (imperceptible).
		Datos Personales	* No genera daño o perjuicio material y/o moral para las personas afectadas, ni se las priva de sus derechos o libertades.
		Continuidad	* Situación con interrupción controlada en la operación de los procesos críticos o en sus componentes con mínimas consecuencias económicas o administrativas
		Ética y Compliance	* Multas de mínima cuantía.
NIVEL 3 MEDIO	10 - 18	Calidad	* Incumplimientos contemplados dentro del contrato asociados a penalidades.
		Medio Ambiente	*Aumento de consumo de recursos no renovables como el agua y la energía.
		Seguridad y Salud en el trabajo	* Incapacidad temporal (mayor a 16 días y menor a 6 meses). Daño a la salud reversible.
		Seguridad de la información	* Incidente de gravedad moderada que afecta la información con bajas consecuencias económicas o administrativas.
		Disponibilidad	* Servicio intermitente o degradado perceptible para el cliente.
		Datos Personales	* Daño o perjuicio material o moral para las personas afectadas, difícil de reparar o que las puede privar de manera parcial de sus derechos o libertades.
		Continuidad	* Interrupción leve en la operación de los procesos críticos o en sus componentes con bajas consecuencias económicas o administrativas.
		Ética y Compliance	* Multas superiores a la mínima cuantía.
NIVEL 4 ALTO	20 - 32	Calidad	* Incumplimiento individual de acuerdos contractuales, requisitos legales o normativos.
		Medio Ambiente	* Afectación del medio ambiente y/o salud de los colaboradores reversible.

NILVEL	PUNTUACIÓN	SISTEMA	DESCRIPCIÓN
		Seguridad y Salud en el trabajo	* Incapacidad total o permanente * Daño a la salud permanente de los colaboradores.
		Seguridad de la información	* Interrupción del acceso a la información con consecuencias económicas o administrativas importantes.
		Disponibilidad	* Servicios completamente inaccesibles e inusables dentro de los niveles de disponibilidad planificados.
		Datos Personales	* Daño o perjuicio material y/o moral para las personas afectadas, difícil de reparar o que las puede privar totalmente de sus derechos o libertades.
		Continuidad	* Interrupción de corto de tiempo en la operación de los procesos críticos con consecuencias económicas o administrativas importantes.
		Ética y Compliance	* Que la organización sea vinculada a investigaciones por LA/FTFAMDM (lavado de activos, financiación del terrorismo y financiación de armas de destrucción masiva, corrupción y/o soborno trasnacional
NIVEL 5	40 - 50	Calidad	* Incumplimiento transversal de acuerdos contractuales, requisitos legales o normativos (a más de un cliente).
		Medio Ambiente	* Muertes múltiples de colaboradores o especies naturales, zona inhabitable, daño irreparable al ecosistema.
		Seguridad y Salud en el trabajo	* Accidentes mortales (Pérdida de vida de colaboradores).
		Seguridad de la información	* Incidente prolongado que afecta el acceso a información crítica o sensible con consecuencias económicas o administrativas graves para la organización.
		Disponibilidad	* Servicios completamente inaccesibles e inusables incumpliendo los niveles de disponibilidad planificados.
		Datos Personales	* Daño o perjuicio material y/o moral para las personas afectadas, imposible de reparar o que las puede privar totalmente de sus derechos o libertades.
		Continuidad	* Interrupción prolongada superior a los niveles definidos en la operación en la que se ven afectados procesos críticos con consecuencias económicas o administrativas relevantes para la organización.
		Ética y Compliance	* Extinción de dominio (declaración de titularidad de los bienes a favor del estado) – Colombia. * Ser incluido en listas restrictivas y el reporte de empresas sancionadas por lavado de activos, corrupción y/o soborno

NILVEL	PUNTUACIÓN	SISTEMA	DESCRIPCIÓN
			trasnacional.

Tabla 7 - Niveles de Riesgos

10. RESPONSABLE DEL RIESGO

Propietario del riesgo, es la persona que acepta el tratamiento del riesgo y el nivel residual de este. Para los riesgos que aplique un plan de tratamiento de riesgo es quién define y/o revisa las actividades que se ejecutarán con el fin de disminuir el nivel de riesgo.

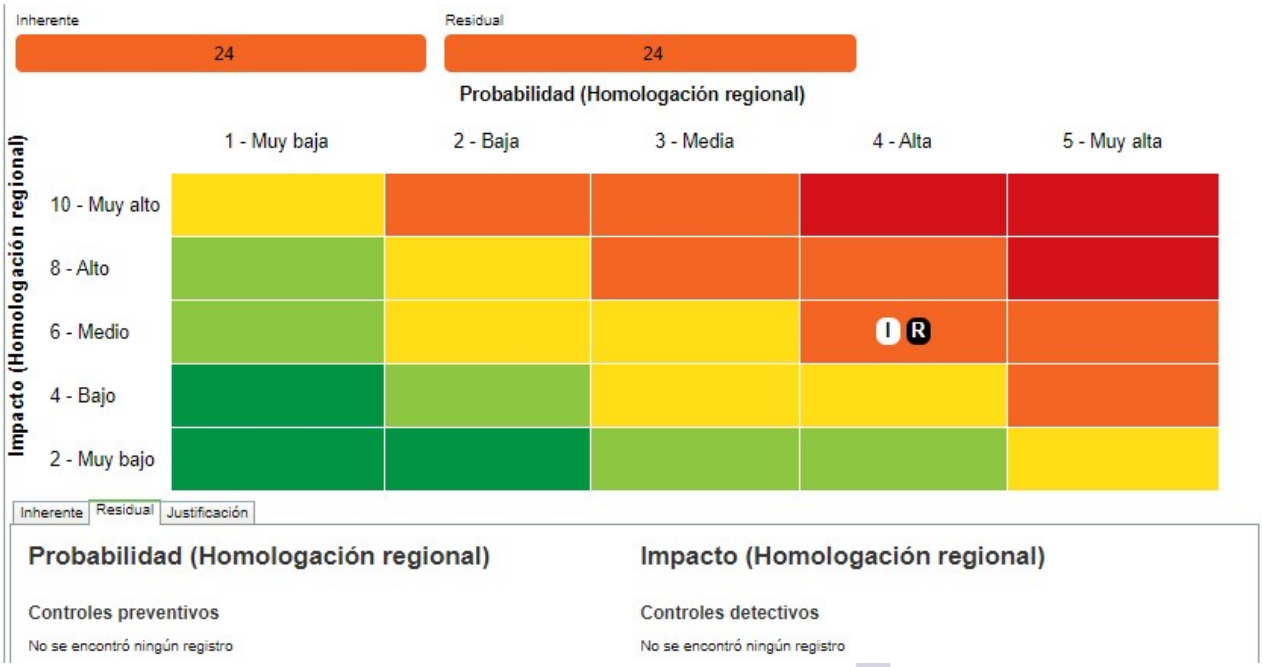
11. CONTROLES

Los controles son medidas que reducen el nivel del riesgo, dependiendo del tipo de control reducen la probabilidad y/o el impacto. Para esta metodología se contemplaron 2 tipos de controles:

Controles preventivos: Evitan que un evento suceda. Por ejemplo: solicitar login y contraseña en un sistema de información es un control preventivo.

Controles correctivos: Estos eventos no prevén que un evento suceda, este tipo de controles permiten enfrentar la situación una vez se ha presentado. Por ejemplo: ante un desastre natural, se puede contar con pólizas y mecanismos de respaldo de información. En la herramienta estos controles se llaman "Detectivos".

De acuerdo con el mapa de calor y la parametrización, en la herramienta en el **X** se evaluarán los controles asociados a la probabilidad y en el eje **Y** los que reducen el impacto. En la figura 1 - Mapa de calor herramienta se evidencia que se tienen en cuenta los 2 tipos de controles mencionados para calcular el riesgo residual. Como aún no se han asociado controles se puede observar que el nivel intrínseco es igual al residual.



Figuras 1 - Mapa de calor herramienta

10.1 ANÁLISIS Y EVALUACIÓN DE CONTROLES

Cuando se habla de evaluación de controles, se refieren a la eficacia que tienen frente al riesgo que se está tratando, el control ideal es el que tiene 100% de eficacia. Para realizar esta actividad se optó por el método que utiliza MAGERIT para evaluar el porcentaje de eficacia de cada uno de los controles.

% DE EFICACIA	NIVEL	SIGNIFICADO
0%	L0	Control inexistente.
20%	L1	No existe un proceso estándar, solo planteamiento que son utilizados de acuerdo con la situación que se presente.
50%	L2	Existe un proceso documentado que se utiliza para realizar tareas repetitivas y es medible.
70%	L3	Existe un proceso documentado medible y es monitoreado.
90%	L4	Los procesos están en un nivel de "mejor práctica" sobre una base de mejora continua y están automatizados.

Tabla 8 - Niveles de madurez y eficacia de controles

FÓRMULA QUE REDUCE LA PROBABILIDAD:

Probabilidad residual = Probabilidad – (Probabilidad * eficacia del control)

En las siguientes tablas se muestra como se reduce la probabilidad en cada uno de los niveles de madurez definidos.

NIVEL INICIAL	PROBABILIDAD INICIAL	% EFECTIVIDAD DE CONTROL	PROBABILIDAD RESIDUAL	NIVEL RESIDUAL
MUY ALTA	5	0%	5	MUY ALTA
ALTA	4	0%	4	ALTA
MEDIA	3	0%	3	MEDIA
BAJA	2	0%	2	BAJA
MUY BAJA	1	0%	1	MUY BAJA

Tabla 9 -Probabilidad residual con el 0% de eficacia de los controles

NIVEL INICIAL	PROBABILIDAD INICIAL	% EFECTIVIDAD DE CONTROL	PROBABILIDAD RESIDUAL	NIVEL RESIDUAL
MUY ALTA	5	20%	4	ALTA
ALTA	4	20%	4	MEDIA
MEDIA	3	20%	3	BAJA
BAJA	2	20%	2	MUY BAJA
MUY BAJA	1	20%	1	MUY BAJA

Tabla 10 - Probabilidad residual con el 20% de eficacia de los controles

NIVEL INICIAL	PROBABILIDAD INICIAL	% EFECTIVIDAD DE CONTROL	PROBABILIDAD RESIDUAL	NIVEL RESIDUAL
MUY ALTA	5	50%	3	BAJA
ALTA	4	50%	2	MUY BAJA
MEDIA	3	50%	2	MUY BAJA
BAJA	2	50%	1	MUY BAJA
MUY BAJA	1	50%	1	MUY BAJA

Tabla 11 Probabilidad residual con el 50% de eficacia de los controles

NIVEL INICIAL	PROBABILIDAD INICIAL	% EFECTIVIDAD DE CONTROL	PROBABILIDAD RESIDUAL	NIVEL RESIDUAL
MUY ALTA	5	70%	2	MUY BAJA
ALTA	4	70%	2	MUY BAJA
MEDIA	3	70%	1	MUY BAJA
BAJA	2	70%	1	MUY BAJA
MUY BAJA	1	70%	1	MUY BAJA

Tabla 12 - Probabilidad residual con el 70% de eficacia de los controles

NIVEL INICIAL	PROBABILIDAD INICIAL	% EFECTIVIDAD DE CONTROL	PROBABILIDAD RESIDUAL	NIVEL RESIDUAL
MUY ALTA	5	90%	1	MUY BAJA
ALTA	4	90%	1	MUY BAJA
MEDIA	3	90%	1	MUY BAJA
BAJA	2	90%	1	MUY BAJA
MUY BAJA	1	90%	1	MUY BAJA

Tabla 13 - Probabilidad residual con el 90% de eficacia de los controles

FÓRMULA QUE REDUCE EL IMPACTO:

Impacto residual = Impacto – (Impacto * eficacia del control)

En las siguientes tablas se muestra cómo se reduce impacto en cada uno de los niveles de madurez definidos.

NIVEL INICIAL	IMPACTO INICIAL	% EFECTIVIDAD DE CONTROL	IMPACTO RESIDUAL	NIVEL RESIDUAL
MUY ALTO	10	0%	10	MUY ALTO
ALTO	8	0%	8	ALTO
MEDIO	6	0%	6	MEDIO
BAJO	4	0%	4	BAJO
MUY BAJO	2	0%	2	MUY BAJO

Tabla 14 - Impacto residual con el 0% de eficacia de los controles

NIVEL INICIAL	IMPACTO	% EFECTIVIDAD DE CONTROL	IMPACTO RESIDUAL	NIVEL RESIDUAL
MUY ALTO	10	20%	8	ALTO
ALTO	8	20%	7	ALTO
MEDIO	6	20%	5	MEDIO
BAJO	4	20%	4	BAJO
MUY BAJO	2	20%	2	MUY BAJO

Tabla 15 - Impacto residual con el 20% de eficacia de los controles

NIVEL INICIAL	IMPACTO	% EFECTIVIDAD DE CONTROL	IMPACTO RESIDUAL	NIVEL RESIDUAL
MUY ALTO	10	50%	5	MEDIO

ALTO	8	50%	4	MEDIO
MEDIO	6	50%	3	BAJO
BAJO	4	50%	2	MUY BAJO
MUY BAJO	2	50%	1	MUY BAJO

Tabla 16 - Impacto residual con el 50% de eficacia de los controles

NIVEL INICIAL	IMPACTO	% EFECTIVIDAD DE CONTROL	IMPACTO RESIDUAL	NIVEL RESIDUAL
MUY ALTO	10	70%	3	BAJO
ALTO	8	70%	3	BAJO
MEDIO	6	70%	2	MUY BAJO
BAJO	4	70%	2	MUY BAJO
MUY BAJO	2	70%	1	MUY BAJO

Tabla 17 - Impacto residual con el 70% de eficacia de los controles

NIVEL INICIAL	IMPACTO	% EFECTIVIDAD DE CONTROL	IMPACTO RESIDUAL	NIVEL RESIDUAL
MUY ALTO	10	90%	1	MUY BAJO
ALTO	8	90%	1	MUY BAJO
MEDIO	6	90%	1	MUY BAJO
BAJO	4	90%	1	MUY BAJO
MUY BAJO	2	90%	1	MUY BAJO

Tabla 18 - Impacto residual con el 90% de eficacia de los controles

Se deben asociar los controles que apliquen para cada riesgo, hay que tener especial cuidado en asociar controles que realmente estén asociados al riesgo, porque de lo contrario se podría estar reduciendo el nivel del riesgo con controles incorrectos. En cuanto a la evaluación de controles, es una actividad que se debe realizar con el conocimiento de la operación y se debe tener presente que, dependiendo del nivel elegido, hay que tener las evidencias.

12.TRATAMIENDO

- **Aceptar:** Dentro de la metodología de gestión de riesgos se determinan niveles y se decide que niveles de riesgos residual aceptará la organización en señal que dichos riesgos cuentan con controles suficientes y eficaces. En este caso la organización aprobó:

- Aceptar los riesgos con niveles residuales en nivel: 1, 2 y 3, para lo riesgos de: ISO 20000-1:2018, ISO 14001:2015, ISO 45001:2018, ISO 27001:2013, ISO 22301:2018, SAGRILATF y PTEE:
- Aceptar los riesgos con niveles residuales en nivel: 1, 2 para la norma ISO 27701:2020.

- **Mitigar:** Definir un plan de tratamiento del riesgo para reducir la probabilidad y/o el impacto de tal forma que el nivel de riesgo residual baje a un nivel aceptado por la organización. Este tratamiento aplica para los siguientes niveles.

  - Niveles 4 y 5 para los riesgos de: ISO 20000-1:2018, ISO 14001:2015, ISO 45001:2018, ISO 27001:2013, ISO 22301:2018, SAGRILATF y PTEE:
  - Niveles 3, 4 y 5 para los riesgos de: ISO 27701:2020.

  Si al concluir el plan de tratamiento de riesgo y evaluar nuevamente los controles el nivel residual se mantiene en un nivel que no es aceptado por la organización, se debe definir un nuevo plan.

- **Evitar:** Eliminar la actividad que origina el riesgo.

- **Transferir:** Cuando la responsabilidad de definición e implantación de controles no es responsabilidad de la organización, se podrían transferir a Proveedores, Clientes, entre otros.

- **Compartir:** Cuando uno o varios controles están asociados a la compra de pólizas, seguros, entre otros. Con lo cual en el caso que se materialice la organización acude a lo contratado para mitigar el impacto.

13. RIESGOS EMERGENTES

La gestión de riesgos debe ser permanente no se debe esperar a la reválida anual de riesgos que se realiza desde el área de experiencia del cliente, para identificar nuevos riesgos. Los riesgos emergentes son los que se van generando en el día a día, debido a cambio de infraestructura, nuevos clientes, cambios en la organización, nuevos requerimientos legales, entre otros. Un riego puede ser identificado por cualquier colaborador de la organización y es responsable de reportarlo al área encargada de gestionar los riesgos.

12.1 COMUNICACIÓN DE RIESGOS

La identificación, registro, evaluación y comunicación de los riesgos se realiza de acuerdo con el documento: Proceso Gestión de Riegos.

14. REEVALUACIÓN DE RIESGOS Y CONTROLES

Mínimo una vez al año se debe realizar una revalida de riesgos y de los controles asociados a los riesgos. Esta reválida se realiza entre los Gestores de procesos, gerente de unidad de

negocio, vertical y/o área de apoyo, con el dueño del riesgo y cualquier otro rol que este involucrado en la gestión de riesgos.

15. ACTIVOS DE INFORMACIÓN (ISO 27001:2013)

La organización debe identificar los activos de información, se debe elaborar un inventario de estos y mantenerlo actualizado. Tener un inventario permite clasificar los activos de información para identificar cuales son los más críticos y por lo tanto a los que se les deben aplicar más controles y vigilarlos de cerca.

El inventario de activos de información mínimo debe tener los siguientes atributos:

- Nombre
- Tipo de Activo
- Propietario
- Custodio Técnico
- Clasificación de la información (privada, publica, confidencial)
- Etiquetado y manipulación de la información
- Ubicación (física y/o electrónica)
- Criticidad
- Roles y privilegios
- Retención
- Disposición final

Para los riesgos relacionados con la norma ISO 27001:2013 se debe relaciona el activo de información involucrado, lo anterior con el fin que también se puedan ver los riesgos por cada uno de los activos de información.

16.GESTIÓN DE RIESGOS EN PROYECTOS

Para los proyectos se deben registrar y gestionar los riesgos en la matriz: 441087 - Matriz de identificación y gestión de Riesgos en proyectos. Aplican los mismos criterios definidos en esta metodología, la única diferencia es que no se registran en la herramienta de gestión, si no en la matriz.

17. OPORTUNIDADES O RIESGOS POSITIVOS

Son los riesgos positivos y para este caso se deben maximizar los resultados que estos generan. Las oportunidades se identifican en varios escenarios:

- Cuando se realiza el análisis del contexto de la organización utilizando una DOFA como herramienta.
- Cuando se identifican circunstancias y/o eventos que pueden llegar a generar:
    - Nuevos productos y/o servicios
    - Productos y/o servicios que complementen a servicios primarios

- Llevar los productos a países diferentes
- La utilización de nuevas tecnologías

Cuando se identifique una oportunidad se evaluará de la siguiente manera:

- Beneficios que traerá para la compañía
- Si se va a requerir recursos económicos para la implementación o desarrollo de esta.
- Que dedicación de recursos humanos se va a necesitar.
- Las unidades de negocio que se verán afectadas por dicha oportunidad
- Si tiene impacto directo en los clientes
- El riesgo asociado a la oportunidad
- El impacto y la probabilidad de ocurrencia utilizando los mismos criterios definidos para riesgos.

La oportunidad deberá ser evaluada por los gerentes de las unidades de negocio y verticales que se verán afectadas y luego será presentada a la alta gerencia para aprobación final. En el caso que sea aprobada como una oportunidad para la cual se va a definir un plan de trabajo, se gestionará de acuerdo con lo mencionado en el documento: Proceso Gestión de Riegos.

18.ANEXOS

16.1 Controles, Causas, Consecuencias

16.4 Matriz de identificación y gestión de riesgos