POLÍTICA CORPORATIVA GESTIÓN DE RIESGOS

ANEXO – Metodología para la Gestión de Riesgos TI

Versión	Descripción de cambios	Aprobación	Vigencia
1.0	Versión inicial	Martín Idígoras	Octubre 2020
2.0	Incorporación de cálculo del riesgo residual	Martín Idígoras	Julio 2022
3.0	Incorporación de tratamiento de riesgos que no aplican y riesgos asumidos	Martín Idígoras	Octubre 2023

Este documento contiene información de propiedad de Coca - Cola Andina, que ha sido preparada estrictamente con el propósito de ser utilizada en las operaciones de la Compañía y no podrá ser proporcionada, refraseada o revelada parcial o totalmente a terceros sin la autorización expresa de la Gerencia Corporativa responsable de este documento.

INDICE

Introducción 3
1. Objetivo 4
2. Consideraciones 4
3. Impacto / Severidad en Coca-Cola Andina 4
4. Metodología 5
4.1. Identificación de Riesgos 5
4.2. Análisis de Riesgos 6
4.3. Evaluación de Riesgos 8
4.4. Método de Cálculo del Riesgo inherente (o severidad del riesgo) 8
4.5. Riesgo residual 9
4.6. Matriz de riesgos 11
5. Tratamiento de riesgos con estatus de “No Aplican” o “Asumidos” 13
6. Conclusiones 14

Introducción

Coca-Cola Andina inició en el año 2019 el desarrollo de 2 proyectos (BIA - Business Impact Analisys- y RIA IT – Risk Impact Analisys Information Technology) regionales para unificar el riesgo y los procesos que son considerados críticos para la compañía por medio de acciones y métodos comunes. Para responder a este cometido, se comenzó por determinar un modelo de BIA estableciendo los procesos críticos para sus operaciones y en función de estos y a partir de los componentes de infraestructura, sus aplicaciones y proveedores que lo soportan, se construyó un RIA de TI donde se materializó el perfil de riesgo tecnológico que impacta sobre cada uno de los ellos, produciendo en el ámbito de la operación de Andina riesgos que el negocio debe considerar en un pilar específico dentro de su modelo de riesgo corporativo.

1. Objetivo

Al inicio del proyecto RIA TI, Coca-Cola Andina no contaba con una metodología formal de evaluación de riesgos de TI, ni tampoco con resultados integrales de análisis; si bien existían prácticas de tratamientos de riesgos y planes de acción, éstas no se encontraban unificadas y controladas de manera central ni alineadas con una definición de procesos críticos del negocio.

Debido a que la metodología utilizada por el RIA difiere en varios aspectos de la metodología de gestión de riesgos corporativo, se hizo necesario generar este documento, el cual contiene los lineamientos necesarios para realizar un proceso adecuado para la evaluación, medición y gestión de los riesgos asociados a la tecnología.

2. Consideraciones

El RIA TI se construyó sobre la base de un proceso de definición de análisis de Impacto de Negocio (BIA) que identificó cuáles unidades de negocio, funciones, procesos y aplicaciones computacionales, son críticas para la viabilidad del negocio ante una situación de desastre. El BIA facilita a la vez la identificación de los parámetros de tiempo asociados a las unidades de negocio críticas, para retornar a su total operación parcial o normal después de un desastre.

También permite determinar el impacto producido al negocio en diversos escenarios de desastre y la habilidad para continuar operando con los procesos de misión crítica. Así también, el BIA permite identificar los recursos necesarios que permitan reanudar las operaciones del negocio al tiempo y nivel de producción que permita la supervivencia del negocio

En consecuencia, el RIA TI se suscribió exclusivamente a las áreas y macroprocesos críticos definidos y aprobados en el BIA por la dirección de Coca-Cola Andina en cada de sus operaciones. Asimismo, para efectos de escenarios de crisis o catástrofe y los recursos requeridos para ello, se define sólo el escenario de interrupción prologada (crisis o catástrofe) en los servicios TI.

3. Impacto / Severidad en Coca-Cola Andina

La Dirección de Coca-Cola Andina en su responsabilidad y compromiso con la Gestión de Continuidad del Negocio, ha conciliado y aprobado los criterios que permitirán a los responsables/dueños de procesos críticos de negocio, determinar de manera objetiva el impacto y criticidad que tendría la disrupción prolongada de un proceso crítico, por causa de la tecnología que se materializó en una Matriz Impacto Criticidad y sobre la misma la dirección de cada país identificó los procesos críticos del negocio por medio de un Acta de sanción de procesos críticos aprobada formalmente por cada operación

4. Metodología

La metodología de conducción del RIA TI, se formuló sobre el criterio de establecer una serie de requisitos de línea base mandatorios, considerados un mínimo razonable de prácticas, que permitan asegurar que la infraestructura de Servicios y Operaciones de TI tienen los riesgos relevantes identificados y razonablemente controlados.

Estos requisitos de línea base consideran prácticas relacionadas a gestión, monitoreo, seguridad TI, seguridad de información, ciberseguridad, seguridad y administración de bases de datos, seguridad y administración de redes y comunicaciones, entre otros. Estos requisitos se ordenaron para conformar 3 grandes ámbitos de riesgos para los procesos de negocio: las Aplicaciones, la Infraestructura y los Proveedores (vendors), todos ellos dispuestos sobre una guía de evaluación de riesgos, dándole una connotación de vulnerabilidad, a lo cual el especialista debe declarar la probabilidad de ocurrencia de esa vulnerabilidad en Coca-Cola Andina, dentro de una escala de probabilidades de 1 a 5 (muy baja, baja, media, alta, o muy alta respectivamente).

Para efectos de levantamiento de los riesgos se diseñó una serie de artefactos para evaluar cada componente tecnológico sobre una serie de requisitos o prácticas mandatorias de línea base (base line), declaradas en una lógica de vulnerabilidad con el propósito que el especialista técnico, por medio de una evaluación experta, le permite afirmar que esa "vulnerabilidad" se encuentra en Coca-Cola Andina con una probabilidad de ocurrencia según la escala definida en el párrafo anterior.

La metodología establece los siguientes elementos que la conforman:

- Un conjunto de componentes tecnológicos cuyos riesgos se evalúan en 3 ámbitos de acción (Aplicaciones, la Infraestructura y los Proveedores)
- Un conjunto de 20 categorías generales de vulnerabilidades TI
- Un conjunto de 222 vulnerabilidades para las 20 categorías dependiendo del componente tecnológico donde se define un subconjunto de amenazas y vulnerabilidades a evaluar en la forma de riesgos tecnológicos.

4.1. Identificación de Riesgos

El propósito de la identificación de riesgos es buscar, reconocer y describir los riesgos que podrían eventualmente impedir que la organización TI cumpla sus objetivos para lo cual se ha definido una línea base de requisitos mandatorios que la organización TI debe cumplir para mitigar los riesgos existentes en los procesos críticos.

Considerando que cada componente tecnológico que soporta un proceso de negocio crítico al momento de su falla, mal funcionamiento, o destrucción, tendrá un impacto de alta severidad sobre el negocio, es que se ha establecido una serie de categorías de riesgos considerando diversos ámbitos, dentro de las cuales se

definen estos requisitos de línea base mandatorios, en términos de "vulnerabilidades" y su probabilidad de ocurrencia en Coca-Cola Andina.

Este requisito de línea base es mandatorio, y es un mínimo de cumplimiento que un componente tecnológico debe cumplir forzosamente por tratarse de un componente que soporta un proceso crítico del negocio. Es por ello que en la escala de probabilidades de ocurrencia, se considerará un riesgo a tratar todas aquellas probabilidades desde 3 (media), 4 (alta), y, 5 (muy alta).

El siguiente cuadro muestra las diversas categorías de riesgos, y la cantidad de "requisitos de línea base" expresadas en "cantidad de vulnerabilidades" según sea la respuesta del evaluador:

#	Categorías de Riesgos TI	# Vulnerabilidades por Categoría
1	Fallas de Aplicaciones o Sistemas Operativos	13
2	Fallas de Enlaces	16
3	Fallas de Hardware	10
4	Fallas de Integridad de Datos	13
5	Backup y Planes de CONTINGENCIA NO Disponibles	9
6	Fallas Funcionales de Sistemas	10
7	Cyber Ataques (interno externo)	15
8	Acceso no Autorizado	5
9	Seguridad Informática	9
10	Falla de Personal (USUARIO)	12
11	Falla de Personal (ESPECIALISTA)	12
12	Administración Basdes de Datos	9
13	Seguridad de Bases de Datos	11
14	Administración SAP	11
15	Seguridad SAP	12
16	Siniestros Salas de Equipos, Datacenter, Shafts, Gabinetes, Equipos	17
17	Vendor - Operación Normal del Servicio	15
18	Vendor - Contrato de Servicio	10
19	Vendor - Resiliencia del Proveedor	8
20	Vendor - Seguridad de Información	5
	TOTAL	222

4.2. Análisis de Riesgos

El propósito del análisis de riesgos es comprender la naturaleza del riesgo y sus características, incluyendo el nivel de riesgo. El análisis de riesgos involucra consideraciones sobre las fuentes de riesgo, niveles de incertidumbre, probabilidades de ocurrencia, eventos de riesgos y sus planes de acción o tratamiento como medida de mitigación. Para los propósitos del RIA-TI, el análisis de riesgo considera la probabilidad de que ciertos requisitos deben cumplirse, de lo contrario, representa una vulnerabilidad y por ende una exposición a un cierto nivel de riesgo.

Otra de las consideraciones basales que establece esta metodología, es que todos los componentes identificados como soporte de procesos críticos, tendrán un impacto constante equivalente a nivel 5 (muy

alto). Ello, porque detrás está la eventual interrupción, prolongada o no, de los procesos críticos que soporta.

Estas definiciones propias del análisis servirán de "input" para el proceso de evaluación de los riesgos y las decisiones relacionadas a si el riesgo debe ser tratado, y cómo. En general todos los riesgos que califiquen de nivel 3 o superior, deberán conformar obligatoriamente un plan de tratamiento de riesgo con el fin de reducirlos a la mínima expresión o simplemente eliminarlos. Los procesos críticos del negocio no pueden tener riesgos críticos en TI sin haberlos debidamente identificado, analizado, evaluado y controlado permanentemente en un proceso de gestión. De lo contrario, expone al negocio a graves consecuencias en caso de fallas.

El siguiente cuadro describe como se configuraron los riesgos para cada tipo de componente tecnológico y la cantidad de requisitos de línea base que cada componente debiera reflejar "libre de riesgo" como exigencia básica para componentes tecnológicos que soportan procesos críticos del negocio.

Cuadro de identificación de perfiles de riesgo para componentes tecnológicos.

#	Categorías de Riesgos TI	SISTEMAS	Aplicaciones	Bases de Datos Aplicaciones	SAP	Bases de Datos SAP	INFRAESTRUCTURA	Servidores	Sistemas Operativos	Hardware	Networking & Comm	ENLACES	Switches	Routers	Firewalls	Storage & Backup	Sistemas Operativos	Hardware	Datacenter & Facilities	Datacenter	Facilities	Vendors	TI VT	Otros
1	Fallas de Aplicaciones o Sistemas Operativos		13						13				13	13	13		13							
2	Fallas de Enlaces											16												
3	Fallas de Hardware									10			10	10	10			10						
4	Fallas de Integridad de Datos		13																					
5	Backup y Planes de CONTINGENCIA NO Disponibles		9						9	9			9	9	9		9	9						
6	Fallas Funcionales de Sistemas		10																					
7	Cyber Ataques (Interno externo)		15						15								15							
8	Acceso no Autorizado		5						5	5			5	5	5		5	5						
9	Seguridad Informática		9						9	9							9	9						
10	Falla de Personal (USUARIO)		12																					
11	Falla de Personal (ESPECIALISTA)		12						12								12							
12	Administración de Bases de Datos			9		9																		
13	Seguridad de Bases de Datos			11		11																		
14	Administración SAP				11																			
15	Seguridad SAP. SAP(15-2): Backup, DRP y Contingencias de Sites				21																			
16	Siniestros Salas de Equipos, Datacenter, Shafts, Gabinetes, Equipos																			17	17			
17	Vendor - Operación Normal del Servicio																						15	15
18	Vendor - Contrato de Servicio																						10	10
19	Vendor - Resiliencia del Proveedor																						8	8
20	Vendor - Seguridad de Información																						5	5
	TOTAL	170	98	20	32	20	353	96	63	33	127	16	37	37	37	96	63	33	34	17	17	76	38	38

4.3. Evaluación de Riesgos

El propósito de la evaluación es apoyar las decisiones relacionadas a las acciones a tomar. La evaluación involucra comparar los resultados del análisis con los criterios establecidos a fin de determinar si requieren acciones adicionales, en particular para el tratamiento de los riesgos, o reformular los objetivos.

4.4. Método de Cálculo del Riesgo inherente (o severidad del riesgo)

El riesgo inherente (o severidad) es aquél al que se enfrenta una Operación en ausencia de acciones mitigantes que modifiquen su probabilidad o impacto.

Las probabilidades de ocurrencia se expresan en los términos y valores siguientes:
- Probabilidad muy baja = 1
- Probabilidad baja = 2
- Probabilidad media = 3
- Probabilidad alta = 4
- Probabilidad muy alta = 5

El impacto se puede definir como el daño que supondría para la Operación el hecho que el riesgo se materialice. La magnitud del impacto se expresa en los términos y valores siguientes:
- Impacto muy bajo = 1
- Impacto bajo = 2
- Impacto medio = 3
- Impacto alto = 4
- Impacto muy alto = 5

Finalmente, el riesgo inherente o severidad del riesgo será el producto de la probabilidad por el impacto. En el caso particular del RIA-TI de procesos críticos del negocio, el impacto siempre será constante e igual a 5 (Impacto muy alto).

El siguiente cuadro representa los valores de riesgo y su severidad. Para efectos del RIA-TI se considerará un riesgo a tratar con un plan de acción, todo valor que esté en los rangos del cuadro.

RIESGO	
10 < R < = 15 MEDIO	3
15 < R < = 20 ALTO	4
20 < R MUY ALTO	5

a) Desde la planilla de evaluación de riesgo llenada por especialistas para cada componente, se contabilizan las instancias de riesgo medio o superior, generando scores múltiplos de 5 (impacto constante), de los cuales finalmente se obtiene un promedio de ellos. Esto se refleja en el punto 4 del

siguiente cuadro, donde se encuentran 2 instancias de riesgo de toda la categoría RTI-01 (indicada en el punto 3), uno alto y uno medio, que generan scores de 20 y 15 respectivamente. Luego el promedio simple de esos riesgos es 17.5, el cual se presenta en el punto 2 del cuadro.

b) A partir del punto 2, se representa el total de riesgos (vulnerabilidades) a modo de resumen de la categoría RTI-01 (indicada en el punto 1).

c) Luego así se contabilizan todos los riesgos (vulnerabilidades) para cada una de las categorías de riesgos definidas para evaluar aplicaciones. Refiérase al punto 4.2 de este documento para ver el perfilamiento de riesgos para cada componente tecnológico.

Método de Cálculo del Riesgo

1 2 3 4

VULN	Total Riesgo	Total Vulnerabilidades	APP Fletero # Vuln.	APP Fletero Riesgo	B2B # Vuln.	B2B Riesgo	COT # Vuln.	COT Riesgo	Lotus Notes # Vuln.	Lotus Notes Riesgo	MapInfo # Vuln.	MapInfo Riesgo	N # Vu
RTI-01	18.7	32	1	20.0	0	0.0	2	20.0	3	20.0	2	17.5	0
RTI-04	16.4	24	0	0.0	2	15.0	1	20.0	0	0.0	1	16.3	2
RTI-05	18.1	15	1	15.0	1	15.0	1	20.0	0	0.0	1	20.0	0
RTI-06	17.7	32	0	0.0	1	25.0	1	15.0	4	20.0	5	16.0	0
RTI-07	15.0	6	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0
RTI-08	17.5	6	0	0.0	0	0.0	0	0.0	1	20.0	0	0.0	0
RTI-09	15.0	36	0	0.0	0	0.0	0	0.0	0	0.0	9	15.0	0
RTI-10	15.0	25	4	15.0	1	15.0	0	0.0	0	0.0	0	0.0	0
RTI-11	17.6	25	0	0.0	0	0.0	0	0.0	0	0.0	3	18.3	0
	16.8	201	6	16.7	5	17.5	5	18.8	8	20.0	24	17.2	2

	Total Riesgo	Total al Vulnerabilida	APP Fletero Prob	APP Fletero Riesgo	B2B Prob	B2B Riesgo	COT Prob	COT Riesgo	Lotus Notes Prob	Lotus Notes Riesgo	MapInfo Prob	MapInfo Riesgo	MCocaCola Prob	MCocaCola Riesgo	Order Prob	Order Riesgo
RTI-01	1	2	2	0.0	1	0.0	1	0.0	1	0.0	2	0.0	1	0.0	1	0.0
	2	2	1	0.0	1	0.0	1			0.0	1	0.0	1	0.0	4	20.0
	3	2	1	0.0	1	0.0	1			0.0	1	0.0	1	0.0	4	20.0
	4	3	1	0.0	1	0.0	1			0.0	1	0.0	1	0.0	1	0.0
	5	2	1	0.0	1	0.0	4	20.0	1	0.0	1	0.0	1	0.0	1	0.0
	6	0	1	0.0	1	0.0	1	0.0	1	0.0	1	0.0	1	0.0	1	0.0
	7	2	1	0.0	1	0.0	4	20.0	1	0.0	1	0.0	1	0.0	1	0.0
	8	2	1	0.0	1	0.0	1	0.0	4	20.0	1	0.0	1	0.0	4	20.0
	9	2	1	0.0	1	0.0	1	0.0	4	20.0	1	0.0	1	0.0	4	20.0
	10	3	4	20.0	1	0.0	1	0.0	1	0.0	1	0.0	1	0.0	1	0.0
	11	5	1	0.0	1	0.0	1	0.0	1	0.0	4	20.0	1	0.0	5	25.0
	12	2	1	0.0	1	0.0	1	0.0	4	20.0	1	0.0	1	0.0	1	0.0
	13	5	1	0.0	1	0.0	1	0.0	1	0.0	3	15.0	1	0.0	4	20.0
		32	1	20.0	0	0.0	2	20.0	3	20.0	2	17.5	0	0.0	4	20.0
	1															

4.5. Riesgo residual

A partir del mes de Julio 2021 se incorporó en el RIA el cálculo del riesgo residual.

La exposición al riesgo o riesgo residual es aquel que permanece después que las Operaciones han puesto en práctica sus acciones mitigantes, y el mismo se calcula en función de la siguiente fórmula:

Riesgo Residual = (Probabilidad * impacto)*(1-Contribución acciones mitigantes)

Por otra parte, el porcentaje de contribución de acciones de mitigación a utilizar será el siguiente:

Porcentaje de contribución de las acciones de mitigación		
Categoría	Porcentaje	Descripción general
Óptima	**95%**	La acción mitiga razonablemente el riesgo y cumple con requisitos tales como: documentación, registro oportuno y adecuado, autorización, formalización, segregación de funciones, supervisión, capacitación del personal y, en el caso de seguros, cobertura, etc.
Buena	**85%**	La acción mitiga razonablemente el riesgo, sin embargo, presenta debilidades de forma que podrían afectar su continuidad y calidad, por ejemplo, en caso de un cambio en la estructura organizacional.
Deficiente	**0%**	No hay acción mitigante o la existente debe ser rediseñada desde su origen para mitigar razonablemente el riesgo.

De lo anterior, se obtiene el siguiente cuadro, en el cual se pueden apreciar los valores de riesgo residual que pueden obtenerse, en función de la severidad del riesgo y del porcentaje de contribución de las acciones de mitigación

Riesgo Residual (Exposición efectiva al riesgo)				
Contribución:		Óptima (95%)	Buena (85%)	Deficiente (0%)
Exposición:		1-95%	1-85%	100%
Severidad Alta	25	1,3	3,8	25
	20	1	3	20
Severidad Media	15	0,8	2,3	15

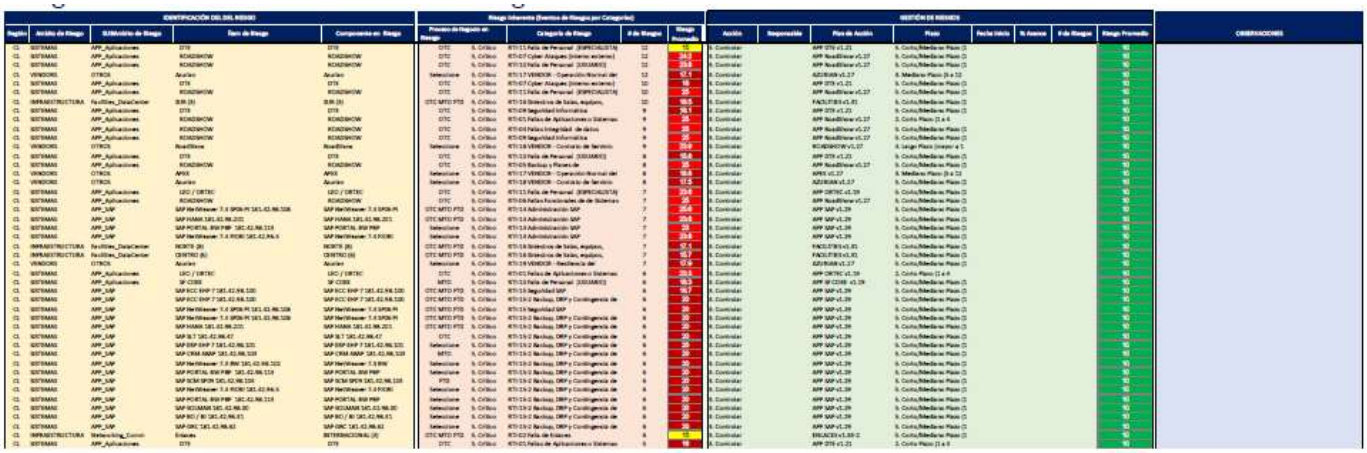
Cuando el riesgo residual se encuentra entre 0,8 y 3,8 se entenderá que el Riego se encuentra mitigados y por ello que no se requieren acciones adicionales, sin embargo, se debe monitorear que se mantenga la eficacia y eficiencia de las ya existentes

Se determina que un riesgo esta mitigado cuando el riesgo residual es aceptado por el especialista, bien sea porque no se considera necesaria una acción adicional a la ya existente y la misma garantiza el correcto funcionamiento del proceso

4.6. Matriz de riesgos

La matriz de riesgos TI asociados a los procesos críticos del negocio de Andina, es una herramienta de gestión y control de los riesgos identificados y sus acciones establecidas para su tratamiento.

El siguiente cuadro muestra la estructura general de la matriz:



El siguiente cuadro parcial de la matriz, **identifica detalladamente los componentes de riesgo evaluados**. Por medio de una serie de menús "drop-down" es posible identificar rápidamente el ítem de riesgo basado en el modelo de perfiles indicado en el punto 4.2 de este documento:

IDENTIFICACIÓN DEL DEL RIESGO				
Región	Ambito de Riesgo	SUBAmbito de Riesgo	Ítem de Riesgo	Componente en Riesgo
CL	SISTEMAS	APP_Aplicaciones	DTE	DTE
CL	SISTEMAS	APP_Aplicaciones	ROADSHOW	ROADSHOW
CL	SISTEMAS	APP_Aplicaciones	ROADSHOW	ROADSHOW
CL	VENDORS	OTROS	Azurian	Azurian

El siguiente cuadro parcial de la matriz**, identifica el riesgo inherente**, detalladamente para cada proceso de negocio, su impacto que siempre es crítico, la categoría de riesgo y la cantidad de riesgos existentes dentro de la categoría. Finalmente, se expresa el "score" del riesgo de la categoría a fin de tenerlo presente.

Riesgo Inherente (Eventos de Riesgos por Categorías)				
Proceso de Negocio en Riessgo		Categoría de Riesgo	# de Riesgos	Riesgo Promedio
OTC	5. Crítico	RTI-11 Falla de Personal (ESPECIALISTA)	12	15
OTC	5. Crítico	RTI-07 Cyber Ataques (interno externo)	12	24.2
OTC	5. Crítico	RTI-10 Falla de Personal (USUARIO)	12	23.8
Seleccione	5. Crítico	RTI-17 VENDOR - Operación Normal del	12	17.1

El siguiente cuadro parcial de la matriz, **identifica las acciones de gestión de los riesgos**, a fin de registrar el estado de avance de los planes de tratamiento de riesgos. Cabe destacar que cada categoría de riesgos asociados a un proceso de negocio específico tiene su respectivo plan de acción, cuyo nombre aparece como el sufijo del nombre de las planillas Excel que contienen los respectivos planes, y que se encuentran en los respectivos repositorios. Esta parte de la matriz permite íntegramente el ingreso de datos de control para efectos de la gestión de riesgos.

GESTIÓN DE RIESGOS							
Acción	Responsable	Plan de Acción	Plazo	Fecha Inicio	% Avance	# de Riesgos	Riesgo Promedio
3. Controlar		APP DTE v1.21	5. Corto/Mediano Plazo (1				10
3. Controlar		APP RoadShow v1.27	5. Corto/Mediano Plazo (1				10
3. Controlar		APP RoadShow v1.27	5. Corto/Mediano Plazo (1				10
3. Controlar		AZURIAN v1.27	3. Mediano Plazo (5 a 12				10

En función de las directrices para el cálculo del riesgo residual indicadas en el punto 4.5, se procedió a actualizar todas las planillas de plan de acción a fin de incorporar en las mismas la fórmula que en función del estatus del riesgo (Mitigado al 85 ó 95%, pendiente, asumido o con plan) permita generar el valor del riesgo residual tanto a nivel de cada riesgo como de cada categoría:

01. MUY Crítica	RIESGO TOTAL	16,4	Riesgo CAT	16,0
	TOTAL de Amenazas	10	Riesgo residual CAT	2,4
	TOTAL de Vulnerabilidades	56	Vulnerabilidades CAT	5

	Responsabilidades	Plazo para el Tratamiento	R. Residual	Revisión y Monitoreo	Estado de Implementación	Costo Estimado	
						Esfuerzos [horas]	Costo [USD$]
a	• Administrador de la Aplicación. • Gestión de Incidentes • Seguridad/Riesgo TI	2. Corto Plazo (1 a 4 meses)	2,3	https://kpandina.sharepoint.com/sites/Corporativo/EY94xdDh1YWHe0Yaxc6KK1WaE46DcJixmkedIzPmHgraGka?e=9eUEug	4. Riesgo Tratado - Bueno 85%		

Por último, se realizó la modificación en cada una de las matrices de riesgo a fin de que, por cada ámbito y componente, tome del plan de acción el valor del riesgo residual de cada categoría:

% Avance	# de Riesgos MITIGADOS	Riesgo Residual	OBSERVACIONES
100,00	5	2,4	Revisar con riesgos
100,00	5	2,7	
91,67	11	3,3	
100,00	10	2,4	
33,33	3	10,8	

5. Tratamiento de riesgos con estatus de "No Aplican" o "Asumidos"

Luego de la evaluación de riesgos en los distintos ámbitos, pudiese suceder que al momento de realizar el análisis para la mitigación del mismo los especialistas concluyan algunas de las siguientes situaciones:

A. Riesgos que No aplican
B. Riesgos Asumidos o No mitigados.

5.1. Se define que un riesgo No Aplica sólo para los casos en que:

- Al momento de realizar el análisis del riesgo se detecta que la herramienta, aplicación, etc., que le da origen será reemplazada por otra en el corto plazo.
- Se determina que la evaluación inicial fue errónea y que el riesgo no afecta a ninguno de los procesos del negocio definidos como críticos dentro del BIA y por ende no debe invertirse ningún tipo de esfuerzo en realizar su mitigación.

Para que pueda definirse que un riesgo no aplica, y por ende sea eliminado de la matriz de riesgos, debe suceder lo siguiente:

a) Una vez que el especialista que evalúa el riesgo identifica que el mismo no aplica por los motivos antes indicados (la herramienta será reemplazada en el corto plazo o la misma no soporta ninguno de los procesos críticos del negocio), debe comunicarlo al IT Business Partner (ITBP) del país que corresponde.

b) Seguidamente, debe generarse una reunión conjunta con el ITBP del país, el CISO (responsable de Seguridad Regional) quien es la persona responsable de la matriz de riesgos, y el CIO ante quienes se deberán exponer los motivos por los cuales el riesgo No Aplica.

c) En caso de que el CIO y el CISO acuerden que el riesgo efectivamente no aplica, la persona solicitante enviará correo al CIO y CISO con copia al ITBP, formalizando la solicitud a lo cual estos últimos deberán responder indicando conformidad. Este documento quedará como respaldo de la operación realizada y justificará en caso de ser necesario, el por qué de la variación del número de riesgos totales del país.

Luego de obtener la aprobación escrita para asignar al riesgo la calidad de "No Aplica" el mismo deberá eliminarse de la Matriz de riesgos dejando sin efecto el scoring o riesgo inherente que le fue asignado al momento de su evaluación y por ende no será incluido dentro del total de riesgos del país al que corresponda

5.2. **El riesgo se asume.** En este caso el riesgo es aceptado por el especialista, bien sea porque la materialización del riesgo no pone en peligro a ninguno de los procesos definidos como críticos o porque la empresa cuenta con un proceso de contingencia para mitigar dicho riesgo en caso de que el mismo se materialice.
En cualquiera de los casos se requerirá de un control y seguimiento periódico de este tipo de riesgos y además deberá quedar documentada la evidencia formal del especialista que indique los motivos que sustenten dicha decisión. Esta documentación debe incluir un informe del especialista y los anexos que demuestren que asumir el riesgo no pone en peligro el correcto funcionamiento del proceso crítico con el que está mapeado. Los riesgos asumidos serán identificados a través del "estatus" del riesgo lo que permite su identificación y seguimiento posterior.

6. Conclusiones

En definitiva, las Operaciones deben asegurar razonablemente que los riesgos tecnológicos asociados a los procesos críticos del negocio se encuentran mitigados. La metodología del RIA establece procesos, procedimientos y controles que permiten identificar y monitorear los riesgos, al mismo tiempo que establece las acciones necesarias para su mitigación.