IMPLEMENTACIÓN DE LA PLATAFORMA ISOLUCIÓN® PARA LA SISTEMATIZACIÓN Y ESTANDARIZACIÓN DE LA GESTIÓN DEL RIESGO EN ONELINK COLOMBIA S.A.S.

ONELINK COLOMBIA S.A.S.

DANIELA BAENA LÓPEZ

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE INGENIERÍAS
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL
MONTERÍA, CÓRDOBA
2021

IMPLEMENTACIÓN DE LA PLATAFORMA ISOLUCIÓN® PARA LA SISTEMATIZACIÓN Y ESTANDARIZACIÓN DE LA GESTIÓN DEL RIESGO EN ONELINK COLOMBIA S.A.S.

ONELINK COLOMBIA S.A.S.

DANIELA BAENA LÓPEZ

Trabajo de grado presentado, en la modalidad de Práctica Empresarial para optar al Título de Ingeniero Industrial

Director (es):

JAIRO DANIEL OCHOA GUERRA, M.Sc.
BRIAN DAVID CARO MARTÍNEZ, Ing.

UNIVERSIDAD DE CÓRDOBA
FACULTAD DE INGENIERÍAS
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL
MONTERÍA, CÓRDOBA
2021

La responsabilidad ética, legal y científica, de las ideas, conceptos, y resultados del proyecto de investigación, serán responsabilidad de los autores.
Artículo 59, Acuerdo N° 022 del 21 de febrero de 2018 del Consejo Superior.

Tener en cuenta los Artículos y directrices establecidos la Resolución 1775, del 21 de agosto de 2019. En donde se establecen las directrices y las políticas de funcionamiento del repositorio institucional de la Universidad de Córdoba (Artículos tercero, octavo, once, entre otros).

"11 – BUENA FE: La universidad considera que la producción intelectual que, los profesores, funcionarios administrativos y estudiantes le presenten, es realizada por éstos, y que no han transgredido los derechos de otras personas. En consecuencia, la aceptará, protegerá, publicará y explotará, según corresponda y lo considere pertinente". Artículo 1, Acuerdo N° 045 del 25 de mayo de 2018 del Consejo Superior.

Nota de aceptación

_____

_____

_____

_____

_____

Firma del jurado

_____

Firma del jurado

TABLA DE CONTENIDO

1. INTRODUCCIÓN 9
2. PLATAFORMA ESTRATÉGICA DE LA EMPRESA 11
2.1. RESEÑA HISTÓRICA 11
2.2. ¿QUIÉNES SOMOS? 11
2.3. LOGOTIPO 12
2.4. UBICACIÓN SEDE AVENTURA 12
2.5. PROPÓSITO 12
2.6. VALORES CORPORATIVOS 12
2.7. POLÍTICAS CORPORATIVAS 12
2.8. DESCRIPCIÓN DEL ÁREA DE TRABAJO 14
3. MARCO TEÓRICO O CONCEPTUAL 16
3.1. GESTIÓN DEL RIESGO 16
3.1.1. Fases para la gestión o administración de riesgo 17
3.2. GOBIERNO DE GESTIÓN DEL RIESGO EN ONELINK 18
3.3. ISOLUCIÓN® 20
4. DIAGNÓSTICO ESPECÍFICO DE LA EMPRESA 21
4.1. METODOLOGÍA PARA GESTIONAR LOS RIESGOS SARO Y SI 21
4.2. OBJETIVOS 25
4.2.1. Objetivo general 25
4.2.2. Objetivos específicos 25
5. ACTIVIDADES DESARROLLADAS 26

5.1. ESTANDARIZACIÓN Y ADECUACION DE LA INFORMACIÓN 26
5.1.1. Diseño de plantilla para registro de los riesgos en Excel 26
5.1.2. Borrado de registros corruptos en el módulo de riesgos (producción) 26
5.2. RECOLECCIÓN Y ANÁLISIS DE INFORMACIÓN 27
5.2.1. Levantamiento de información con dueños de proceso, subproceso o área .. 27
5.3. DEFINICIÓN DE METODOLOGÍA PARA LA GESTIÓN DE LOS RIESGOS 27
5.3.1. Fases para la gestión del riesgo 27
5.3.1.1. Identificación. 27
5.3.1.1.1. Parametrización fase de identificación. 28
5.3.1.2. Análisis del riesgo. 32
5.3.1.3. Valoración del riesgo. 35
5.3.1.4. Calificación general residual. 38
5.3.1.5. Envío de riesgo. 39
5.3.2. Generación versión del riesgo 39
5.3.3. Comunicación y consulta. 40
5.4. REVISIÓN, MODIFICACIÓN, CREACIÓN Y ACTUALIZACIÓN DE CAMPOS EN ISOLUCIÓN® 42
5.4.1. Creación de listados en la plataforma 42
5.4.2. Parametrización del módulo 42
5.5. CARGUE DE INFORMACIÓN EN ISOLUCIÓN® 43
5.5.1. REGISTRO DE RIESGOS 43
5.6. PROGRAMA DE CAPACITACIÓN DEL MÓDULO ISOLUCIÓN® PARA LA GESTIÓN DE RIESGO 45

5.7. SOCIALIZACIÓN DEL PROYECTO DE GRADO Y ENTREGABLES 45
6. PROPUESTA DE MEJORAMIENTO 46
7. APORTES DEL ESTUDIANTE 48
8. CONCLUSIONES 50
9. RECOMENDACIONES 52
10. BIBLIOGRAFÍA 54
ANEXOS 55

Listado de tablas

Tabla 1. Tiempo de ejecución planes de acción. 23
Tabla 2. Probabilidad de ocurrencia. 33
Tabla 3. Calificación de acuerdo con la confidencialidad, integridad y disponibilidad. 34
Tabla 4. Clasificación de los controles. 36
Tabla 5. Naturaleza del control. 37
Tabla 6. Ejecución del control. 38

Listado de figuras

Figura 1. Logotipo OneLink. 12
Figura 2. Componentes marco de referencia. 17
Figura 3. Proceso para la gestión o administración de riesgo. 18
Figura 5. Gobierno de Riesgo OneLink. 20
Figura 6. Flujo de comunicación de riesgos OneLink. 41

Listado de anexos

Anexo 1. Valores corporativos de OneLink. 55
Anexo 2. Gestión de prevención de fraude en OneLink. 55

Anexo 3. Estructura organizacional del área gestión de riesgos y continuidad. 56
Anexo 4. Mapa de procesos de OneLink. 57
Anexo 5. Mapa de subprocesos del proceso Gestión de gobierno, riesgo y cumplimiento. 58
Anexo 6. Establecimiento del contexto interno, externo y contexto del proceso. 59
Anexo 7. Riesgos cargados en ISOlución®. 60
Anexo 8. Fase de identificación en ISOlución®. 61
Anexo 9. Nombre del riesgo. 62
Anexo 10. Listado de procesos. 68
Anexo 11. Listado de subprocesos. 69
Anexo 12. Listado de servicios. 70
Anexo 13. Fase de Análisis del riesgo en ISOlución®. 77
Anexo 14. Fase de valoración del riesgo en ISOlución®. 78
Anexo 15. Calificación general residual en ISOlución®. 80
Anexo 16. Envío y revisión de los riesgos en ISOlución®. 81
Anexo 17. Ficha del riesgo. 82
Anexo 18. Generación de versión del riesgo en ISOlución®. 85
Anexo 19. Fase identificación ISOlución® enfocado a seguridad de la información. 86
Anexo 20. Fase de identificación ISOlución® enfocado a riesgo Saro. 87
Anexo 21. Ejemplo de agendamiento de reuniones. 88
Anexo 22. Envío de riesgos. 89
Anexo 23. Riesgos por proceso, subproceso y área. 90
Anexo 24. Certificado del curso Seguridad Corporativa Básico. 91
Anexo 25. Evidencia de socialización proyecto de grado. 92
Anexo 26. Acta de socialización proyecto de grado. 93
Anexo 27. Ejemplo riesgo en Excel. 94
Anexo 28. Instructivo matriz de riesgo en Excel. 97
Anexo 29. Matriz de riesgo en ISOlución®. 100

1. INTRODUCCIÓN

El presente documento se refiere al informe final de práctica profesional como opción de grado para el título de Ingeniero Industrial, donde se implementa la plataforma ISOlución® para la sistematización y estandarización de la gestión de los riesgos asociados a la compañía y los clientes; apoyándose en el uso del software Excel para la recolección de la información de los riesgos.

El proyecto se lleva a cabo en la empresa OneLink Colombia S.A.S. que brinda los servicios de atención al cliente al diseñar y mejor las indagaciones sobre productos y servicios, resolución de quejas y encuestas de retroalimentación de los consumidores; soporte técnico en los canales preferidos por consumidores sin importar si es por voz, chat, email, SMS, dentro de una aplicación o por redes sociales; ventas y retención siendo aliados estratégicos los clientes, trabajan para mejorar y aumentar las tasas de conversión, así como para ampliar y cruzar las impulsando ingresos adicionales; back office para dar soluciones tecnológicas como humanas que mejoren los procesos, transar más rápido, reducir costos, mejorar la experiencia de atención y proteger tu marca; moderación de contenido para gestionar contactos directos e indirectos con los consumidores mejorando la integridad de la marca y experiencia del usuario generando alertas sobre consumidores con comportamientos repetitivos en lo referente a contenido no autorizado; y finalmente, ofrece servicios de redes sociales para conectar las marca con los consumidores a través de los canales de redes sociales, añadiendo valor, relaciones con los consumidores, lealtad de consumidor y fidelidad de marca.

Se tiene como guía la Norma Técnica Colombiana ISO 31000 (2018) que establece las directrices genéricas que permiten lograr una gestión de riesgo eficaz a través de la definición de un número de principios necesarios para alcanzar el objetivo dado haciendo primordial trazar una arquitectura que conlleve esos principios, el marco y los procesos contemplados en la norma. Además, también la ISO 27001 (2013) nos sirve de maestra para gestionar la seguridad de la información preservando la integridad, la disponibilidad

y la confidencialidad de la información, pilares sumamente importantes para la compañía y el cumplimento a la norma PCI DSS (Payment Card Industry Data Security Standard o Estándar de seguridad de datos de la industria de tarjetas de pago).

Primeramente, se parte de la conceptualización clave para llevar a cabo la gestión de los riesgos. De esta manera se inicia con la estandarización de la información que contaba la empresa. Posteriormente se crea la plantilla en Excel que cumpla con los requisitos, metodología y campos que nos suministra la plataforma ISOlución® donde será migrada la información; teniendo en cuenta cómo debe redactarse el riesgo y hacer uso de la mayor cantidad de información estandarizada como son las causas, consecuencias, factores, controles para el tratamiento del riesgo, entre otros.

Al tener esta plantilla inicia el proceso de aprendizaje y preparación para saber cómo llevar a cabo esa recolección de información de forma correcta, apuntando siempre a cumplir con los principios establecidos para la gestión de riesgo, es decir, se hace un estudio de qué trata cada interrogante dispuesto en ISOlución® y como debe ser abordado creando unas instrucciones o metodología. De este modo, se inicia la fase de recolección de información con cada dueño de los procesos, subprocesos y/o áreas de la compañía, validando y completando la información que se tiene de sus riesgos o llevando a cabo un levantamiento de riesgos desde la etapa cero, enfocado siempre a las necesidades de la compañía y su política de riesgos. Simultáneamente se da el proceso de adecuación de la plataforma llevando a cabo la verificación y cargue de los parámetros, listas o cualquier información solicitada por el módulo en ISOlución®. Los errores o inconsistencias encontradas al momento de hacer el cargue de los riesgos se notifican al área responsable para su corrección.

Finalmente, se realiza una guía escrita y audiovisual que sirvan de instructivo para el módulo de riesgos en ISOlución® donde se explica la gestión de los riesgos en la plataforma y la metodología usada.

2. PLATAFORMA ESTRATÉGICA DE LA EMPRESA

2.1. RESEÑA HISTÓRICA

Los orígenes de OneLink se remontan a mediados de los noventa cuando una compañía llamada Transantel se fundó como el primer proveedor de servicio de su tipo en Guatemala. En el 2013 se completa la transición de OneLink abriendo operaciones en El Salvador y Colombia. Luego, un año más tarde se estableció como proveedor de servicios de Centro de Contacto y BPO con oficinas en El Salvador, Guatemala, Colombia y Nicaragua. Luego, en el 2015 expande sus instalaciones en El Salvador y diversifica su portafolio de servicios al adquirir un proveedor de servicios financieros y contables.

En el 2016 se abren nuevos Sites en Guatemala, Nicaragua y Colombia y para el 2017. Durante el 2018 OneLink expande sus operaciones a nuevas geografías al abrir oficinas en Obregón, México. En Bogotá, se adquirió un nuevo centro de Operaciones: CANAPRO.

En 2019, se le dio bienvenida a GigaMonster, Rappi y Colmédica como socios de negocios, y se amplió la capacidad de operación en Bogotá con dos nuevos edificios con 10.000 Increybles®.

2.2. ¿QUIÉNES SOMOS?

Somos un Contact Center que brinda soluciones innovadoras y a la medida para cada uno de nuestros clientes. Estamos ubicados en El Salvador, Guatemala, Colombia, Nicaragua, México y Brasil. Nos hemos denominado “The Contact Center with a Smile” ya que velamos por la plenitud de nuestros trabajadores y que le sonrían a la vida.

2.3. LOGOTIPO

Figura 1. Logotipo OneLink.
Tomada de: OneLink, 2021.

2.4. UBICACIÓN SEDE AVENTURA

Dirección: Carrera 52 # 65 - 86, Centro Comercial Aventura, Medellín, Antioquia.

2.5. PROPÓSITO

Revolucionar la industria de BPO (Business process outsourcing) a través de la innovación, el espíritu emprendedor y la cultura de la felicidad. Generando valor para nuestros asociados, clientes y nuestra comunidad.

2.6. VALORES CORPORATIVOS

Consideramos que la ecuación perfecta es: Liderazgo, excelencia, innovación, felicidad, compromiso y solidaridad (ver Anexo 1. Valores corporativos de OneLink).

2.7. POLÍTICAS CORPORATIVAS

- **Política de privacidad y protección de datos personales**

Comunicar a los usuarios, clientes, proveedores, empleados y postulantes titulares de la información personal, el tipo de datos, las finalidades del tratamiento para hacer posible la prestación de nuestro servicio, la protección y los derechos que le asisten como titular de la información y los procedimientos para ejercerlos.

- **Política de seguridad de la información**

OneLink reconociendo la importancia de la seguridad, privacidad y confidencialidad de la información personal que los usuarios, clientes, proveedores, empleados y postulantes suministran a nuestras Compañías a través de los diversos canales habilitados (incluyendo sitios web, aplicaciones, documentos físicos entre otros), nos comprometemos con la protección y tratamiento adecuado de los mismos datos, conforme al régimen legal de protección de datos personales aplicable a cada territorio donde operemos (ver Anexo 2. Gestión de prevención de fraude en OneLink).

- **Política de piso operativo**

En OneLink nos encanta velar por la seguridad de nuestro Increybles® y de la operación, por lo cual, se establecieron reglas para ingresar a las áreas operativas de la compañía como:

- **Kit de identificación:** Utilízalo siempre en lugar visible.
- **Bloquea tu computador:** Garantiza la información de nuestros clientes, bloqueando tu computadora al levantarte de tu puesto.
- **No compartas tu contraseña:** No compartas tu usuario ni contraseña de acceso al sistema con nadie, tampoco los dejes al descubierto.
- **Guarda tu celular:** Guarda en el casillero tu celular, cámara o cualquier dispositivo que capture información.
- **Usa siempre los casilleros:** Antes de ingresar al piso de operaciones guarda todas tus pertenencias en los casilleros (loncheras, billeteras, mochilas, etc.)
- **Informa irregularidades:** Cualquier actividad sospechosa o funcionamiento irregular en tu equipo, informarlo al área de seguridad de la información.

2.8. DESCRIPCIÓN DEL ÁREA DE TRABAJO

De acuerdo con el organigrama de la estructura del área de gestión de riesgos y continuidad de negocio (ver Anexo 3. Estructura organizacional del área gestión de riesgos y continuidad de negocio), el proceso es encabezado por el director de seguridad corporativa que es dirigido por el Ingeniero Fernando Moreno Álvarez y se encarga de establecer los lineamientos para el manejo de activos de información.

El subproceso de Gestión de Continuidad se enmarca en el proceso de Gestión de Gobierno, Riesgo y Cumplimiento (ver Anexo 4. Mapa de procesos de OneLink) que tiene además los subprocesos de Gestión de Seguridad de la Información, Gestión de Continuidad, Gestión de Prevención de Fraude, Gestión de Seguridad Física, Gestión de Cumplimiento, Gestión Integral de Procesos y Gestión de Seguridad de la Información (ver Anexo 5. Mapa de subprocesos del proceso Gestión de gobierno, riesgo y cumplimiento). Por otro lado, la empresa definió al subproceso de Gestión de Riesgo dentro de la Gestión Integral de Procesos, pero responden a la misma dirección, es decir, al director de seguridad corporativa incluyendo al subproceso de Gestión de Continuidad de negocio. En este sentido, desempeño mi rol de practicante en el área de Gestión del Riesgo y Continuidad de Negocio abarcando los dos subprocesos y respondiendo al Coordinador de Gestión de Riesgo y Continuidad de Negocio.

Primeramente, en el área de continuidad de negocio se hacen los procesos de realización del análisis BIA (Análisis de impacto al negocio), generación de programas de sensibilización, capacitación y entrenamiento para todos los colaboradores de la Organización, diseño de los planes BCP (Plan de continuidad de negocio) y DRP (Plan de Recuperación de Desastres) para las cuentas críticas, subprocesos y unidades de negocio ante la no disponibilidad de los servicios y operaciones, planeación y ejecución de ejercicios controlados de continuidad de negocio que permitan verificar la funcionalidad de los planes BCP (Plan de continuidad de negocio) y DRP (Plan de Recuperación de

Desastres) y la implementación de estos planes para las cuentas críticas, subprocesos y unidades de negocio ante la no disponibilidad de los servicios y operaciones.

Por otro lado, el área de gestión del riesgo se encarga de la planificación, integración e implementación de acciones para abordar riesgos dentro de los procesos pertenecientes al Sistema de Gestión, ejerciendo control en procura de la eficacia y mejora de estos. Derivando de allí la aplicación sistemática de las políticas, procedimientos y prácticas a las actividades de la comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. Además, el área al abarcar de forma transversal cada uno de los procesos sirve de apoyo para toda la compañía y de ayuda para diferentes actividades, principalmente con el subproceso de seguridad de la información que guarda estrecha relación debido a que está inmerso el módulo de Gestión de Activos de Información con el módulo de Riesgo SARO, el cual, vela por el cumplimiento de los tres pilares de información que son la disponibilidad, integridad y confidencialidad. De esta manera existe una gran sinergia entre los subprocesos, por ejemplo, para abordar un riesgo y subirlo a la plataforma ISOlución® es necesario que previamente se tengan los activos relacionados a estos ya definidos en el módulo de Activos.

El compromiso del área es vital para la compañía y cada uno de los subprocesos, debido a que se debe trabajar en conjunto para lograr una buena gestión de riesgos que evite la realización de eventos que perjudiquen la operatividad y/o prestación de servicios de OneLink.

3. MARCO TEÓRICO O CONCEPTUAL

3.1. GESTIÓN DEL RIESGO

Según la Norma Técnica Colombiana ISO 31000 (2018) la gestión o administración de riesgo hace referencia a las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Así mismo, se debe tener en cuenta las siguientes definiciones y/o conceptos:

- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Entendiéndose que la incertidumbre es el estado de falta de información asociada al conocimiento o entendimiento de un evento, su consecuencia o probabilidad.
- **Evento:** Ocurrencia o cambio de un conjunto particular de consecuencias. Donde un evento podrá tener una o varias consecuencias y causas. Además, este puede convertirse en una fuente de riesgo.
- **Consecuencia:** Resultado de un evento que afecta los objetivos. Además, esta podrá ser cierta o incierta y generar efectos positivos o negativos afectando directa o indirectamente los objetivos.
- **Probabilidad:** Posibilidad de que algo suceda. Puede describirse de forma objetiva o subjetiva, cualitativa o cuantitativa y en términos generales o matemáticos.
- **Control:** Medida que mantiene y/o modifica un riesgo. Es importante saber que este no siempre produce el efecto de modificación hacia el riesgo que se prevé.

Para lograr una adecuada gestión o administración de riesgo se debe tener:

- **Marco de referencia para la gestión del riesgo:** Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de toda la organización. Los componentes de este marco de referencia se muestran a continuación:

Figura 2. Componentes marco de referencia.
Tomada de: (ISO 31000, 2018)

- **Política para la gestión del riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

- **CIA:** Confidencialidad, integridad, disponibilidad. Se refieren a los principios básicos de la seguridad de la información (ISO 27001, 2013).

3.1.1. Fases para la gestión o administración de riesgo

Teniendo como referente la Norma Técnica Colombiana (ISO 31000, 2018) el proceso de la gestión o administración de riesgo debe tener una aplicación de forma sistemática de diferentes fases (ver Figura 3. Proceso para la gestión o administración de riesgo) teniendo en cuenta las políticas, procedimientos, actividades, y el contexto interno y externo de la organización.

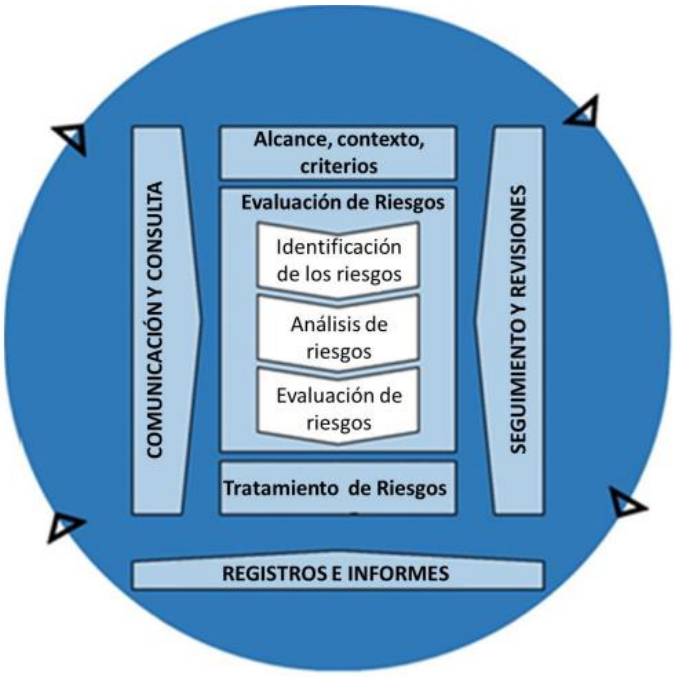


Figura 3. Proceso para la gestión o administración de riesgo.
Tomada de: (ISO 31000, 2018).

3.2. GOBIERNO DE GESTIÓN DEL RIESGO EN ONELINK

El gobierno de gestión del riesgo establecido en el manual de Gestión de Riesgos y Oportunidades Corporativo de la compañía se basa en el modelo de las tres líneas de defensa, el cual, fue adaptado de la declaración de posición del IIA sobre las tres líneas de defensa en gestión de riesgos y control eficaces.

Este modelo ayuda en el objetivo de garantizar la efectividad del marco de gestión de riesgos de la organización, donde la alta dirección se debe apoyar adecuadamente en las líneas de funciones dentro de la organización. Además, pretende ser un modo de explicar la relación entre las funciones y como una guía de cómo las responsabilidades deben ser divididas.

- **Primera línea de defensa:** Esta línea es la propietaria de los riesgos operativos y por lo mismo la responsable de implementar acciones correctivas para abordar el proceso y las deficiencias de control. La gestión operativa se encarga del mantenimiento efectivo de los controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. La gestión operativa de los riesgos identifica, evalúa, controla y mitiga los riesgos, orienta el desarrollo e implementación de políticas y procedimientos internos y asegura que las actividades sean compatibles con las metas y objetivos.

- **Segunda línea de defensa:** Esta línea de defensa monitorea los riesgos y los controles que soportan el manejo de las funciones de las unidades o procesos de negocio. Su función es la de supervisar la implementación de prácticas de gestión de riesgo eficaces por parte de la primera línea de defensa, y recomendar a los responsables de los riesgos sobre la implementación de controles y prácticas que permitan tratar el riesgo.

- **Tercera línea de defensa (auditoría interna):** Tiene como misión proveer aseguramiento independiente al C-level con respecto a la efectividad del manejo de los riesgos y controles. La función de la auditoría, a través de un enfoque basado en el riesgo, proporcionará aseguramiento sobre la eficacia del gobierno, gestión de riesgos y control interno al C-level de la organización, incluidas las maneras en que funciona la primera y segunda línea de defensa.

Cada vez que la primera línea de defensa identifique un nuevo riesgo, causas, la materialización del riesgo o una oportunidad, el dueño del proceso o cualquiera que éste delegue debe reportar al área de Gestión de Riesgos para actualizar la matriz de riesgos y proceder con el acompañamiento para la implementación de un Plan de Acción.

Figura 4. Gobierno de Riesgo OneLink.
Tomada de: Curso Gobierno de Riesgo OneLink, 2021.

3.3. ISOLUCIÓN®

ISOlución®, es una herramienta integral paga que se encuentra en la nube y tiene acceso web, esta facilita la planeación, la implantación, la administración, el mantenimiento y mejoramiento del Sistema de Gestión de la Organización. Además, permite la administración ágil y eficaz de los Sistemas de Gestión como ISO 9001, SG-SST, ISO 45001, control de la bioseguridad, HSEQ, Gestión de Riesgos, Continuidad de Negocio, MIPG, SARLAFT y SAGRILAFT, ISO 27001, y el cumplimiento normativo de su organización. Bajo esta perspectiva, es una herramienta participativa, dinámica e interactiva, proporcionando un manejo al 100% del sistema de gestión de la organización generando eficiencia de gestión documental; seguimiento de acciones correctivas y preventivas, mejoramiento continuo de los procesos, auditorías internas de calidad, manejo de indicadores de gestión y por supuesto comunicación constante entre los usuarios de la empresa.

4. DIAGNÓSTICO ESPECÍFICO DE LA EMPRESA

OneLink en cumplimiento de las normas ISO aplicables a la gestión de riesgos lleva a cabo su implementación según lo estipulado en las normativas. Por consiguiente, todo el proceso comprende: la comunicación y consulta, establecimiento del contexto, valoración del riesgo y tratamiento del riesgo, monitoreo y revisión, y registro del proceso para la gestión del riesgo (ISO 31000, 2013). A continuación, se describe de forma general en qué consiste cada una dentro de la compañía actualmente.

4.1. METODOLOGÍA PARA GESTIONAR LOS RIESGOS SARO Y SI

OneLink planifica, integra e implementa acciones para abordar riesgos dentro de los procesos pertenecientes al Sistema de Gestión, ejerciendo control en procura de la eficacia y mejora de estos. De esta manera el proceso de gestión del riesgo implica la aplicación sistemática de las políticas, procedimientos y prácticas a las actividades de la comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.

Cabe resaltar que las acciones tomadas para abordar los riesgos deben ser consecuentes al impacto potencial en la no conformidad de los servicios prestados, teniendo en cuenta esta metodología para su identificación y tratamiento. En consecuencia, conocer en detalle las posibles consecuencias negativas (riesgo) y sus impactos potenciales. A continuación, se explica cada etapa brevemente teniendo como guía la ISO 31000 (2013).

- **Comunicación y consulta:** Tiene como propósito asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas.

- **Establecimiento del contexto:** Hace referencia al conocimiento de las entradas y salidas de un proceso, conocer sus interacciones y de esta forma los involucrados en la

ejecución de actividades (ver Anexo 6. Establecimiento del contexto interno, externo y contexto del proceso).

- **Evaluación del riesgo:** En este se llevaban a cabo las etapas de identificación, análisis y evaluación del riesgo. Por consiguiente, consiste en comparar todos los resultados obtenidos con los criterios definidos por la compañía y de esta forma conocer la magnitud de los riesgos de acuerdo con los niveles previamente definidos, por ejemplo, en esta fase se validan los impactos de la organización en términos económicos basados en una probabilidad de impacto, para poder evaluar la gestión de riesgos en conjunto con el área estratégica que define los niveles y calificación que se le puedan dar a cada nivel.

- **Tratamiento del riesgo:** Aquí se tiene la primera línea de defensa como se muestra en la sección 3 de este informe – "Figura 5. Gobierno de Riesgo OneLink", la cual, es responsable de identificar, establecer y ejecutar los controles o planes de acción que ayudarán a mitigar la probabilidad e impacto de las causas que generen el riesgo.

- **Monitoreo y revisión:** En esta fase interviene la segunda línea de defensa para realizar el monitoreo en cuanto al cumplimiento de la metodología de riesgos definida, asesoría y acompañamiento a la primera línea de defensa, la tercera línea de defensa es la encargada de validar o revisar la aplicabilidad de los controles y planes de acción definidos por la primera línea de defensa y de validar el acompañamiento de la segunda línea de defensa, tal como se muestra en la sección 3 de este informe – "Figura 5. Gobierno de Riesgo OneLink". Teniendo en cuenta lo anterior cuando los riesgos son identificados por el proceso de Gestión de Riesgos, se solicita al dueño de cuenta y/o proceso dar a conocer los planes de acción y/o controles que mitigan el riesgo en un plazo de 5 días hábiles a partir de la fecha de socialización, mismo tiempo que se solicitará al cliente o proveedor establecer sus planes de acción o aceptación del riesgo en caso de no aplicar ningún control.

Dependiendo la valoración del riesgo (crítico, alto, medio o bajo) los tiempos de implementación y ejecución de los planes de acción serán acorde a los establecidos, conforme a la metodología de riesgos en OneLink.

Tabla 1. Tiempo de ejecución planes de acción.

Riesgo	Tiempo de ejecución
Bajo	En seguimiento
Medio	Entre 3 a 6 meses
Alto	Inmediato a 6 meses
Crítico	Inmediato a 1 mes máximo

Tomada de: Gestión de riesgos OneLink, 2021.

Posteriormente, toda esa gestión documental se almacena en SharePoint de Office 365. De esta forma se requiere de la realización de procedimientos manuales como la gestión de correos, permisos de acceso, comunicados y deficiente control hacia los tres pilares de la información que son la confidencialidad, la disponibilidad y la integridad (ISO 27001, 2013). Además, genera una centralización de la información teniendo en cuenta que se tiene presencia en diferentes países y la gestión de riesgos debe ser a nivel transversal en todas las sedes de la compañía, es decir, esta debe ser manejada y difundida de forma íntegra a todos los actores que la requieran.

Con relación a la problemática expuesta el uso de esas herramientas limita el acceso a la información y control de ella, es por ello la deficiencia de sinergias entre áreas al momento de la toma de decisiones basadas en la documentación manejada por cada una. Esta modalidad de documentación ocasiona alta dependencia hacia los creadores de ella, no permite una correcta asignación de custodios, usuarios permitidos y divulgación; por consiguiente, se observan retrasos en los canales de comunicación y dificultades en la ejecución de procedimientos en general.

Por otra parte, no se está haciendo parte a los dueños de los procesos de toda la información relacionado con ellos debido a que la gestión de los riesgos es llevada a cabo en todas las líneas de defensa por el área de Gestión de Riesgo impidiendo principalmente

que estos no sean levantados de forma objetiva por cada dueño de proceso, quienes son los que conocen sus riesgos y todo lo que implica de ellos. Además, con esta metodología no pueden conocer las actualizaciones en tiempo real, estado de los procesos, porcentaje de cumplimiento, mediciones e indicadores, en general todo el acceso a ella. Por ejemplo, la matriz de riesgos es un único documento donde se consolidan todos los riesgos de la compañía, con un alto valor de confidencialidad y necesario para la toma de decisiones en los diferentes procesos de OneLink; su elaboración recae en el área de Gestión de Riesgos pero cada dueño de proceso debe conocer la información descrita y asociada a sus riesgos de acuerdo con la información suministrada por ellos y/o analizada por el área directamente, es decir, estos deben conocer, entender y socializar la matriz a los actores necesarios concerniente a su proceso.

Finalmente, con la metodología para la gestión del riesgo aplicada actualmente (ver Anexo digital 1. Metodología de riesgos antigua) no se hace una valoración del riesgo rigurosa que permitiese controlar las causas dispuestas en cada uno de los riesgos sino que por el contrario se establece un control general sin especificar evidencias, responsable del control, tipo de control, ejecución del control, documentación que soportaban el control y también pueden definirse controles que no dependan del área sino de un tercero haciendo difícil el lograr tener una responsabilidad para su ejecución que evite la materialización del riesgo. Igualmente se establecen campos que son netamente subjetivos y no responden como resultado de cálculos siendo incoherentes en muchas ocasiones a la información descrita.

Es por esta razón que como respuesta a lo anterior y para una mejora continua de su gestión se plantea el uso de la plataforma ISOlución® (software de proveedor externo) como reemplazo a plantillas en Excel para lograr una sistematización y estandarización de los procesos llevados en el área permitiendo un sistema eficaz de gestión del riesgo que cree ventajas para la compañía. Se tienen como objetivos para el desarrollo del proyecto los siguientes:

4.2. OBJETIVOS

4.2.1. Objetivo general

Implementar la plataforma ISOlución® para la sistematización y estandarización de la gestión de riesgo generando un sistema eficaz que permita la supervisión, el monitoreo y el acceso a la información entre usuarios de la compañía velando por el cumplimiento de los tres pilares de la información.

4.2.2. Objetivos específicos

- Estandarizar la información de la gestión de riesgos contemplada en la matriz de riesgo actual.

- Realizar la recolección, análisis y definición de información necesaria para culminar la matriz de riesgos.

- Desarrollar las fases de identificación, análisis y valoración que no se encuentran definidas en la matriz de riesgos para cada uno de los procesos de la compañía obteniendo un consolidado que relacione toda la información.

- Revisar, modificar y actualizar la información en los campos requeridos por ISOlución®.

- Migrar la información recolectada en la matriz de riesgos en Excel a la plataforma ISOlución®.

- Desarrollar un programa de capacitación para el manejo de la plataforma ISOlución® en la gestión de riesgo con sesiones en vivo, creación de instructivo del manejo de módulo de riesgos y actualización del procedimiento sobre gestión de riesgos.

5. ACTIVIDADES DESARROLLADAS

5.1. ESTANDARIZACIÓN Y ADECUACION DE LA INFORMACIÓN

Se llevó a cabo inicialmente una revisión de los riesgos que contaba el área donde se validó ortografía, redacción y metodología, esta última hace referencia a que el nombre del riesgo cumpliera con las características definidas en la nueva metodología.

Seguidamente se estandarizaron las causas (ver Anexo digital 2. Listado de causas) conforme a unas categorías y se sacó un listado de consecuencias (ver Anexo digital 3. Listado de consecuencias) con el fin de homologar causas y consecuencias que estuvieran enfocadas al mismo tema. Sin embargo, este fue un primer listado base que se cargó a ISOlución® y a medida que se iban registrando los riesgos se agregan aquellos ítems que fueran necesarios en los listados.

5.1.1. Diseño de plantilla para registro de los riesgos en Excel

Con el fin de llevar a cabo un levantamiento de información coherente y conforme a los campos requeridos con la nueva metodología establecida en la plataforma ISOlución® se diseñó y creó una plantilla en Excel para usarla en cada sesión e ir consolidando la información (ver Anexo digital 4. Plantilla de riesgos).

Por otra parte, el proceso de levantamiento de información no se llevó a cabo directamente en la plataforma debido a la dependencia con el módulo de activos de información que se creó en paralelo con el módulo de riesgos. Por tal motivo, se decidió trabajar en la plantilla y posteriormente hacer el cargue de información a ISOlución®.

5.1.2. Borrado de registros corruptos en el módulo de riesgos (producción)

Se llevó a cabo una depuración de los riesgos de prueba que se habían subido anteriormente por parte del equipo de riesgos para validar la funcionalidad de la plataforma.

Por consecuente, se partió desde cero para la gestión de los riesgos en ISOlución® donde aparece como responsable mi persona debido a que lleve a cabo la gestión de todos los riesgos (ver Anexo 7. Riesgos cargados en ISOlución®).

5.2. RECOLECCIÓN Y ANÁLISIS DE INFORMACIÓN

5.2.1. Levantamiento de información con dueños de proceso, subproceso o área

El levantamiento de información se llevó a cabo a través de reuniones virtuales por Microsoft Teams con cada uno de los dueños relacionados a los riesgos, donde inicialmente se hizo la homologación de campos de la matriz de riesgos versión 4 (ver Anexo digital 1. Metodología de riesgos antigua) para cada uno de los riesgos de los procesos con la nueva matriz. También se hizo el traslado de información para la plantilla de riesgos nueva (ver Anexo digital 4. Plantilla de riesgos). Esta nueva metodología logró satisfacer la valoración del riesgo debido a que no se tenía información detallada de los controles porque anteriormente estos se establecen de forma general para todo el riesgo y ahora es necesario establecer mínimo un control por causa que mitigue o elimine esta de forma directa evitando la materialización del riesgo.

5.3. DEFINICIÓN DE METODOLOGÍA PARA LA GESTIÓN DE LOS RIESGOS

5.3.1. Fases para la gestión del riesgo

5.3.1.1. Identificación.

En esta fase se dio la identificación y definición de sucesos o eventos que se pueden presentar o producir en la organización, los cuales no pueden ser controlados. Fue ejecutada en compañía la mayoría de las veces por un miembro del equipo y cada líder de proceso en conjunto, identificando los riesgos potenciales o materializados que pudieran impactar la operación. Se analizaron los objetivos de negocio que se pudieran ver impactados en caso de materializarse un riesgo, basados en las debilidades y amenazas a las que se enfrentaba la compañía en caso de los riesgos asociados a los procesos de esta

o los riesgos de las cuentas que corresponde a los clientes de OneLink como Claro, Avianca, Rappi, etcétera.

Para identificar el riesgo fue importante realizar las siguientes actividades:

- **Entendimiento de los objetivos de la organización y de sus procesos**: La organización cuenta con los objetivos estratégicos que van relacionados con su misión y visión, así mismo cada objetivo de sus procesos deben estar alineados para poder ser cumplidos, es decir, los riesgos debían ser eventos que impidan o retrasen el cumplimiento de dichos objetivos. Como resultado la identificación del riesgo inicia con el entendimiento de los objetivos de la organización y/o de sus procesos.

- **Identificación de activos de información:** Esta actividad fue responsabilidad de la primera línea de defensa. Por consiguiente, la identificación de los riesgos depende directamente de la identificación de activos por parte del área de Seguridad de la Información siendo necesarias la creación de sinergias entre el área para poder avanzar en el proceso mutuamente y así lograr relacionar los activos identificados con cada uno de los riesgos y garantizar la confidencialidad, disponibilidad e integridad de la información.

- **Estructura o redacción de un riesgo:** La estructura general para la redacción de los riesgos es la siguiente: sustantivo + verbo en participio + adjetivo, adverbio o complemento circunstancial negativo (INEE, 2014). Este no debe mencionar causas, consecuencias, activos de información o cualquier otra información que no estuviese enfocado directamente a lo que no se puede controlar.

5.3.1.1.1. *Parametrización fase de identificación.*

La fase de identificación permite la creación de riesgos y se tiene los siguientes campos de acuerdo con ISOlución® (ver Anexo 8. Fase de identificación en ISOlución®).

- **Riesgo:** En este se escoge el nombre del riesgo o se crea un registro en caso de no encontrarse en los ya registrados. Para este campo se fue creando una lista a medida que iba haciendo los registros de los riesgos y se cargó el listado mostrando en (ver Anexo 9. Nombre del riesgo.).

- **Fecha de creación:** Es otorgado por la plataforma de acuerdo con la fecha del registro del riesgo.

- **Fecha del riesgo:** Corresponde a la definición de la fecha en la cual se identificó el riesgo en la organización inicialmente y solo cambia cada que se hace un nuevo registro, es decir, en caso de modificaciones seguirá la misma fecha inicial.

- **Responsable:** Muestra el nombre del usuario responsable de llevar a cabo la identificación del riesgo.

- **Activo:** Casilla de verificación para activar o inactivar un riesgo.

- **Proceso**: Opción de buscar riesgos identificados según el proceso al que pertenece el riesgo y se cargó a la plataforma el listado conforme a la división organizacional de la empresa (ver Anexo 10. Listado de procesos).

- **Subproceso:** Opción de buscar riesgos identificados según el subproceso al que pertenece el riesgo y se cargó a la plataforma el listado conforme a la división organizacional de la empresa (ver Anexo 11. Listado de subprocesos).

- **Objetivo**: Buscador para seleccionar el objetivo del proceso seleccionado anteriormente y este fue suministrado por parte del equipo de Gestión Integral de Procesos. Sin embargo, a lo largo del proyecto se fueron solicitando las modificaciones necesarias al equipo para los subprocesos que aún no contaban con objetivo impidiendo el cargue de información.

- **Servicio**: En caso de que los riesgos estén asociado a una cuenta (clientes externos) o área que ofrezca un servicio como podemos observar en el listado (ver Anexo 12. Listado de servicios) deberá escogerse una o varias opciones. Este listado fue suministrado al equipo de Gestión Integral de Proceso conforme a lo que se iba encontrando en los riesgos, es decir, se fue solicitando agregar más ítems a lo largo del proceso y se hizo una depuración de los servicios que ya no se ofrecían.

- **Área**: De acuerdo con la división organizacional estaba definido previamente unas áreas las cuales no pueden ser modificadas a menos que exista un cambio en la estructura organizacional. Por consiguiente, este listado ya estaba definido inicialmente y no fue modificado.

- **Causa**: Corresponde al ¿cómo puede suceder? Estas fueron identificadas inicialmente al momento de estandarizar las causas que se tenían en los riesgos gestionados previos a la realización del proyecto dividiéndose por categorías. Primeramente, se hizo el cargue de ese primer listado de causas y luego se fueron subiendo a medida que se iban encontrando más en el proceso de identificación del riesgo (ver Anexo digital 2. Listado de causas).

- **Site**: Referente a las sedes de la compañía en los diferentes países. Esta no fue modificada.

- **Factor del riesgo**: Es el elemento o conjunto de elementos que estando presentes en una actividad o proceso pueden desencadenar o disparar las causas que generan la materialización del riesgo. El listado fue realizado el año pasado por el equipo de riesgos, es decir, no fue modificado.

- **Consecuencias**: Corresponde a los efectos que podría tener el riesgo en caso de su materialización. Estas fueron identificadas inicialmente al momento de estandarizar las consecuencias que se tenían en los riesgos gestionados previos a la realización del

proyecto. Primeramente, se hizo el cargue de ese primer listado de consecuencias y luego se fueron subiendo a medida que se iban encontrando más en el proceso de identificación del riesgo (ver Anexo digital 3. Listado de consecuencias).

- **Cuenta**: Asociado a los clientes que tiene la compañía, por ejemplo, Avianca, Frito Lay, Claro, Rappi, entre otros. Este campo no fue modificado.

- **Tipo de riesgo**: Los tipos de riesgos son el conjunto de características que se evidencian en algún evento o situación que permiten ser enmarcados en un solo concepto. Este campo no fue modificado.

- **Afecta la continuidad del negocio**: Los riesgos identificados que tuviesen una alta probabilidad de generar una indisponibilidad de los servicios y de la operación se marcaron con un "Sí" indicando que deben generarse planes de acción para mitigar el impacto en caso de materialización o en caso contrario se marcó con un "No". Este campo no fue modificado.

- **Activos**: En este se hace referencia a todos los activos de información relacionados a los riesgos, es decir, aquellos que sufrirían un efecto en caso de materialización del riesgo. Inicialmente la identificación de los activos fue llevada a cabo por mi persona, pero luego fue delegada al equipo de Seguridad de la información.

Cabe resaltar que este campo nos generaba dependencia con el área debido a que si aún no se encontraban los activos asociados a los riesgos no se podía llevar a cabo la identificación de riesgo porque todos los campos son obligatorios. Por lo cual, el módulo de activos y módulo de riesgos debían tener sinergias y trabajar en conjunto.

- **Clasificación de la información**: Se refiere al tipo de información contenida en el activo de información e inicialmente estaba definida como pública, interna o confidencial pero debido a que no siempre se ve afectado un activo de información al

momento de materializarse el riesgo se solicitó al equipo de Gestión Integral de Proceso incluir el ítem "No aplica".

Nota: Cuando se solicita agregar un ítem a un listado a través del equipo de Gestión Integral de Procesos es debido a que hay tablas y/o campos que solo pueden ser modificados por un usuario administrador y requiere del envío de una solicitud. Además, aquellos campos que no fueron modificados debido a que estaban parametrizados previamente por el equipo de riesgos antes del desarrollo del proyecto.

5.3.1.2. Análisis del riesgo.

En esta fase se llevó a cabo la valoración y priorización de los riesgos donde se hizo la medición de probabilidad de ocurrencia de los riesgos y su impacto en caso de materializarse. La medición llevada a cabo fue de tipo cuantitativo y cualitativo.

En el análisis del riesgo se tuvo como objetivo determinar la probabilidad y el impacto, implicando una consideración detallada de las incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Además, considerando que un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos (ver Anexo 13. Fase de Análisis del riesgo en ISOlución®).

Se consideraron los siguientes campos:

- **La probabilidad:** Se entiende como la posibilidad de ocurrencia o materialización del riesgo (ver Tabla 3. Probabilidad de ocurrencia). Este campo no fue modificado.

Tabla 2. Probabilidad de ocurrencia.

PROBABILIDAD DE OCURRENCIA			
Ponderación	**Calificación**	**Definición**	
1	**Raro**	Una vez entre 2 y 4 años.	Probabilidad de ocurrencia del 10% sobre la vida del activo
2	**Improbable**	Una vez entre 1 y 2 años.	Probabilidad de ocurrencia entre el 10% y el 35% sobre la vida del activo
3	**Probable**	Una vez entre 6 meses y 1 año.	Probabilidad de ocurrencia entre el 35% y el 65% de la vida del activo
4	**Casi Seguro**	Hasta una vez entre 1 mes y 6 meses.	Probabilidad de ocurrencia mayor al 65% de la vida del activo

Tomada de: Manual de Gestión de Riesgos y Oportunidades Corporativo, 2021.

- **El impacto:** Se entiende como las pérdidas y/o consecuencias a los tres pilares de la información de acuerdo con la disponibilidad, integridad y confidencialidad (ver Tabla 3. Calificación de acuerdo con la confidencialidad, integridad y disponibilidad).

Tabla 3. Calificación de acuerdo con la confidencialidad, integridad y disponibilidad.

IMPACTO				
PONDERACIÓN	**TIPO**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**
1	**Baja**	En caso de materialización del riesgo la información puede ser revelada a cualquier individuo, entidad o proceso.	En caso de materialización del riesgo y que exista corruptibilidad del activo, los procesos o procedimientos no se afectan con el daño de este.	En caso de materialización del riesgo y que sufra daños el activo, los procesos dentro del alcance definido, no pueden ser interrumpidos por más de 24 horas.
2	**Media**	En caso de materialización del riesgo la información no es pública y sólo podrá estar disponible para un grupo de personas, entidades y procesos autorizados.	En caso de materialización del riesgo y que exista corruptibilidad del activo, los procesos o procedimientos pueden ser interrumpidos por un lapso de tiempo.	En caso de materialización del riesgo y que sufra daños el activo, los procesos dentro del alcance definido, no pueden ser interrumpidos por más de 8 horas.
3	**Alta**	En caso de materialización del riesgo la información solo se puede divulgar a un grupo privilegiado de personas, entidades y procesos autorizados.	En caso de materialización del riesgo y que exista corruptibilidad del activo, los procesos o procedimientos son interrumpidos de manera desastrosa.	En caso de materialización del riesgo y que sufra daños el activo, los procesos dentro del alcance definido, no pueden ser interrumpidos por más de 4 horas.
4	**Crítica**	En caso de materialización del riesgo la información solo se puede divulgar a un excepcional grupo de personas, entidades y procesos autorizados.	En caso de materialización del riesgo y que exista corruptibilidad del activo, los procesos o procedimientos son interrumpidos de manera inmediata y catastrófica.	En caso de materialización del riesgo y que sufra daños el activo, los procesos dentro del alcance definido, no pueden ser interrumpidos por más de 2 horas.

Tomada de: Elaboración propia, 2021.

En el caso de esta fase no se llevó a cabo ninguna modificación en cuanto a parametrización en ISOlución® y se trabajó con los parámetros que el equipo de riesgo había establecido previamente.

5.3.1.3. Valoración del riesgo.

En esta fase se identificaron cada uno de los controles que mitigan o eliminan las causas establecidas en la identificación del riesgo, los cuales debían relacionarse directamente con las causas (ver Anexo 14. Fase de valoración del riesgo en ISOlución®).

Inicialmente se contaba con una base de datos para los controles enfocados específicamente al SOA (declaración de aplicabilidad de controles y medidas de seguridad aplicadas en la organización) pero debido a que los controles establecidos solo se enfocan a la seguridad de la información (ver Anexo digital 5. Controles SOA) fue necesario establecer una nueva categoría de controles llamada control operativo (ver Anexo digital 6. Controles operativos) donde se refieren los controles directamente relacionados a los procedimientos del subproceso. De igual forma, se debe tener presente que en la empresa la mayoría de los subprocesos no cuentan con procedimientos definidos de acuerdo con las actividades realizadas. Teniendo en cuenta lo antes mencionado el objetivo de esta fase era determinar si las causas contaban con controles suficientes o si presentaban alguna deficiencia que potencializa la materialización del riesgo, para lo cual, se debía comprobar la existencia o no de controles y así describir los controles existentes.

Se consideraron los siguientes campos:

- **Controles existentes:** Se entiende como los controles que se están ejecutando actualmente para mitigar o eliminar las causas (ver Anexo digital 5. Controles SOA) y (ver Anexo digital 6. Controles operativos).

- **Responsabilidad del control:** Se entiende como la(s) persona(s) encargada(s) por velar el cumplimiento del control, pero en este se escoge el(los) cargo(s) de ese(os) responsable(s).

- **Tipo de control:** Se entiende como la evaluación de la acción y pueden ser de tipo preventivo, correctivo o detectivo (ver Tabla 4. Clasificación de los controles).

Tabla 4. Clasificación de los controles.

CLASIFICACIÓN DE CONTROLES	
TIPO	**DESCRIPCIÓN**
Preventivo	Permite anticiparse a la posibilidad de que se materialice el riesgo.
Detectivo	Se lleva a cabo en el momento de realizar las actividades e identifica las faltas u omisiones previo a la conclusión del proceso y permitiendo una anticipación a la materialización del riesgo.
Correctivo	Se da al final de proceso cuando el riesgo se ha materializado o es inminente su materialización, actuando directamente en la reducción del impacto y se complementan con los controles detectivos.

Tomada de: Elaboración propia, 2021.

- **Naturaleza del control:** Se entiende como el tipo de control de acuerdo con la forma en que es ejecutado, existen tres tipos que son automático, dependiente de IT y manual (ver Tabla 5. Naturaleza del control).

Tabla 5. Naturaleza del control.

NATURALEZA DEL CONTROL	
TIPO	**DESCRIPCIÓN**
Manual	Es ejecutado totalmente por una persona
Dependiente de TI	Es ejecutado por una persona, pero basado en la información generada por un sistema automatizado y/o el control requiere de una acción de inicio manual y un sistema lo ejecuta.
Automático	Cuando es llevado a cabo de forma automatizada sin ninguna intervención humana.

Tomado de: Elaboración propia, 2021.

- **Funcionalidad del control:** Se entiende en el cómo se encuentran en control actualmente, es decir, si se está llevando a cabo de forma adecuada o inadecuada.

- **Periodicidad:** Se entiende como la frecuencia con la cual se lleva a cabo el control que puede ser anual, bimestral, diario, mensual, semanal, semestral, quincenal, trimestral o cuando se requiera.

- **Documentación:** Se entiende como el soporte del control de acuerdo con la documentación que se encuentra dispuesta en la plataforma, es decir, solo puede estar documentando si ya existe un documento cargado en esta. Posteriormente, se selecciona esa referencia documental que se encuentra dentro de una lista desplegable otorgada por la plataforma.

- **Evidencia que compone el control:** Se entiende como aquel soporte que se tiene del control que soportan su ejecución, estas son necesarias para los procesos de auditorías y sirven de prueba acerca del control. Es importante tener en cuenta que las evidencias deben tenerse de acuerdo con la periodicidad establecida anteriormente y pueden ser adecuadas o inadecuadas.

- **Ejecución del control:** Se entiende como la aplicación del control en el subproceso y si este se lleva a cabo de forma fuerte, moderada o débil (ver Tabla 6. Ejecución del control).

Tabla 6. Ejecución del control.

EJECUCIÓN DEL CONTROL	
TIPO	**DESCRIPCIÓN**
Débil	No se ejecuta de forma correcta o no se está ejecutando.
Moderado	Se ejecuta de forma adecuada, pero existen aún fallas o debilidades en su ejecución.
Fuerte	Se debe ejecutar siempre y no existe margen de error.

Tomada de: Elaboración propia, 2021.

- **Importancia del control:** Se entiende como la valoración que se le da al riesgo conforme a su funcionalidad o utilidad, la cual puede ser muy importante, importante o poco importante. Sin embargo, por razones de parametrización se determinó la calificación importante para todos los controles que se definan en la compañía en la actualidad.

5.3.1.4. Calificación general residual.

- **Disminuye la probabilidad:** Se entiende como la calificación posterior a los controles que les da el dueño del proceso de forma subjetiva donde evalúa si después de la aplicación de controles la probabilidad de ocurrencia de este disminuye de forma débil, moderada o fuerte (ver Anexo 15. Calificación general residual en ISOlución®).

- **Disminuye el impacto**: Se entiende como la calificación posterior a los controles que les da el dueño del proceso de forma subjetiva donde evalúa si después del tratamiento del riesgo el impacto de este disminuye de forma débil, moderada o fuerte (ver Anexo 15. Calificación general residual en ISOlución®).

- **Acciones de mejora:** Aquí se establece el tratamiento del riesgo para aquellos riesgos que obtuvieron una calificación alta o crítica.

5.3.1.5. Envío de riesgo.

En esta fase se enviaron los riesgos a los responsables, es decir, los dueños de cada proceso relacionado al riesgo. Sin embargo, como se expresó inicialmente la metodología antes era trabajada únicamente por el equipo de riesgos, los cuales se encargaban de crear el riesgo y aprobarlos (ver Anexo 16. Envío y revisión de los riesgos en ISOlución®). Por consecuente, con el uso de la plataforma estos deberán ser revisados por los interesados o partícipes de estos, es así, que se solicita al equipo de Gestión Integral de Proceso la creación de un grupo de gestores de riesgo donde se incluya cada uno de los dueños de proceso para que sean ellos quienes verifiquen y aprueben o rechacen sus riesgos, estos visualizarán una ficha del riesgo que contiene la información más importante de este (ver Anexo 17. Ficha del riesgo). De esta forma no serán revisados por el mismo equipo de riesgos.

5.3.2. Generación versión del riesgo.

En esta fase se permite cambiar o modificar los campos llenados en las fases anteriores. Debemos tener en cuenta que cada una de las fases cuenta con un campo para “cerrar etapa”, el cual, una vez se haya seleccionado y guardado los cambios no va a permitirnos editar esa fase (ver Anexo 18. Generación de versión del riesgo en ISOlución®). Además, cada una de las fases se llena en orden cronológico y no nos permite avanzar ISOlución® mientras no se encuentre cerrada. De esta manera a través de esta fase podemos hacer modificaciones a los riesgos que ya han sido aprobados y que

muy seguramente sufrirán cambios en la compañía a lo largo del tiempo por diferentes aspectos. Por otra parte, en la fase de identificación es posible dejar inactivo el riesgo indicando que este fue eliminado de la compañía.

5.3.3. Comunicación y consulta.

El Comité de Riesgos Corporativo será la única entidad designada para aceptar riesgos valorados en niveles 'Alto' y 'Crítico'. La aceptación de este tipo de riesgos quedará documentados y aprobados en las actas del comité, con el respectivo voto emitido por cada uno de sus miembros.

Los riesgos aceptados con una valoración de 'Medio' y 'Bajo' se les deberá dar un seguimiento periódico por parte de los responsables designados (directores/ C-Level), y actualizar en los casos que sea necesario si se detecta que el nivel de valoración del riesgo aumenta, dicho monitoreo y seguimiento debe realizarse al menos una vez por año.

Cuando se identifica que el tratamiento del riesgo es de responsabilidad de un tercero (cliente, proveedor), desde la gestión de riesgos una vez evaluados los alcances de la compañía para mitigar el riesgo, solicitará mediante el formato IP-T-F-001 Informe de Gestión de Riesgo o mediante correo electrónico al tercero la aceptación del riesgo o el plan de tratamiento de éste.

Por lo anterior, el flujo de comunicación sería de la siguiente manera:

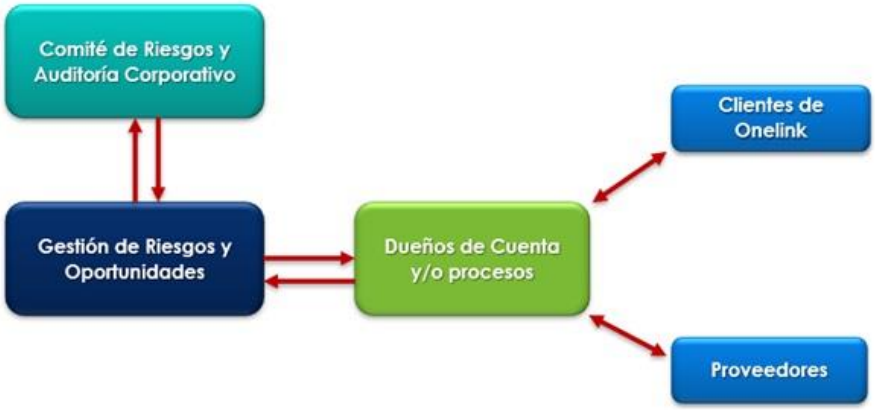


Figura 5. Flujo de comunicación de riesgos OneLink.
Tomada de: Referencia documental OneLink, 2021.

Cuando los riesgos son identificados por el proceso de Gestión de Riesgos y Oportunidades, se solicita al dueño de cuenta y/o proceso dar a conocer los planes de acción y/o controles que mitigarán el riesgo, en un plazo de 5 días hábiles a partir de la fecha de socialización, mismo tiempo que se solicitará al cliente o proveedor establecer sus planes de acción o aceptación del riesgo en caso de no aplicar ningún control.

En esta fase se solicitó al equipo de Gestión Integral de Procesos agregar el ítem "quincenal" al campo de periodicidad. Por otro lado, se llevó a cabo la identificación y cargue de los controles de tipo operativo como se mencionó inicialmente en esta fase, los cuales fueron definidos a medida que se desarrollaba esta fase para cada uno de los riesgos. Finalmente, se realizó la actualización y modificación de los controles SOA debido a que no se encontraban todos en el listado de la plataforma o estaban errados.

Los demás campos no fueron modificados, por lo cual, se trabajó con los parámetros que el equipo de riesgo había establecido previamente. Además, se debe tener en cuenta que todos los riesgos analizados formaron una base sobre la cual la compañía tiene la capacidad de construir un perfil de riesgo corporativo, o visualizar el estado actual de sus riesgos y potenciales pérdidas.

5.4. REVISIÓN, MODIFICACIÓN, CREACIÓN Y ACTUALIZACIÓN DE CAMPOS EN ISOLUCIÓN®

5.4.1. Creación de listados en la plataforma

Para el módulo se establecieron los listados que debían ser cargados para tener la información requerida al momento de subir los riesgos. Esta información corresponde a las tablas de: causas (ver Anexo digital 2. Listado de causas), consecuencias (ver Anexo digital 3. Listado de consecuencias), controles SOA (ver Anexo digital 5. Controles SOA), controles operativos (ver Anexo digital 5. Controles operativos) y servicios (ver Anexo 12. Listado de servicios), este último se hizo necesario pasar un listado al equipo de Gestión Integral de Procesos. De igual manera se incluyen los cambios mencionados en la sección de parametrización donde se debieron agregar otros ítems a diferentes campos.

5.4.2. Parametrización del módulo

Inicialmente se llevó a cabo la validación del módulo en la plataforma ISOlución® donde se observó que se encontraba enfocado a la metodología de análisis de riesgos de seguridad de la información y no riesgo SARO (riesgo operativo), por lo cual, para ese módulo se establecen controles a las consecuencias (ver Anexo 19. Fase identificación ISOlución® enfocado a seguridad de la información), pudiéndose observar que al final llamaba era a las consecuencias en lugar de las causas donde estas últimas son las que se les establecen los controles para el análisis de riesgos Saro. Por consiguiente, como solución se hizo un intercambio de tablas en la plataforma para poder llamar a las causas en lugar de las consecuencias al momento de establecer los controles (ver Anexo 20. Fase de identificación ISOlución® enfocado a riesgo Saro).

Posteriormente se revisó la etapa de análisis del riesgo donde se piden los campos de probabilidad, disponibilidad, integridad y confidencialidad (referentes al impacto).

Definiendo la metodología enfocada a riesgo Saro debido a que anteriormente está definida para los activos de información y contaba solo con ponderaciones del 1 al 3 y no tenía relación con la afectación que tendrá el activo al momento de materializarse el riesgo quedando con una ponderación 1 a 4 (ver Tabla 3. Calificación de acuerdo con la confidencialidad, integridad y disponibilidad).

Teniendo en cuenta lo anterior se ajustaron los criterios a los tipos: bajo, medio, alto y crítico. Se tuvo en cuenta que los pilares de confidencialidad, integridad y disponibilidad se verán afectados en caso de materializarse el riesgo y esta evaluación es previa a los controles, es decir, de estas calificaciones se obtuvo los resultados de riesgo inherente (es el riesgo a un activo en la ausencia de cualquier control directo o enfocado para alterar su severidad).

5.5. CARGUE DE INFORMACIÓN EN ISOLUCIÓN®

5.5.1. REGISTRO DE RIESGOS

El registro de los riesgos se realizó a través del uso de la plataforma ISOlución® y se llevó en paralelo con el levantamiento de información. Por lo cual, los riesgos fueron registrados cuando se contaba con toda la información necesaria para cada uno de los campos, especialmente los activos de información (ver Anexo 7. Riesgos cargados en ISOlución®).

En cuanto a la metodología se agendaban las sesiones necesarias para culminar con la revisión, actualización y creación de los riesgos conforme a la necesidad (ver Anexo 21. Ejemplo de agendamiento de reuniones). Estas sesiones eran acompañadas en la mayoría de los casos por un miembro del equipo de riesgos y se hacía un estudio del procedimiento o la documentación que se tenía del área cargada en la plataforma. Además, era necesaria validar la información suministrada debido a que en muchos casos los dueños del proceso desconocían los procedimientos que llevaban a cabo y los riesgos que podrían salir respecto a esto; gracias a esto era necesario buscar información adicional

para lograr una correcta identificación de los riesgos y diligenciamiento de cada uno de ellos.

En este orden de ideas los riesgos que se habían registrado inicialmente con la metodología antigua no siempre eran socializados con los dueños, por tal razón, eran desconocidos por ellos. Como resultado se envió la matriz con los campos faltantes y se hizo una socialización previa para validar toda la información que se tenía de los riesgos y posteriormente crear nuevos riesgos, eliminarlos, actualizarlos o modificar la información que se tenía.

Este método de recolección de información solo fue aplicado a los riesgos de la compañía y no los asociados a las cuentas (clientes) debido a que no existe una buena disposición por parte de los gerentes de cuenta para lograr validar la información. Para el caso de estas se validó y culminó la información conforme a nuestra subjetividad y el estudio realizado a cada una de las cuentas como los planes de mejora, reporte de riesgos, información de auditorías internas, entre otros.

Una vez culminado el registro de los riesgos se envió a los dueños del proceso para su aprobación y revisión quedando en etapa de cerrado (ver Anexo 22. Envío de riesgos). Sin embargo, debido a solo tenían licencia de Usuarios administradores para el módulo de riesgos los miembros del equipo de seguridad de la información, gestión integral de proceso y equipo de riesgos. Por lo cual, se solicitó al equipo de Gestión Integral de Procesos la otorgación de las licencias a los actores involucradas para que puedan hacer uso del módulo no solo desde usuarios de consulta. Con respecto a esta solicitud ya fue aprobada y se envió el listado especificando las restricciones y acceso especifico que podrán tener a las diferentes fases y carpetas.

5.6. PROGRAMA DE CAPACITACIÓN DEL MÓDULO ISOLUCIÓN® PARA LA GESTIÓN DE RIESGO

Se creó y diseñó una guía (ver Anexo digital 7. Guía del módulo de riesgos en ISOlución®) y un video (ver Anexo digital 8. Manejo del módulo de riesgos en ISOlución®) con la metodología de riesgo para socializar el uso de la plataforma y del módulo. De tal manera que se continúe utilizando ISOlución® para todo el manejo de la información permitiendo una mayor supervisión y monitoreo generando cultura en todos los Increybles® (recurso humano de OneLink) para la gestión de riesgos en la organización.

5.7. SOCIALIZACIÓN DEL PROYECTO DE GRADO Y ENTREGABLES

A través de un encuentro virtual por la plataforma de Microsoft Teams se socializó el proyecto de grado incluida la guía y el video de capacitación con mi jefe directo que fue el Coordinador de Riesgo y Continuidad de Negocio, Brian David Caro Martínez (ver Anexo digital 9. Acta de socialización de proyecto de grado). Además, se entregó la plantilla en Excel para la documentación de los riesgos (ver Anexo digital 4. Plantilla de riesgos) donde se anexa un riesgo de ejemplo diligenciado (ver Anexo 27. Ejemplo riesgo en Excel) en todas sus etapas y un instructivo para el uso de esta (ver Anexo 28. Instructivo matriz de riesgo en Excel). Finalmente, se muestra como queda la matriz de riesgos en ISOlución® (ver Anexo 29. Matriz de riesgo ISOlución®).

6. PROPUESTA DE MEJORAMIENTO

El desarrollo de la práctica se llevó a cabo en el área de gestión de riesgos y continuidad de negocio. Este subproceso está conformado por dos miembros que son el coordinador y analista de riesgos y continuidad de negocio. Por ese motivo, aun siendo un área de bastante complejidad y transversal en toda la compañía para los diferentes países y sedes en cada uno, no cuenta con todo el talento humano necesario para abarcar todas las actividades relacionadas a riesgos y continuidad de negocio, por lo cual, hasta ahora ha cobrado mayor importancia en gran parte por la coyuntura ocasionada por la pandemia y temas de certificaciones como la norma ISO 27001 (2013).

Dado lo anterior, la empresa contaba con grandes debilidades en la gestión de los riesgos en temas de metodología y gestión documental, haciendo necesario implementar un sistema que permitiese la documentación de toda la información y logrará un importante aspecto que es la participación de cada dueño de riesgo en el proceso de gestión, donde no solo fuera partícipe el gestor de riesgos sino todos los actores involucrados.

Por consiguiente, respondiendo a esa necesidad se llevó a cabo este proyecto para lograr una gestión de riesgo eficaz que ayudará a eliminar los reprocesos presentados en el diario vivir de la compañía. De esta manera, se hizo toda la gestión de riesgos conforme a la nueva metodología y fortaleciendo todo el proceso en cada fase para ser trasladado a la plataforma ISOlución®. Cabe resaltar que el objetivo de la organización es dejar de usar las plantillas de Excel a corto plazo y registrar los riesgos directamente en la plataforma.

Se obtuvo como resultado que el principal aporte de esta nueva metodología y gestión documental, fue hacer partícipes a todos los actores involucrados, gestionar riesgos de forma correcta bajo una parametrización, obtención de resultados y

calificaciones objetivas, riesgos creados de acuerdo a información suministrada por los mismos dueños conocedores del proceso, posibilidad de llevar una traza cronológica del riesgo incluido planes de acción y asignación de responsables para los controles, todo lo anterior agiliza y ayuda en los procesos de certificación, es decir, cuando se llevan a cabo las auditorias se contará con una información sintetizada en una plataforma donde se encontrará toda la documentación requería de forma específica, por ejemplo, se establece las evidencias de cada uno de los controles.

Es preciso señalar que este proyecto se llevó a cabo con la intención de poder hacer uso de la plataforma ISOlución® implementando el módulo de riesgos, el cual, había sido creado hace más de dos años, pero no era implementado por motivos de parametrización, problemas en la plataforma, tiempo, recurso humano, definición de metodología, entre otros.

Finalmente, se hizo necesario generar una capacitación de aprendizaje para el uso del módulo de riesgos en ISOlución® donde cualquier actor involucrado a futuro pueda crear sus riesgos y el equipo de riesgos sea quien verifique toda esa gestión, es decir, todo lo contrario, a como se está haciendo en la actualidad; permitiendo que no solo el equipo de riesgos sean los únicos conocedores del módulo sino todos.

7. APORTES DEL ESTUDIANTE

Por lo que se refiere al desarrollo de la práctica esta fue realizada en un ambiente complejo debido a la coyuntura que afronta el país por la pandemia ocasionada a raíz del virus Covid-19, tuvo como modalidad el teletrabajo. De modo que todas las reuniones se llevaron a cabo de forma virtual a través de la plataforma Microsoft Teams (ver Anexo 21. Ejemplo de agendamiento de reuniones) al igual que todas las actividades necesarias para la realización del proyecto.

En el desarrollo de la práctica se tuvo como meta implementar el módulo de riesgos en OneLink para cada uno de los procesos, haciendo inicialmente una actualización de riesgos de acuerdo con la actualidad y necesidades de cada subproceso. También la inclusión de nuevos riesgos que se hayan presentado en la compañía o los clientes de esta.

Por otro lado, se dejó un consolidado por áreas y subprocesos de cada uno de los riesgos gestionados (ver Anexo 23. Riesgos por proceso, subproceso y área) con todos los campos exigidos en la plataforma haciendo uso de matriz de Excel (ver Anexo digital 4. Plantilla de riesgos). Así mismo se implementó la plataforma con el traslado de esa misma información en la plataforma, pero por motivos de seguridad de la información y tratamiento de datos estos no pueden ser mostrados en el trabajo los riesgos. Sin embargo, se mostrarán capturas de algunos riesgos de ejemplo (ver Anexo 7. Riesgos cargados en ISOlución®).

Finalmente, la realización del programa de capacitación para el manejo del módulo de riesgos en ISOlución® permitió generar una culturalización que ayudará que los líderes de los procesos y la compañía en general cree consciencia y conocimiento sobre la gestión de sus riesgos debido a que en la actualidad estos solo eran de conocimiento por los gestores del riesgo aun cuando estos se generaban conforme a sus procesos. Razón por la cual, esta mala práctica generaba inconveniente en las auditorías donde estos no eran

sustentados por los actores de los procesos sino por el equipo de riesgos debido al desconocimiento total de matriz aun cuando muchos riesgos eran socializados con estos.

En conclusión, esta implementación de ISOlución® permitió una gestión documental acertada y sistematizada, donde se puede llevar un control y monitoreo. Además, se vela por los tres pilares de la información y se pueden asociar a los dueños y custodios de la información allí cargada.

8. CONCLUSIONES

Este informe fue desarrollado basado en las normas de Gestión de Riesgos (ISO 31000, 2018), Sistemas de Gestión de Seguridad de la Información (ISO 27001, 2013), Sistemas de Gestión de la Calidad (ISO 9001, 2015), Metodología de Gestión de Riesgos de Seguridad de la Información (ISO 27005, 2008) y Sistema de Administración de Riesgo Operativo (SARO). En compañía del coordinador y el analista de riesgos y continuidad de negocio.

- El uso de la plataforma ISOlución® permitió llevar un control de los riesgos en cada una de sus fases, participación de todos los actores involucrados, una gestión de riesgos eficaz bajo parametrizaciones, obtención de resultados y calificaciones objetivas, riesgos creados de acuerdo a información suministrada por los mismos dueños conocedores del proceso, posibilidad de llevar una traza cronológica del riesgo incluido planes de acción y asignación de responsables para los controles agilizando los procesos y ayudando en las diferentes auditorias de certificación.

- La estandarización de la información de diferentes campos permitió generar riesgos genéricos y específicos que evitará la duplicidad de información y/o riesgos que estuviesen apuntando al mismo objetivo.

- Llevar el proceso de levantamiento de información con los dueños de los riesgos permitió que estos fueran gestionados de forma objetiva y atendiendo a las problemáticas del área, estableciendo controles que estuviesen bajo su alcance y fueran acordes a sus procedimientos una valoración del riesgo que realmente mitigara o eliminará la materialización de estos.

- La modificación y adaptación de la metodología de riesgos permitió la generación de una matriz de riesgos integral que abarcara todos los campos que permitieran gestionarlos de forma eficaz.

- La realización del programa de capacitación a través de un manual y video permitió que se generará un acercamiento de todos los actores involucrados a la gestión de riesgos ayudando en un futuro que estos sean quienes lleven a cabo todo el proceso de identificación de riesgos en la plataforma de forma correcta y de acuerdo la metodología establecida.

- Las sinergias entre la dirección, equipo de seguridad de la información y equipo de gestión integral de procesos fueron fundamentales para la implementación del módulo de riesgos debido a que cada uno jugó un rol importante para cada una de las fases necesarias para la gestión de los riesgos.

- Todos los riesgos analizados formaron una base sobre la cual la compañía tiene la capacidad de construir un perfil de riesgo corporativo o visualizar el estado actual de sus riesgos y potenciales pérdidas. Además, podrá cumplir sus objetivos y prevenir la interrupción del negocio.

- Los beneficios de la utilización del software ISOlución® en la compañía es administrar de manera ágil y eficaz todos los componentes de su Sistema de Gestión ISO 9001 e integrarlo con otros Sistemas de Gestión ISO o con otros modelos de cumplimiento normativo como la Gestión de Riesgos. Además, apoya la toma de conciencia, el manejo de riesgos y el contexto estratégico, facilitando el mantenimiento de sus certificaciones.

9. RECOMENDACIONES

- Continuar con la implementación de la plataforma ISOlución® y anular las plantillas de Excel.

- Debe mejorarse las sinergias entre las áreas para evitar reprocesos y afectación en los tiempos de ejecución de las actividades, es decir, lograr una dependencia de terceros mínima para una mayor agilidad de los procesos.

- Solicitar al proveedor de plataforma ISOlución® mejoras en el módulo como la visualización de la información, permisos de administradores, por ejemplo, la ficha del riesgo que se envía a la persona que aprobará el riesgo, pero no muestra toda la información que se trazó en gestión del riesgo haciendo que la verificación de esta no sea completa para la aprobación o rechazo del mismo. Además, hoy día solo el responsable del riesgo que es mi persona es la que puede tener acceso a ellos en cada fase, impidiendo que los demás miembros del equipo puedan validar la información que he suministrado y/o cargado.

- Se debe generar una cultura fuerte en la gestión de riesgos que permita un compromiso por parte de cada proceso, subproceso y áreas de la compañía, debido a que era difícil llevar a cabo las reuniones por disponibilidad y muchos actores no creían importante el proceso de identificación de sus riesgos. Además, dejaban a cargo al área toda la responsabilidad para identificarlos aun cuando estos son los que deben suministrar la información. Teniendo en cuenta todo lo anterior se generaron obstáculos y demoras en el proceso debido a que había que llevar a cabo todo el estudio de este conforme a la información documentada en la plataforma en muchas ocasiones.

- En ocasiones muchos campos permitían la creación de duplicidades, es decir, no contaban con una validación que bloqueara la creación de campos que ya se encontraban. Es necesario resaltar que esto se daba en muchas ocasiones debido a que se tenían más de

300 registros y la validación de coincidencias para la plataforma debía ser exacta, haciendo difícil aún más validar los campos.

- Inclusión de mejoras relacionadas a la posibilidad de cargues masivos en el módulo de riesgos, evitando reprocesos debido a los listados y bases de datos extensas.

10. BIBLIOGRAFÍA

NTC, 31000, Norma técnica colombiana sobre Gestión de Riesgos. Principios y directrices, 1-25, (2018).

NTC, 27001, Norma técnica colombiana sobre Sistemas de Gestión de Seguridad de la Información, 1-45, (2013).

NTC, 9001, Norma técnica colombiana sobre Sistemas de Gestión de la Calidad. Requisitos, 1-47, (2015).

NTC, 27005, Norma técnica colombiana sobre Metodología de Gestión de Riesgos de Seguridad de la Información, tecnología de la información, técnicas de la seguridad, 1-74, (2008).

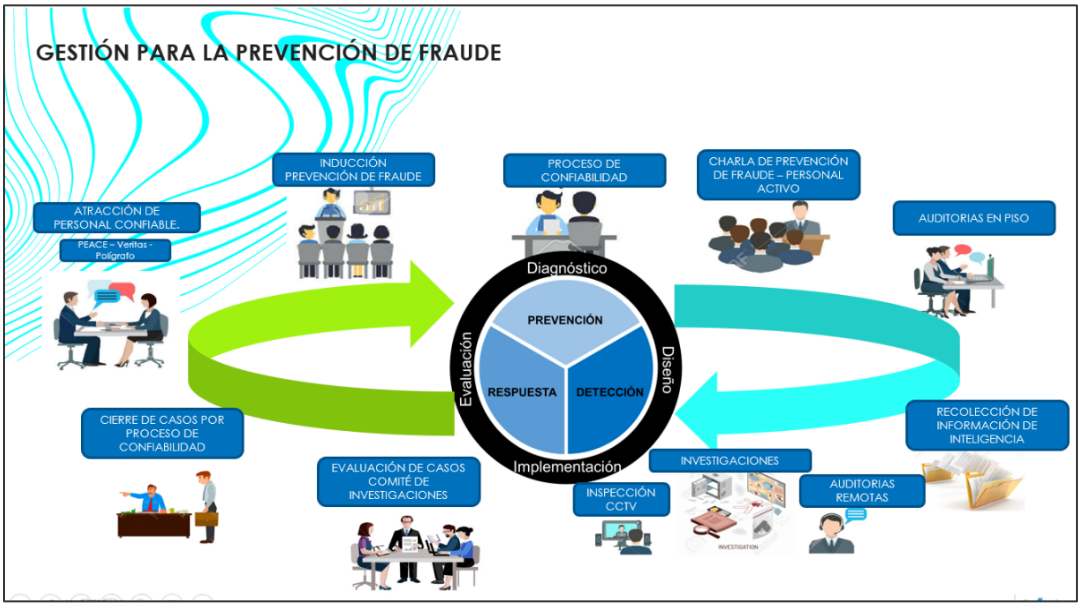
Instituto Nacional para La Evaluación de la Educación (2014), Metodología de Administración de Riesgos del Instituto Nacional para la Evaluación de la Educación. https://www.inee.edu.mx/wp-content/uploads/2019/01/Metodolog%C3%ADa_de_Administraci%C3%B3n_de_Riesgos_del_INEE.pdf

The Institute of Internal Auditors (2019), Tres líneas de defensa. https://global.theiia.org/translations/PublicDocuments/3LOD-IIA-Exposure-Document-Spanish.pdf

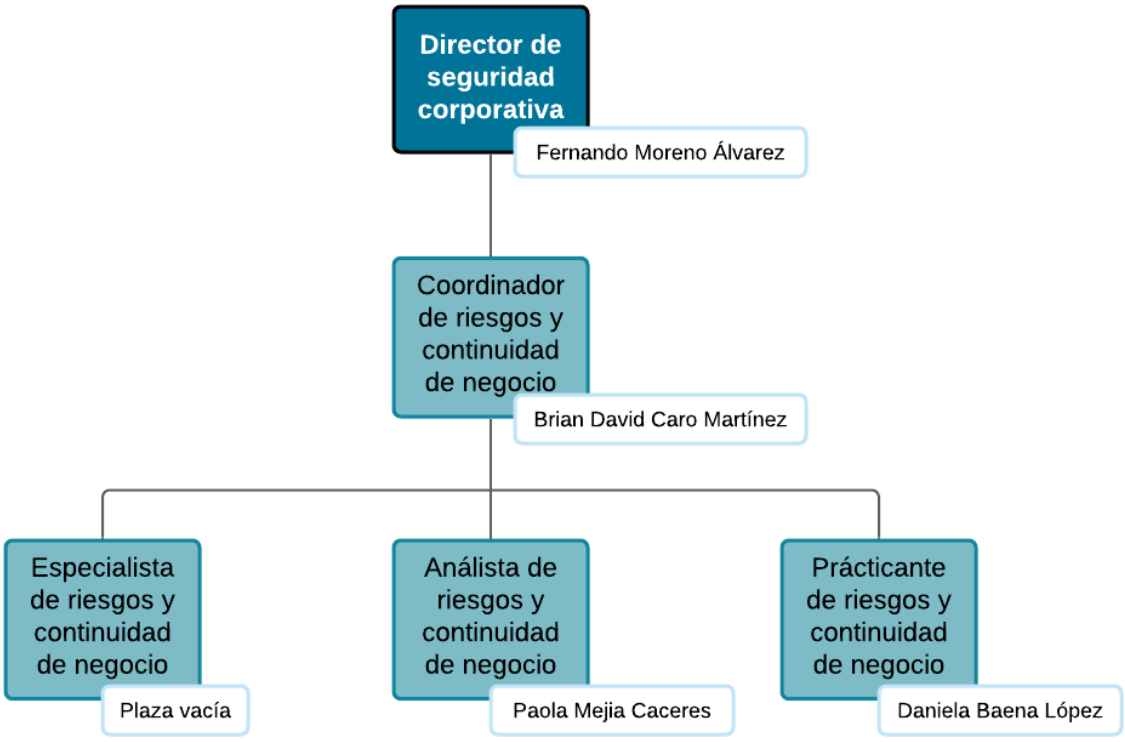
ANEXOS

Anexo 1. Valores corporativos de OneLink.

Anexo 2. Gestión de prevención de fraude en OneLink.



Anexo 3. Estructura organizacional del área gestión de riesgos y continuidad.



Anexo 4. Mapa de procesos de OneLink.

Anexo 5. Mapa de subprocesos del proceso Gestión de gobierno, riesgo y cumplimiento.

Anexo 6. Establecimiento del contexto interno, externo y contexto del proceso.

ESTABLECIMIENTO DEL CONTEXTO INTERNO
Estructura organizacional
Funciones y responsabilidades (políticas, objetivos y estrategias implementadas)
Recursos y conocimientos con que se cuenta (económicos, personas, procesos, sistemas, tecnología e información)
Relaciones con las partes involucradas
Cultura organizacional

ESTABLECIMIENTO DEL CONTEXTO EXTERNO
Políticos
Económicos y financieros
Sociales y culturales
Tecnológicos
Ambientales
Legales y reglamentarios

ESTABLECIMIENTO DEL CONTEXTO DEL PROCESO
Objetivo y alcance del proceso
Interrelación con otro proceso
Procedimientos asociados
Responsable del proceso
Activos del proceso

Anexo 7. Riesgos cargados en ISOlución®.

isolución 4.8.21.09.20.38

¿Qué desea hacer? Daniela Baena López

Tareas Documentacion Medición Mejora Sistemas Configuración

Filtro de Riesgos SARO

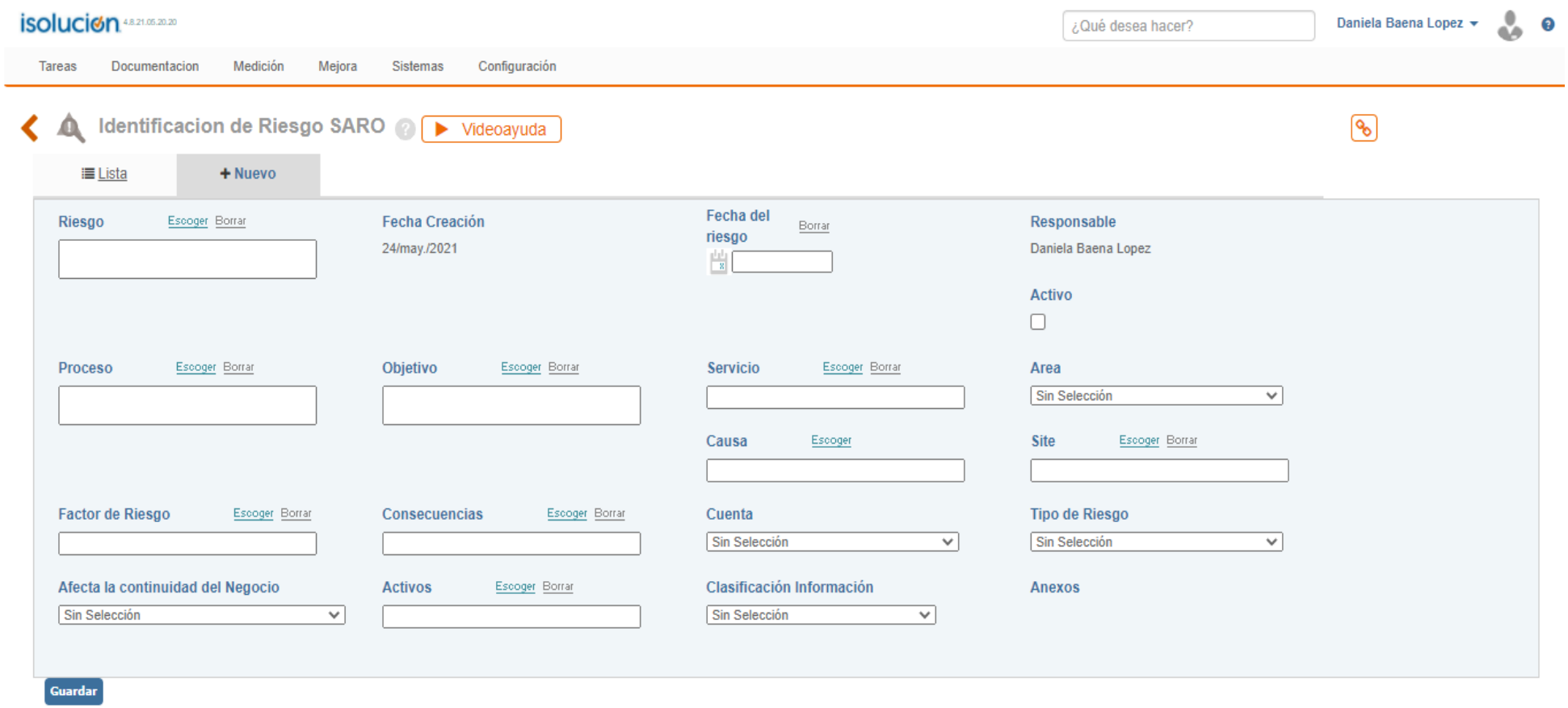
Filtrar lista Otros filtros

Filtrar por palabra

Número de resultado(s): (176) Página 1 de 4 > >>

Num.	Riesgo	Versión	Etapa	Fecha del Riesgo	Proceso	Área	Objetivo Proceso	Factor del Riesgo	Responsable	Site	Tipo de Riesgo	Historial
GP - R -2	Fuga de información confidencial de los procesos de investigación	1	Cerrado	18/dic./2019	Gestión de prevención de fraude	Prevención Fraude	Prevenir, detectar e investigar las conductas del recurso humano para mitigar los riesgos de fraude interno y externo.	Recursos Humanos	Practicante Riesgos y continuidad	Todas	Riesgo de Seguridad de la Información	Historial Cambios
CN - R -1	Interrupción prolongada de los servicios por la inefectividad de los planes de contingencia de OneLink.	1	Cerrado	02/jun./2019	Gestión de continuidad	No aplica	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	Recursos Humanos	Practicante Riesgos y continuidad	Todas	Riesgos de Administración de Procesos	Historial Cambios
CN - R -2	Entrega inoportuna de las estrategias de continuidad	1	Cerrado	07/jul./2020	Gestión de continuidad	No aplica	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	Procesos	Practicante Riesgos y continuidad	Todas	Riesgos de Administración de Procesos	Historial Cambios
CN - R -3	Estrategias de continuidad erradas o no efectivas	1	Cerrado	07/jul./2020	Gestión de continuidad	No aplica	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	Procesos	Practicante Riesgos y continuidad	Todas	Riesgos de Administración de Procesos	Historial Cambios
CN - R -4	Pérdida de confidencialidad de la información	1	Cerrado	07/jul./2020	Gestión de continuidad	No aplica	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	Tecnología	Practicante Riesgos y continuidad	Todas	Riesgo Legal o de Cumplimiento	Historial Cambios
GP - R -3	Inoportunidad en la ejecución de actividades de prevención fraude	1	Cerrado	02/jun./2018	Gestión de prevención de fraude	Prevención Fraude	Prevenir, detectar e investigar las conductas del recurso humano para mitigar los riesgos de fraude interno y externo.	Procesos,Recursos Humanos	Practicante Riesgos y continuidad	Todas	Riesgos de Administración de Procesos	Historial Cambios
GP - R -4	Apreciación y análisis inadecuado de un evento de conducta fraudulenta	1	Cerrado	18/dic./2019	Gestión de prevención de fraude	Prevención Fraude	Prevenir, detectar e investigar las conductas del recurso humano para mitigar los riesgos de fraude interno y externo.	Procesos,Recursos Humanos	Practicante Riesgos y continuidad	Todas	Riesgos de Administración de Procesos	Historial Cambios
CM - R -2	Incumplimientos regulatorios y contractuales de seguridad y privacidad de datos	1	Cerrado	27/ago./2019	Gestión de cumplimiento	Legal y cumplimiento	Realizar un seguimiento sistemático en la aplicabilidad de los requisitos normativos y legales de la seguridad de la información.	Procesos	Practicante Riesgos y continuidad	Todas	Riesgo Legal o de Cumplimiento	Historial Cambios

Anexo 8. Fase de identificación en ISOlución®.



Anexo 9. Nombre del riesgo.

Se colocaron los nombres de los riesgos a doble columna por motivos de espacio.

NOMBRE DEL RIESGO	
Acceso a la información en SAP por parte de proveedores	Inadecuada gestión del SGSI en la compañía
Adquirir beneficio económico propio o de un tercero	Inadecuada planeación de presupuesto de actividades para el proceso de Gestión del Talento Humano
Afectación de la imagen de la compañía	Inadecuada selección de futuros Increybles® teniendo en cuenta el perfil del cargo
Afectación de la integridad física del Increyble®	Inadecuado establecimiento de alcance de los procesos a asegurar por parte de la auditoría interna financiera
Afectación del bienestar de los empleados de la compañía por incumplimiento de los lineamientos de seguridad y salud en el trabajo	Incumplimiento al cronograma de auditoría interna financiera
Afectación en el monitoreo de las implementaciones nuevas o cambios en la infraestructura	Incumplimiento al indicador de completion
Apreciación y análisis inadecuado de un evento de conducta fraudulenta	Incumplimiento de las normas para el cálculo de la nómina
Asignación salarial errada	Incumplimiento de los BHG
Aumento o disminución en la tasa de cambio contra lo presupuestado	Incumplimiento de los estándares establecidos para la implementación, documentación y sostenibilidad del Sistema de Gestión

NOMBRE DEL RIESGO	
Bonos entregados de manera errada	Incumplimiento en los tiempos de recaudos pactados contractualmente
Cambio desfavorable de la percepción de las partes interesadas de la compañía	Incumplimientos regulatorios y contractuales de seguridad y privacidad de datos
Cambios desfavorables del mercado, variaciones del dólar y demás divisas en donde la compañía esté invirtiendo	Indebida promoción de Increybles®
Daño a la infraestructura física de los site por eventos externos	Indebida promoción de Increybles®
Daño a la integridad moral y emocional del empleado en el proceso de selección	Indisponibilidad de la prestación del servicio por parte del proveedor
Daño en la infraestructura física por manifestaciones, marchas y/o cualquier evento externo	Indisponibilidad de los servicios
Daño inesperado de la infraestructura física y/o inmuebles	Indisponibilidad de los servicios de VPN
Daño o hurto de los recursos físicos y/o tecnológicos de la compañía	Indisponibilidad de los servicios de red
Debilidad en el análisis estratégico y/o asignación del presupuesto para la implementación de nuevos proyectos o el sostenimiento de los actuales dentro de la compañía	Inefectividad del SGI por incumplimiento a la política de seguridad de la información

NOMBRE DEL RIESGO	
Debilidad en la aplicación de controles de acceso	Inoportunidad en la captación de clientes por desactualización de los portafolios de servicios
Debilidad en la gestión de vulnerabilidades de seguridad de la información	Inoportunidad en la ejecución de actividades de prevención fraude
Deficiencia en el análisis y entrega de resultados	Inoportunidad en la notificación de hallazgos identificados a los procesos auditados
Demora en la ejecución de las actividades	Insatisfacción del cliente interno
Demora en la prestación del servicio	Interrupción de las operaciones
Demora en la solución de incidentes mayores	Interrupción inesperada en la prestación del servicio
Demoras o fallas en la prestación del servicio de seguridad física	Interrupción prolongada de los servicios por la inefectividad de los planes de contingencia de OneLink.
Desactualización del Sistema de Gestión e incumplimiento de los requisitos normativos	La asignación del presupuesto es asignada erradamente
Desajuste o desbalance en los estados financieros	La prestación del servicio es deficiente

NOMBRE DEL RIESGO	
Desconocimiento de las metodologías de mejora continua del Sistema de Gestión	Los enlaces de datos e internet son prestados de manera deficiente
Detrimento económico por fraude en proceso de abastecimiento	No realización de ajustes al plan anual de auditoría interna
Detrimento económico y fraude por ausencia de control en pago a proveedores	No realización de seguimiento de las situaciones reportadas a los procesos
Disminución de la calidad del servicio	Pago no oportuno a proveedores
Distribución de información no autorizada por correo electrónico	Pérdida de accesos a la documentación de los procesos, procedimientos y acciones de mejora registrados en ISOlución®
Distribución no controlada de información confidencial	Pérdida de accesos al SGI registrado en ISOlución®
Distribución y/o envío de información confidencial por canales de comunicación no controlado	Pérdida de confidencialidad de la información
Distribución y/o envío de información confidencial por canales de comunicación no controlados	Perdida de confidencialidad de las estrategias de negocio
Entrega demorada de los servicios	Perdida de impacto comercial
Entrega inoportuna de las estrategias de continuidad	Perdida de la confidencialidad, integridad y disponibilidad de la información
Entrega inoportuna de licitaciones o propuestas comerciales	Perdida de la confidencialidad, integridad y disponibilidad de la información en operaciones WFH

NOMBRE DEL RIESGO	
Estrategias de continuidad erradas o no efectivas	Perdida de la disponibilidad, integridad y confidencialidad de la información almacenada en SharePoint OL
Exigencia de dinero a cambio del beneficio propio y de mantener proveedores dentro de los vínculos comerciales con OneLink	Pérdida de la información por robo de activos de información
Exposición al fraude por la vinculación de personal no idóneo para la compañía	Perdida de oportunidad en el uso de plataforma Moodle/One University
Falla en los balances financieros e información contable errada o incompleta	Perdida de personal idóneo para área
Falla en los componentes de la infraestructura del data center y otros sistemas de las instalaciones	Pérdida de posicionamiento en el mercado
Falta de colaboración en el levantamiento de gestión de conocimiento	Perdida de reputación por incumplimientos contractuales e inversiones desfavorables
Fraude en la generación de la nómina	Pérdida del know-how sobre cómo se realiza a nómina, teniendo en cuenta las particularidades del grupo OneLink
Fuga de información confidencial de los procesos de investigación	Perdida en posicionamiento y participación

NOMBRE DEL RIESGO	
Fuga de información personal del Increyble®	Pérdida operativa y de servicios de las operaciones en WFH
Fuga de información por uso de recursos tecnológicos no corporativos	Posibilidad de vínculos con clientes y/o proveedores involucrados con LAFT
Inadecuada gestión del ciclo de auditorías internas	Posibilidad de vínculos con personal, clientes y/o proveedores involucrados con LAFT
Inadecuada definición de las políticas de gestión de accesos	Presencia de vulnerabilidades a virus o ataques
Prestación deficiente del servicio	Prestación del servicio deficiente por el desconocimiento de los lineamientos del cliente o estratégicos por parte del personal
Propuestas comerciales no beneficiosas	Toma de acciones inoportunas o no adecuadas por el desconocimiento del objetivo y alcance de los indicadores de gestión
Transmitir erradamente las comunicaciones a toda la organización	Uso de Software no controlado
Uso inadecuado de usuarios de las plataformas de información	

Anexo 10. Listado de procesos.

PROCESOS
Ejecución y control de operaciones
Estrategia corporativa
Gestión comercial
Gestión de gobierno riesgo y cumplimiento
Gestión de infraestructura física
Gestión de marca y comunicaciones
Gestión de satisfacción con el cliente
Gestión del recurso financiero
Gestión del talento humano
Gestión jurídica
Gestión tecnológica
Planeación e implementación operativa

Anexo 11. Listado de subprocesos.

SUBPROCESOS
Auditoría interna financiera
Construcción de propuesta comerciales
Cuidado integral del Increybles® y medio ambiente
Cultura, propósito y sostenibilidad
Ejecución y control de operaciones
Estrategia corporativa
Estrategia financiera
Gestión de continuidad
Gestión de cumplimiento
Gestión de infraestructura física
Gestión de iniciativas comerciales
Gestión de la seguridad de la información
Gestión de marca y comunicaciones
Gestión de prevención de fraude
Gestión de seguridad física y monitoreo
Gestión de servicios y soporte de TI
Gestión del diseño organizacional
Gestión Integral de procesos
Gestión jurídica
Gestión y desarrollo de Increybles®
Implementación operativa
Planeación de la operación
Provisión, implementación y entrega de TI
Transacciones financieras

Anexo 12. Listado de servicios.

El listado se colocó a triple columna debido al espacio.

SERVICIOS		
Account Specialist	Centro de monitoreo	ESolution
Aclaraciones y Asesoría comercial	Chat	E-solution front
Acquisition	Chat (WP)	Establecimiento de la Compensación
Activaciones	Chat Correo Móvil	Estandares
Actividades y Eventos	Chat Correo Multimedia	Estructura Organizacional
Activos Fijos	Chat mp	Exámenes
Acumulaciones Retro	Chatbot	Experian Lead
Administración de Acceso	Cierre de Ciclo	Experience Center
Administración de logística y despacho	Cirugía Estética	Facebook
Administración de servicios de back office	Claro Corporativo	Farmacias
Advisor	Cobros	Feed
Afiliación	Comercial Multimedia	FFI Conciliación
Agendamiento	Commercial	FFI Lifemiles
Aliados Empresas SAC	Compensación	FFI Pagos & Servicios
Aliansalud	Comprador	FFI recuperación
Alojamiento	Concierge	FFI Validación
Ambiental	Construcción de Cargo Nuevo	Fidelización

SERVICIOS		
Apoyo Operación	Contabilidad	Fijo
Apoyo staff	Contención	Filtro retención
Arus	Contratación	Financial Accounting
Asignación de Citas	Control de Ingresos	Finanzas y contabilidad
Asistencia al Directorio	Control de Trafico	Formación
Atención al cliente	Convenios	Formulario Web
Atención Distribuidores	Coronavirus	Fraudes
Auditoría de factura	Correo	Front
Autorizaciones Regionales	Correo electrónico	Front II Nivel
Avianca	Correos High Value Customer	Full Service Vendor
BA Specialist	Correos Lm	Gaming Support
Back Office PQRS	Costos	Gerencia de Servicios
Back remisiones	Costos e Inventario	Gerente
BackOffice	CPG - OCC	Gerente de Operaciones
Bank	CPG - pickers	Gestiones especiales
Base de Datos y Soporte Aplicaciones (inconcert)	CPG- shoppers	Gestores
Bilingues live / non live	CPG´S	Getsolution

SERVICIOS		
Blending	Créditos	Glosas
BO Business Connect	Critico	Grupo Roble
BO Business Connect Francia	CSAT analyst	Grupos
Bo Chat	Cuentas Por Cobrar	High Value Customer
Bo Conciliación TC	Cuentas Por Pagar	High Value Support
Bo Contraentrega	Cumplimiento y Seguridad de las operaciones de IT	IMEI
BO Despacho	Customer Support	Inbound
Bo Equipajes	CVS	Inbound Sales
Bo e-solution	Data Center	Incapacidad
BO Eventos Operacionales–IROPS Support	Despacho	Incidentes
Bo Front Desk	Despacho Dinámico	Inducción de Demanda
Bo Market Place	Despacho Nivel I	Información & asesoría
Bo Rc	Despacho Santa Ana	Ingresos y Afiliadas
Bo SAC Ingreso Casos	Diamond Live	Intercompany
Bo Servicio al Cliente	DIAMOND LIVE BILINGÜES	Inventarios
Bono Virtual	Diamond Non Live	IT
Bonos de dotación	Diferencia de precios	L&F
BPO	Dinamica	LBCS
Buen gobierno	Dirección de Aplicaciones y desarrollo	Lead
Buffer	Dirección de Operaciones	Lealtad
Business Connect	Director	Lifemiles

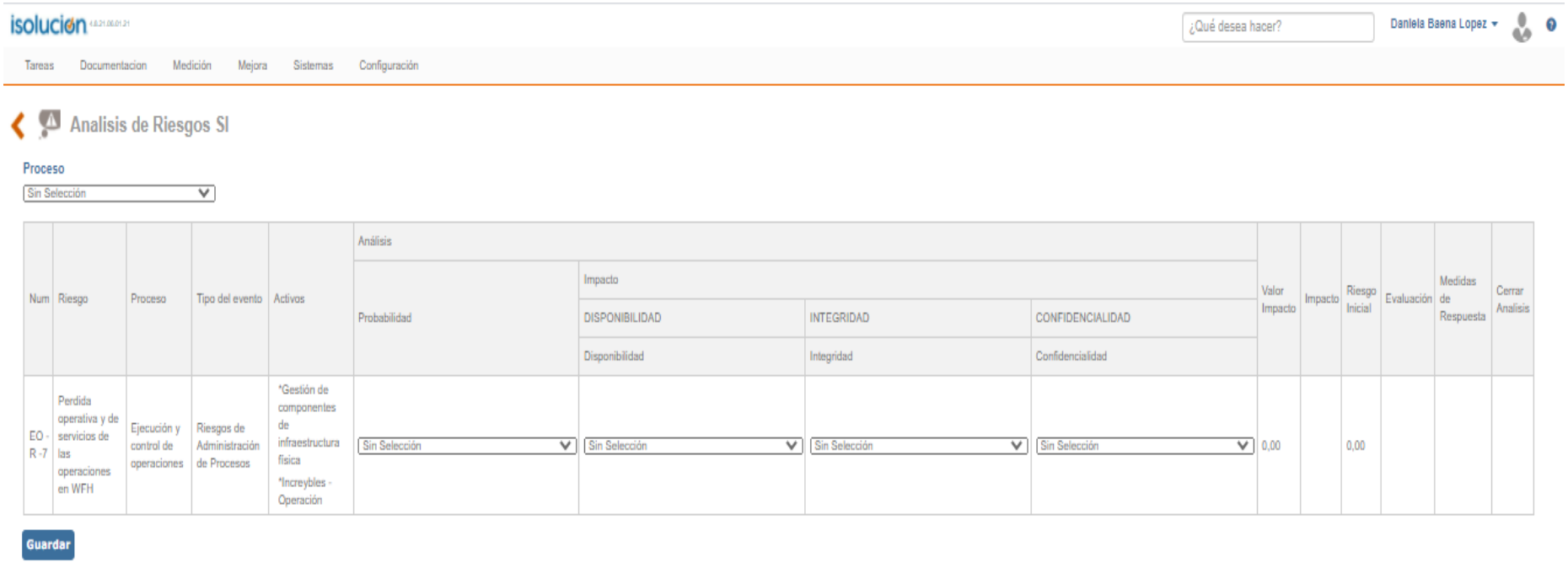
SERVICIOS		
C2c	Dpto Especializado	Lifemiles Pin
Caja y Bancos	EAAB	Lifemiles Silver AV
Calidad	E-commerce - live	Línea Ética
Cambio paquetes	E-commerce - non live	Live Chat
Cambios Operacionales	EE/POTX Collections	Market Place
Cambios Voluntarios	Egresos y Activos Fijos	Medicamentos
Cambios Voluntarios Expertos	Email	Mejora Continua
Cambios Voluntarios Millas	Emergente	Mensajería
Cancelaciones	Emi	Mentor
CAP	Emisión de Pagos	Mercado envíos
Care	Empleo y Emprendimiento	Migracion_DTA
Cartera de Crédito	Encuestas	Moderation
CCT1 Email	Energía - Data Center	Monitoreo
CCT1 Messaging	Enlace de datos e internet	Monitoreo Digital
Ce manager	Equipajes	Monitoreo Fraudes
Centro Administrativo Documental	Escalation	Móvil

SERVICIOS		
Movil Torre	Service Desk	OPS manager
Multimedia	Servicedesk 1.5	Outbound
Multimedia Santa Ana	Servicio al Cliente	OYS salud
Múltiple	Servidores	Pagos & Servicios front
Múltiple Akyta	Smart/Pos	Papiamento
Múltiple AnchorFree	Social	PBS
Múltiple Claro NIC	Social media	Perfil fraude
Múltiple Claro SV	Solicitud de Crédito	Plan carrera
Múltiple TXU NIC	Solucion en línea	Plan Complementario
Múltiple VHL	Soporte Agencias	Pospago
MultiSkill	Soporte Carga	Post Compra
Multiskill Q6	Soporte Comercial	Potencial Live
NetWorking	Soporte Comercial Móvil	Potencial Non Live
NLOB	Soporte Corporativo	Prepago
No aplica	Soporte en Procesos Comerciales	Prevención de fraude
Nóminas	Soporte Internet	Pricing
Nóminas y Procesos Fiscales	Soporte multimedia	Procesos Disciplinarios
Notificación eventos operacionales	Soporte Nuevos Rappitenderos Activación	Procesos Fiscales
Offline	Soporte Nuevos Rappitenderos Chat	Producción
Operaciones	Soporte Operaciones Irregulares	Protecciones
Oportunidad de Citas	Soporte Procesos de Talento Humano	Proyectos

SERVICIOS		
Rappitenderos	Soporte Procesos Regulatorios y Alianzas	Proyectos IT
Rappitenderos Actualización De Datos	Soporte técnico	Proyectos Validaciones
Redes Sociales	Sostenibilidad	Prustomer
Redes Sociales Email	Spanish	Puntos Colombia
Registro	Spanish Email	Rappi pay Wap
Reintegros	Specialist	Rappisupport
Relaciones laborales	SSO	Telesales
Reporte de incidentes mayores	Staff	Televentas
Reservation Inbound	Standard Live	Todos
Residential	Submissions	TPV
Restaurantes AAA	Subsidio Monetario	Transacciones en Línea
Restaurantes BO	Super salud	UGA
Restaurantes Live	Supervisión	UK
Restaurantes Monitoreo Centralizado	Supervisor	Umd Ips

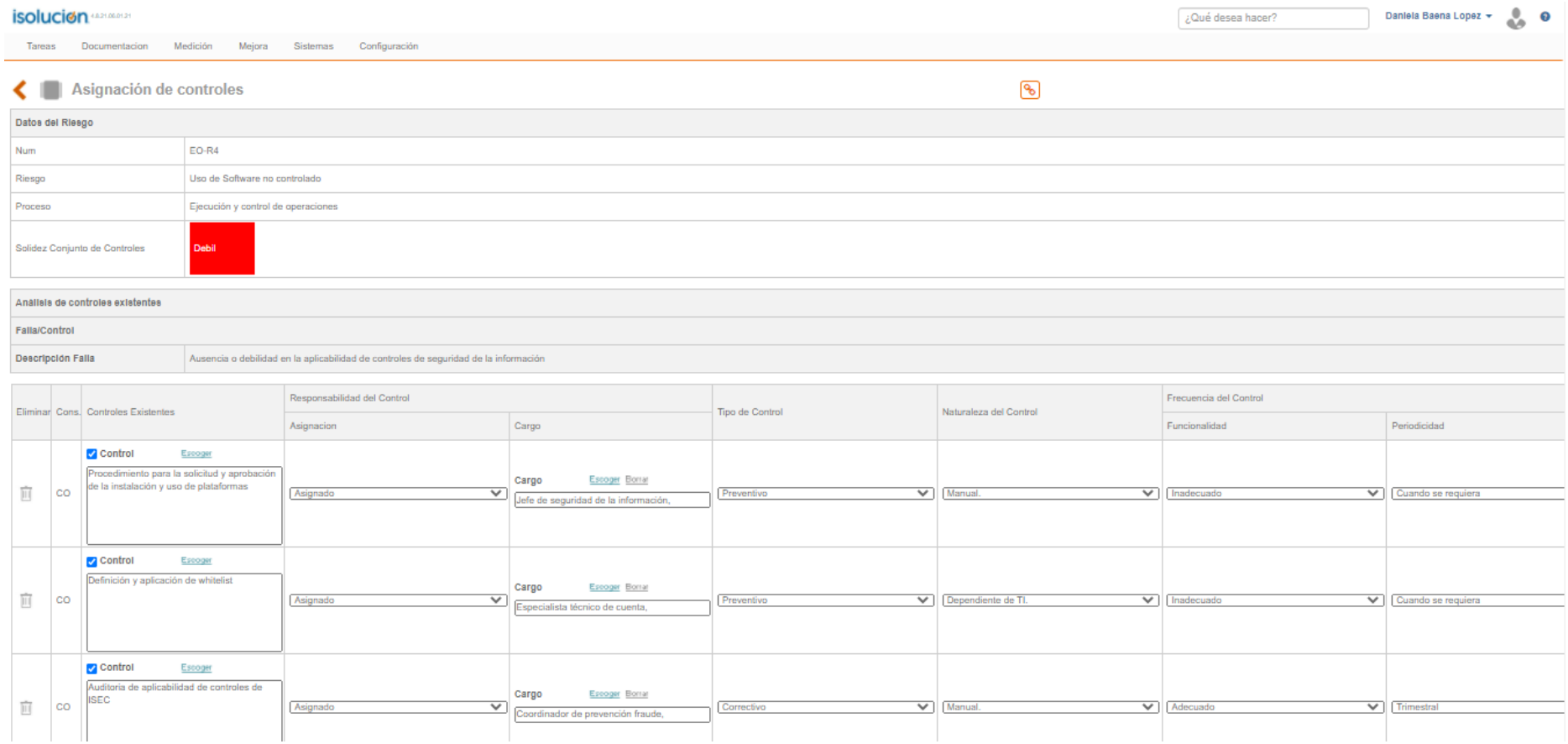
SERVICIOS		
Restaurantes Pagos	Supervisor Operaciones	USC
Reubicaciones	T2	Vacunación Empresarial
SAC	Tech Support I	Validación de documentos
SAC Técnico de cuenta (TAM)	Tech Support II	Vendedor
Salud Administrada	Tecnología	Ventas Entrantes
Salud Oral	Tecnología Informática	Ventas Salientes
SCSM	Tel Sell	Verifications
Sec (soporte experiencia al cliente)	Telefonía - Avaya	Viajes
Service	Telegestion	Vip
Vital comercial	VPN	Voice Specialist
Vital salud	Web	WFH
Vivienda	Web Center	Voice
VLAN	WF	Whatsapp
Workforce		

Anexo 13. Fase de Análisis del riesgo en ISOlución®.



Anexo 14. Fase de valoración del riesgo en ISOlución®.

Parte uno de la valoración del riesgo. Las capturas corresponden a ejemplos de riesgos carga



isolución

¿Qué desea hacer? Daniela Baena Lopez

Tareas Documentacion Medición Mejora Sistemas Configuración

Asignación de controles

Datos del Riesgo	
Num	EO-R4
Riesgo	Uso de Software no controlado
Proceso	Ejecución y control de operaciones
Solidez Conjunto de Controles	Debil

Analisis de controles existentes	
Falla/Control	
Descripción Falla	Ausencia o debilidad en la aplicabilidad de controles de seguridad de la información

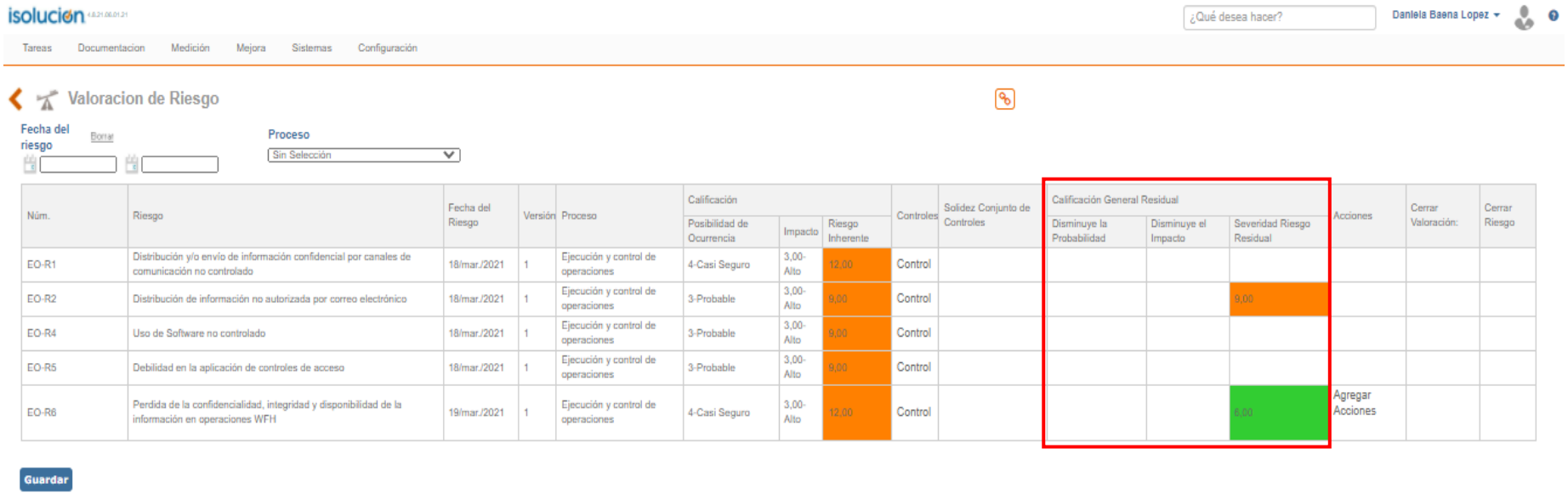
Eliminar	Cons.	Controles Existentes	Responsabilidad del Control		Tipo de Control	Naturaleza del Control	Frecuencia del Control	
			Asignacion	Cargo			Funcionalidad	Periodicidad
	CO	Control Escoger: Procedimiento para la solicitud y aprobación de la instalación y uso de plataformas	Asignado	Cargo Escoger Borrar: Jefe de seguridad de la información,	Preventivo	Manual.	Inadecuado	Cuando se requiera
	CO	Control Escoger: Definición y aplicación de whitelist	Asignado	Cargo Escoger Borrar: Especialista técnico de cuenta,	Preventivo	Dependiente de TI.	Inadecuado	Cuando se requiera
	CO	Control Escoger: Auditoria de aplicabilidad de controles de ISEC	Asignado	Cargo Escoger Borrar: Coordinador de prevención fraude,	Correctivo	Manual.	Adecuado	Trimestral

Parte dos de valoración del riesgo. Las capturas corresponden a ejemplos de riesgos cargados.

Documentación del Control		Evidencia que Compone el Control.		Diseño del Control	Observaciones frente al diseño del Control	Ejecución del Control	Solidez individual del Control	Importancia del Control
Documentacion	ReferenciaDocumental	Evidencia	Descripcion					
No Documentado.		Adecuadas	Solicitud del TAM a ISEC	Debil	SI	Debil	Debil	Importante
No Documentado.		Adecuadas	Whitelist de la cuenta	Debil	SI	Debil	Debil	Importante
Documentado	Prevención Fraude, Borrar Escoger	Adecuadas	Matriz de auditoria prevención fraude	Moderado	SI	Fuerte	Moderado	Importante
Sin Selección	Borrar Escoger	Sin Selección				Sin Selección		Sin Selección

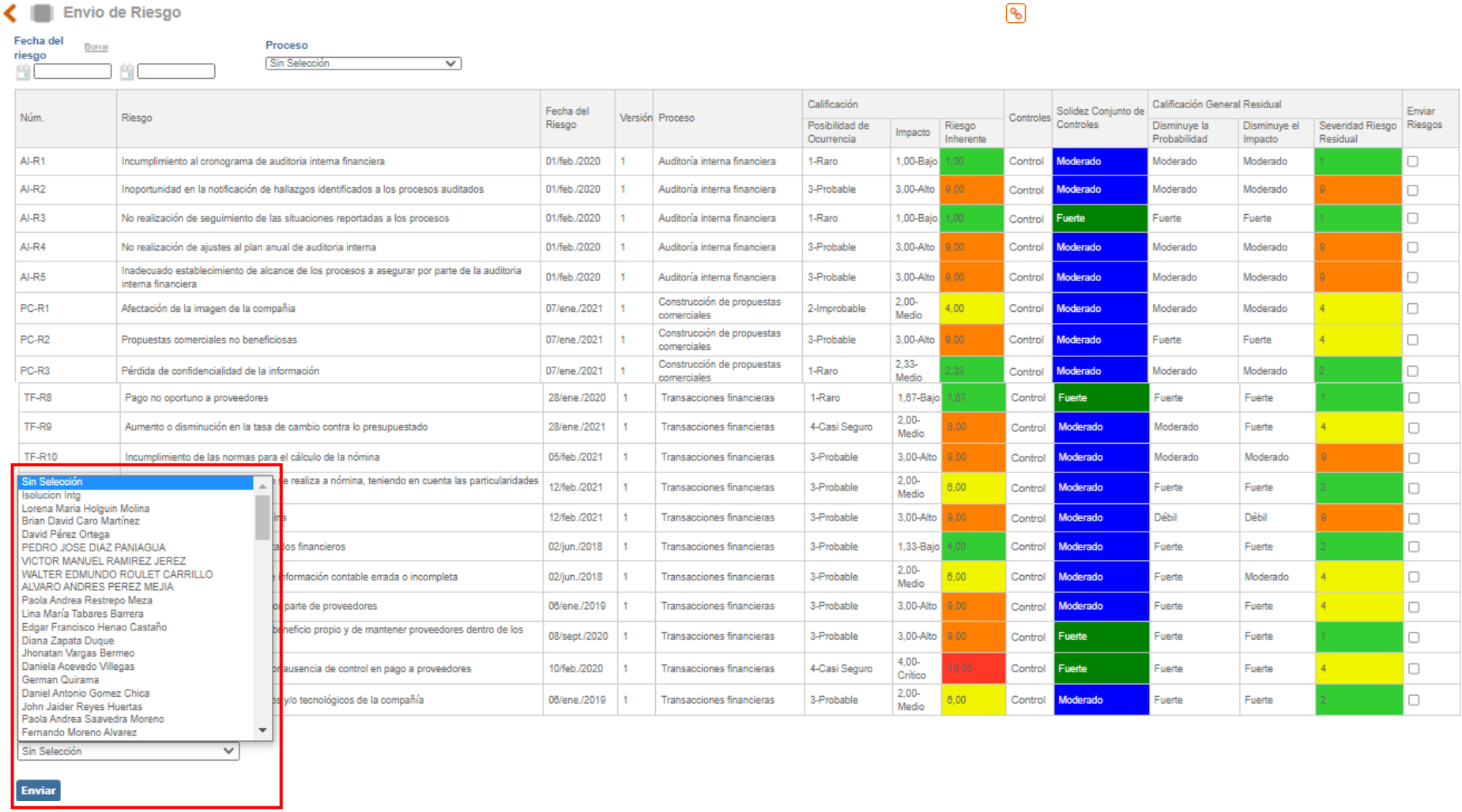
Anexo 15. Calificación general residual en ISOlución®.

Las capturas corresponden a ejemplos de riesgos cargados



Núm.	Riesgo	Fecha del Riesgo	Versión	Proceso	Calificación			Controles	Solidez Conjunto de Controles	Calificación General Residual			Acciones	Cerrar Valoración:	Cerrar Riesgo
					Posibilidad de Ocurrencia	Impacto	Riesgo Inherente			Disminuye la Probabilidad	Disminuye el Impacto	Severidad Riesgo Residual			
EO-R1	Distribución y/o envío de información confidencial por canales de comunicación no controlado	18/mar./2021	1	Ejecución y control de operaciones	4-Casi Seguro	3,00-Alto	12,00	Control							
EO-R2	Distribución de información no autorizada por correo electrónico	18/mar./2021	1	Ejecución y control de operaciones	3-Probable	3,00-Alto	9,00	Control				9,00			
EO-R4	Uso de Software no controlado	18/mar./2021	1	Ejecución y control de operaciones	3-Probable	3,00-Alto	9,00	Control							
EO-R5	Debilidad en la aplicación de controles de acceso	18/mar./2021	1	Ejecución y control de operaciones	3-Probable	3,00-Alto	9,00	Control							
EO-R6	Perdida de la confidencialidad, integridad y disponibilidad de la información en operaciones WFH	19/mar./2021	1	Ejecución y control de operaciones	4-Casi Seguro	3,00-Alto	12,00	Control				6,00	Agregar Acciones		

Anexo 16. Envío y revisión de los riesgos en ISOlución®.



Envio de Riesgo

Fecha del riesgo Borrar

Proceso: Sin Selección

Núm.	Riesgo	Fecha del Riesgo	Versión	Proceso	Calificación			Controles	Solidez Conjunto de Controles	Calificación General Residual			Enviar Riesgos
					Posibilidad de Ocurrencia	Impacto	Riesgo Inherente			Disminuye la Probabilidad	Disminuye el Impacto	Severidad Riesgo Residual	
AI-R1	Incumplimiento al cronograma de auditoria interna financiera	01/feb./2020	1	Auditoría interna financiera	1-Raro	1,00-Bajo	1,00	Control	Moderado	Moderado	Moderado	1	
AI-R2	Inoportunidad en la notificación de hallazgos identificados a los procesos auditados	01/feb./2020	1	Auditoría interna financiera	3-Probable	3,00-Alto	9,00	Control	Moderado	Moderado	Moderado	9	
AI-R3	No realización de seguimiento de las situaciones reportadas a los procesos	01/feb./2020	1	Auditoría interna financiera	1-Raro	1,00-Bajo	1,00	Control	Fuerte	Fuerte	Fuerte	1	
AI-R4	No realización de ajustes al plan anual de auditoria interna	01/feb./2020	1	Auditoría interna financiera	3-Probable	3,00-Alto	9,00	Control	Moderado	Moderado	Moderado	9	
AI-R5	Inadecuado establecimiento de alcance de los procesos a asegurar por parte de la auditoria interna financiera	01/feb./2020	1	Auditoría interna financiera	3-Probable	3,00-Alto	9,00	Control	Moderado	Moderado	Moderado	9	
PC-R1	Afectación de la imagen de la compañia	07/ene./2021	1	Construcción de propuestas comerciales	2-Improbable	2,00-Medio	4,00	Control	Moderado	Moderado	Moderado	4	
PC-R2	Propuestas comerciales no beneficiosas	07/ene./2021	1	Construcción de propuestas comerciales	3-Probable	3,00-Alto	9,00	Control	Moderado	Fuerte	Fuerte	4	
PC-R3	Pérdida de confidencialidad de la información	07/ene./2021	1	Construcción de propuestas comerciales	1-Raro	2,33-Medio	2,33	Control	Moderado	Moderado	Moderado	2	
TF-R8	Pago no oportuno a proveedores	28/ene./2020	1	Transacciones financieras	1-Raro	1,67-Bajo	1,67	Control	Fuerte	Fuerte	Fuerte	1	
TF-R9	Aumento o disminución en la tasa de cambio contra lo presupuestado	28/ene./2021	1	Transacciones financieras	4-Casi Seguro	2,00-Medio	8,00	Control	Moderado	Moderado	Fuerte	4	
TF-R10	Incumplimiento de las normas para el cálculo de la nómina	05/feb./2021	1	Transacciones financieras	3-Probable	3,00-Alto	9,00	Control	Moderado	Moderado	Moderado	9	
	e realiza a nómina, teniendo en cuenta las particularidades	12/feb./2021	1	Transacciones financieras	3-Probable	2,00-Medio	6,00	Control	Moderado	Fuerte	Fuerte	2	
		12/feb./2021	1	Transacciones financieras	3-Probable	3,00-Alto	9,00	Control	Moderado	Débil	Débil	9	
	os financieros	02/jun./2018	1	Transacciones financieras	3-Probable	1,33-Bajo	4,00	Control	Moderado	Fuerte	Fuerte	2	
	formación contable errada o incompleta	02/jun./2018	1	Transacciones financieras	3-Probable	2,00-Medio	6,00	Control	Moderado	Fuerte	Moderado	4	
	parte de proveedores	06/ene./2019	1	Transacciones financieras	3-Probable	3,00-Alto	9,00	Control	Moderado	Fuerte	Fuerte	4	
	neficio propio y de mantener proveedores dentro de los	08/sept./2020	1	Transacciones financieras	3-Probable	3,00-Alto	9,00	Control	Fuerte	Fuerte	Fuerte	1	
	ausencia de control en pago a proveedores	10/feb./2020	1	Transacciones financieras	4-Casi Seguro	4,00-Crítico	16,00	Control	Fuerte	Fuerte	Fuerte	4	
	y/o tecnológicos de la compañía	06/ene./2019	1	Transacciones financieras	3-Probable	2,00-Medio	6,00	Control	Moderado	Fuerte	Fuerte	2	

Sin Selección
Isolucion Intg
Lorena Maria Holguin Molina
Brian David Caro Martínez
David Pérez Ortega
PEDRO JOSE DIAZ PANIAGUA
VICTOR MANUEL RAMIREZ JEREZ
WALTER EDMUNDO ROULET CARRILLO
ALVARO ANDRES PEREZ MEJIA
Paola Andrea Restrepo Meza
Lina María Tabares Barrera
Edgar Francisco Henao Castaño
Diana Zapata Duque
Jhonatan Vargas Bermeo
Daniela Acevedo Villegas
German Quirama
Daniel Antonio Gomez Chica
John Jaider Reyes Huertas
Paola Andrea Saavedra Moreno
Fernando Moreno Alvarez

Sin Selección

Enviar

Anexo 17. Ficha del riesgo.

Todas estas imágenes representan la ficha final del riesgo y es visualizada por la persona que se le asigna el riesgo o quien realice el cargue de información.

Información Riesgo

Identificación del riesgo	
Proceso	Gestión de prevención de fraude
Código del Riesgo	GP-R2
Nombre del Riesgo	Fuga de información confidencial de los procesos de investigación
Fecha de creación	02/mar./2021
Fecha del riesgo	18/dic./2019
Responsable	Daniela Baena Lopez
Tipo de Riesgo	Riesgo de Seguridad de la Información
Objetivo	Prevenir, detectar e investigar las conductas del recurso humano para mitigar los riesgos de fraude interno y externo.
Riesgo Relacionado	
Área	Prevención Fraude
Factor de Riesgo	Recursos Humanos
Afecta la continuidad del negocio	No
Falla	Conflicto de interés,Divulgación no autorizada de información confidencial
Activos	Matriz de Prevención de Fraude,Pruebas de Polígrafo,Estudios de Seguridad
Clasificacion Información	Confidencial
Anexos	

Análisis del riesgo	
Posibilidad de ocurrencia	1 - Raro
Impacto	3 - Alto
Calificación	Bajo
Evaluación	Bajo
Medidas de respuesta	Compartir o transferir el riesgo Evitar el riesgo Reducir el riesgo

Todas estas imágenes representan la ficha final del riesgo y es visualizada por la persona que se le asigna el riesgo o quien realice el cargue de información.

Fallas	
Código	158
Descripción	Conflicto de interés

Controles

Código del Control	Descripción del Control	Responsabilidad del Control		Tipo de Control	Naturaleza del Control	Frecuencia del Control		Documentación del Control		Evidencia que Compone el Control.		Diseño del Control	Ejecución del Control	Solidez Individual del Control	Importancia del Control
		Asignacion	Cargo			Funcionalidad	Periodicidad	Documentacion	ReferenciaDocumental	Evidencia	Descripcion				
7.1.2	Términos y condiciones del empleo	Asignado	Analista de prevención fraude Coordinador de prevención fraude Jefe de prevención fraude Supervisor de prevención fraude	Preventivo	Manual.	Adecuado	Cuando se requiera	Documentado	Anexo de confidencialidad propiedad intelectual conflicto de interes, vigilancia y control	Adecuadas	Contrato de los increybles	Fuerte	Fuerte	Fuerte	Importante
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Asignado	Analista de prevención fraude Coordinador de prevención fraude Jefe de prevención fraude Supervisor de prevención fraude	Preventivo	Manual.	Adecuado	Anual	Documentado	Aceptación código de ética colaborador Seguridad de la información	Adecuadas	Lista de aplicación de cada uno de los cursos	Fuerte	Fuerte	Fuerte	Importante

Código	169
Descripción	Divulgación no autorizada de información confidencial

Controles

Código del Control	Descripción del Control	Responsabilidad del Control		Tipo de Control	Naturaleza del Control	Frecuencia del Control		Documentación del Control		Evidencia que Compone el Control.		Diseño del Control	Ejecución del Control	Solidez Individual del Control	Importancia del Control
		Asignacion	Cargo			Funcionalidad	Periodicidad	Documentacion	ReferenciaDocumental	Evidencia	Descripcion				
9.1.2	Acceso a redes y a servicios en red	Asignado	Analista de prevención fraude Coordinador de prevención fraude Jefe de prevención fraude Supervisor de prevención fraude	Preventivo	Dependiente de TI.	Adecuado	Cuando se requiera	Documentado	Control de accesos	Adecuadas	Listado de las personas con acceso al Sharepoint	Fuerte	Fuerte	Fuerte	Importante
7.1.2	Términos y condiciones del empleo	Asignado	Analista de prevención fraude Coordinador de prevención fraude Jefe de prevención fraude Supervisor de prevención fraude	Preventivo	Manual.	Adecuado	Cuando se requiera	Documentado	Anexo de confidencialidad propiedad intelectual conflicto de interes, vigilancia y control	Adecuadas	Contrato de los increybles	Fuerte	Fuerte	Fuerte	Importante
12.1.1	Procedimientos de operación documentados	Asignado	Analista de prevención fraude Coordinador de prevención fraude Jefe de prevención fraude Supervisor de prevención fraude	Preventivo	Manual.	Adecuado	Diario	Documentado	Prevención Fraude	Adecuadas	Formatos, registros, matrices, correor,entre otros	Fuerte	Fuerte	Fuerte	Importante

Todas estas imágenes representan la ficha final del riesgo y es visualizada por la persona que se le asigna el riesgo o quien realice el cargue de información

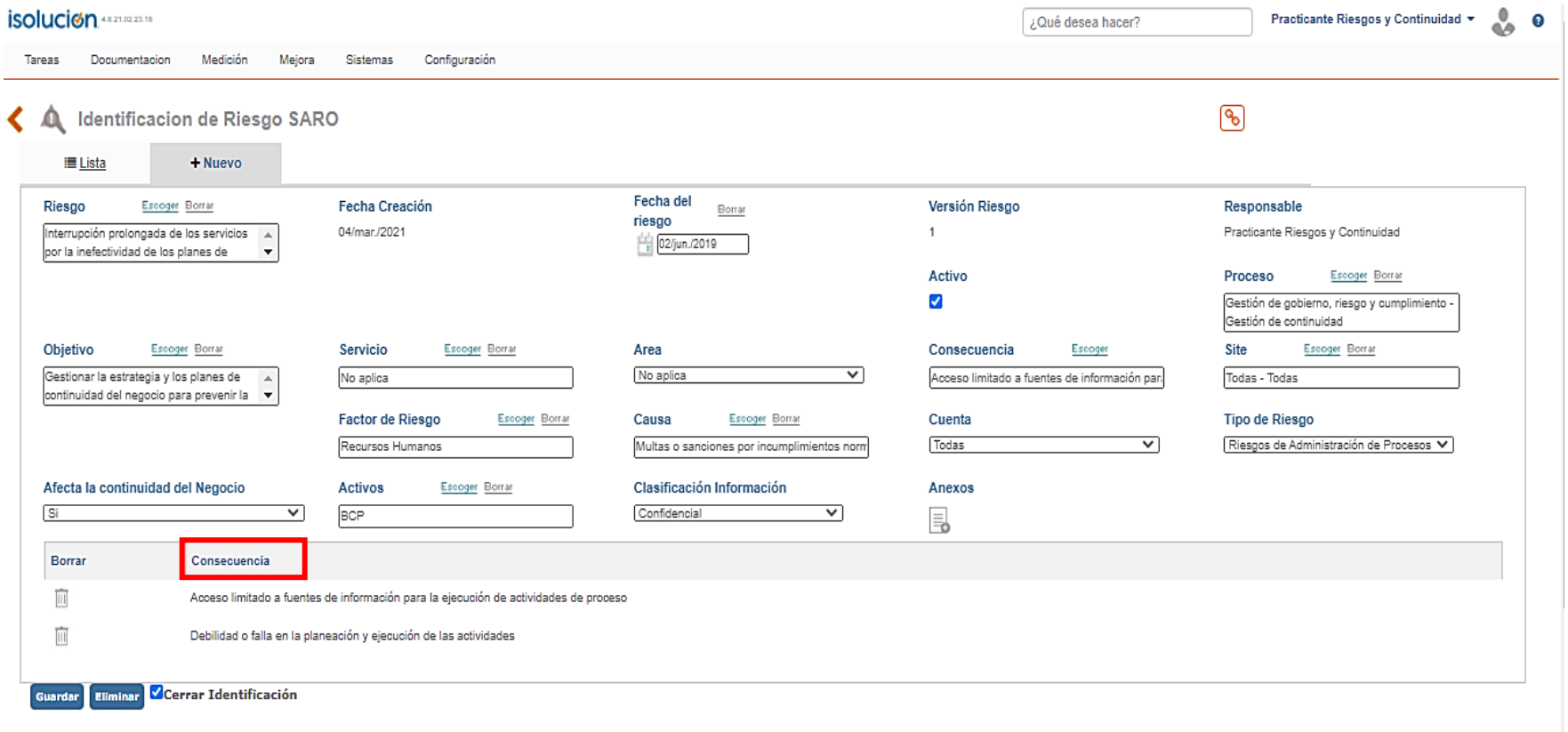
Valoración del riesgo	
Solidez Conjunto de controles	Fuerte
Disminuye la Probabilidad	Fuerte
Disminuye el Impacto	Fuerte
Severidad Riesgo Residual	
Acciones	

Anexo 18. Generación de versión del riesgo en ISOlución®.

Sel.	Num.	Riesgo	Versión	Fecha del Riesgo	Proceso	Descripción	Razón
☐	CN-R2	Entrega inoportuna de las estrategias de continuidad	1	07/jul./2020	Gestión de continuidad	Entrega inoportuna de las estrategias de continuidad	
☐	CN-R3	Estrategias de continuidad erradas o no efectivas	1	07/jul./2020	Gestión de continuidad	Estrategias de continuidad erradas o no efectivas	
☐	CN-R4	Pérdida de confidencialidad de la información	1	07/jul./2020	Gestión de continuidad	Pérdida de confidencialidad de la información	
☐	SI-R1	Inadecuada definición de las políticas de gestión de accesos	1	02/jun./2018	Gestión de la seguridad de la información	Inadecuada definición de las políticas de gestión de accesos	
☐	SI-R2	Perdida de la disponibilidad, integridad y confidencialidad de la información almacenada en SharePoint OL	1	10/ago./2020	Gestión de la seguridad de la información	Perdida de la disponibilidad, integridad y confidencialidad de la información almacenada en SharePoint OL	
☐	SI-R3	Debilidad en la gestión de vulnerabilidades de seguridad de la información	1	02/jun./2018	Gestión de la seguridad de la información	Debilidad en la gestión de vulnerabilidades de seguridad de la información	
☐	SI-R4	Inadecuada gestión del SGSI en la compañía	1	02/jun./2018	Gestión de la seguridad de la información	Inadecuada gestión del SGSI en la compañía	

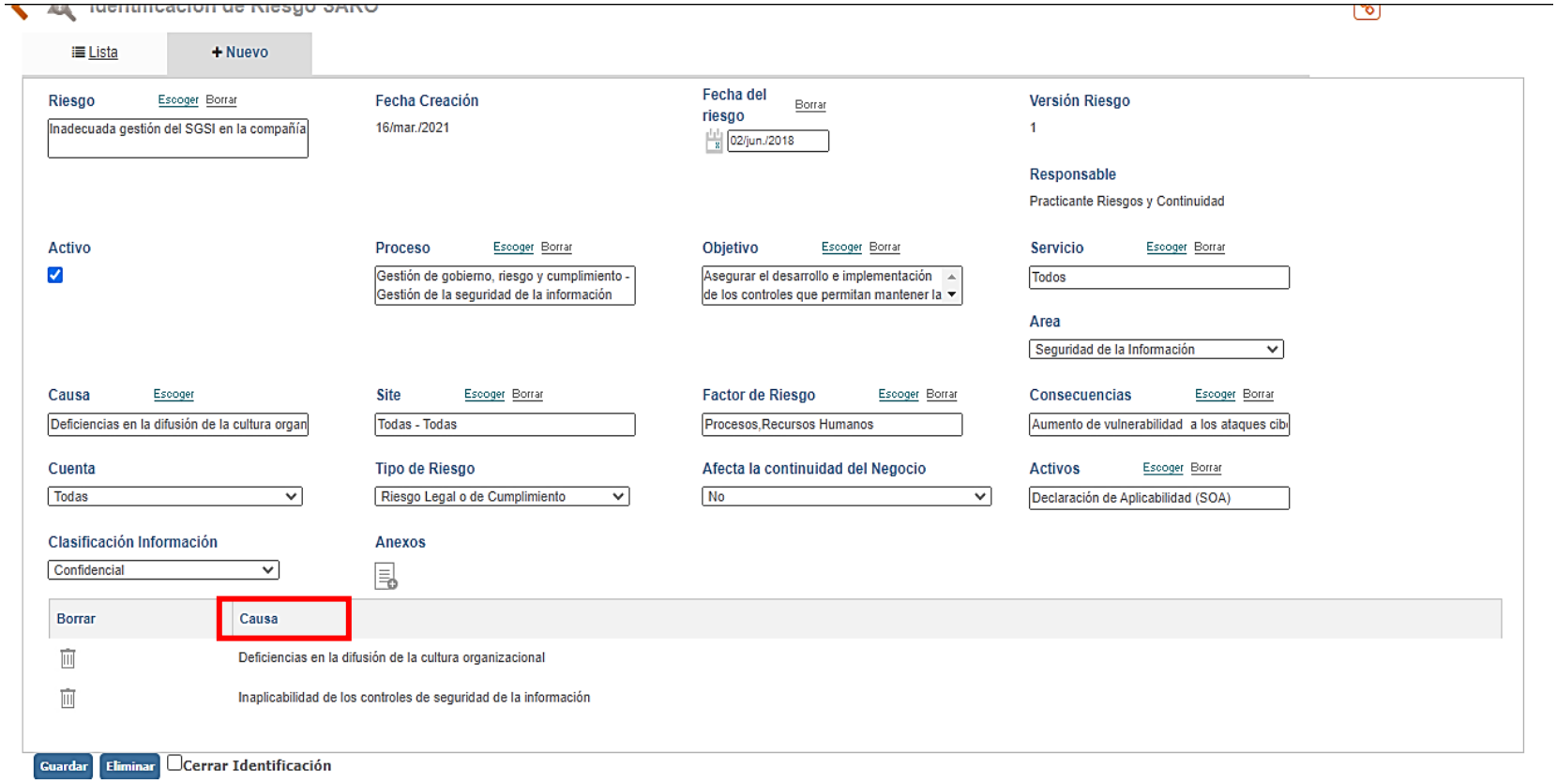
Anexo 19. Fase identificación ISOlución® enfocado a seguridad de la información.

Podemos observar que en lugar de llamar a las causas tiene en cuenta las consecuencias debido a que esta enfocado al módulo de seguridad de la información.

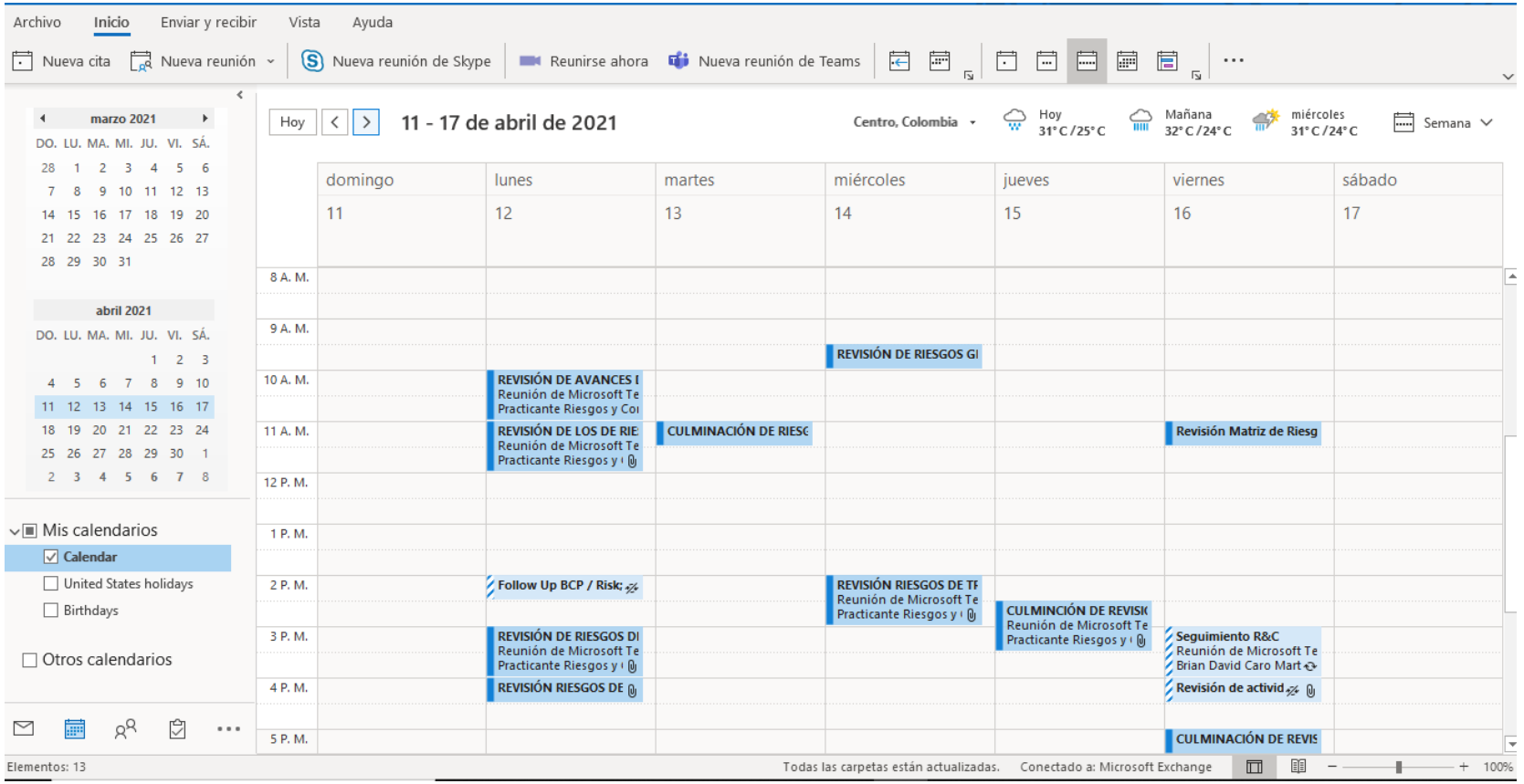


Anexo 20. Fase de identificación ISOlución® enfocado a riesgo Saro.

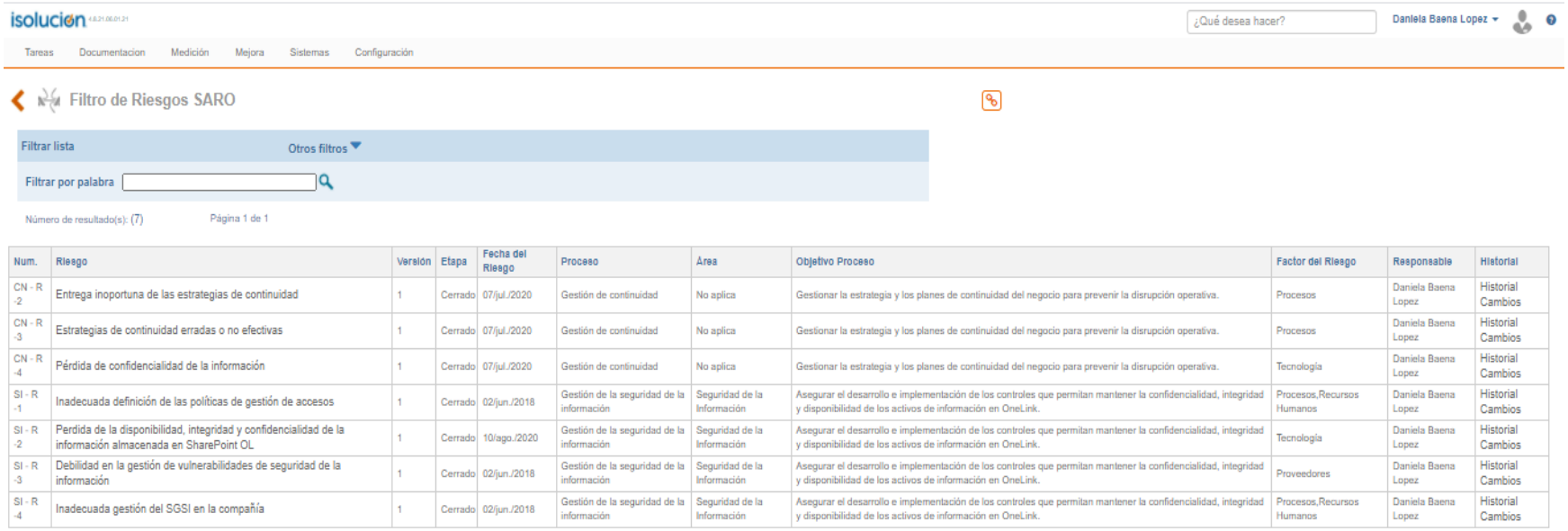
Podemos observar que ahora si son las causas las que nos muestra en la parte de abajo que corresponde a los items que seran aplicados los controles para mitigar o eliminar la materialización de los riesgos.



Anexo 21. Ejemplo de agendamiento de reuniones.

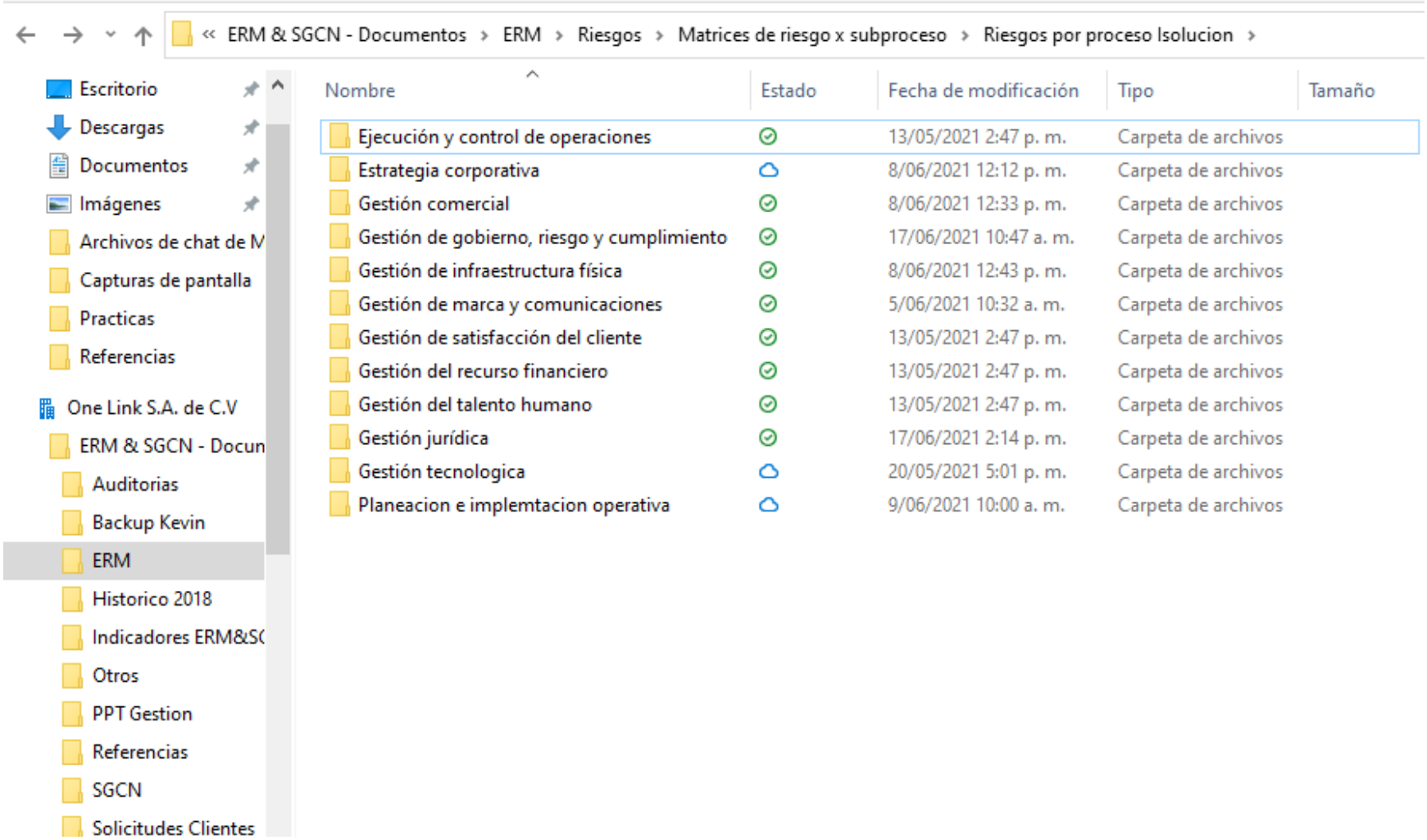


Anexo 22. Envío de riesgos.



Num.	Riesgo	Versión	Etapa	Fecha del Riesgo	Proceso	Área	Objetivo Proceso	Factor del Riesgo	Responsable	Historial
CN - R -2	Entrega inoportuna de las estrategias de continuidad	1	Cerrado	07/jul./2020	Gestión de continuidad	No aplica	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	Procesos	Daniela Baena Lopez	Historial Cambios
CN - R -3	Estrategias de continuidad erradas o no efectivas	1	Cerrado	07/jul./2020	Gestión de continuidad	No aplica	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	Procesos	Daniela Baena Lopez	Historial Cambios
CN - R -4	Pérdida de confidencialidad de la información	1	Cerrado	07/jul./2020	Gestión de continuidad	No aplica	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	Tecnología	Daniela Baena Lopez	Historial Cambios
SI - R -1	Inadecuada definición de las políticas de gestión de accesos	1	Cerrado	02/jun./2018	Gestión de la seguridad de la información	Seguridad de la Información	Asegurar el desarrollo e implementación de los controles que permitan mantener la confidencialidad, integridad y disponibilidad de los activos de información en OneLink.	Procesos,Recursos Humanos	Daniela Baena Lopez	Historial Cambios
SI - R -2	Perdida de la disponibilidad, integridad y confidencialidad de la información almacenada en SharePoint OL	1	Cerrado	10/ago./2020	Gestión de la seguridad de la información	Seguridad de la Información	Asegurar el desarrollo e implementación de los controles que permitan mantener la confidencialidad, integridad y disponibilidad de los activos de información en OneLink.	Tecnología	Daniela Baena Lopez	Historial Cambios
SI - R -3	Debilidad en la gestión de vulnerabilidades de seguridad de la información	1	Cerrado	02/jun./2018	Gestión de la seguridad de la información	Seguridad de la Información	Asegurar el desarrollo e implementación de los controles que permitan mantener la confidencialidad, integridad y disponibilidad de los activos de información en OneLink.	Proveedores	Daniela Baena Lopez	Historial Cambios
SI - R -4	Inadecuada gestión del SGSI en la compañía	1	Cerrado	02/jun./2018	Gestión de la seguridad de la información	Seguridad de la Información	Asegurar el desarrollo e implementación de los controles que permitan mantener la confidencialidad, integridad y disponibilidad de los activos de información en OneLink.	Procesos,Recursos Humanos	Daniela Baena Lopez	Historial Cambios

Anexo 23. Riesgos por proceso, subproceso y área.



Anexo 24. Certificado del curso Seguridad Corporativa Básico.

La empresa OneLink Colombia S.AS. contaba con una plataforma de capacitación llamada Litmos en la cual lleve a cabo los cursos de Seguridad Corporativa y Gestión de Riesgos referentes al área y otros relacionados con la empresa o su cultura organizacional; estos fueron realizados previo al desarrollo de mis funciones en la compañía. Sin embargo, esta plataforma no contaba con la opción de obtención de certificados, por lo cual, al momento de ser reemplazada por OneUniversity debí llevar a cabo de nuevo los cursos. En esta última se dictan cursos y capacitaciones en diferentes cargos con el propósito de impartir teorías y dar los recursos necesarios para lograr un excelente desempeño dentro del cargo. Por consecuente, en cumplimiento a la asignación de cursos realice el curso referente a Seguridad Corporativa Básico

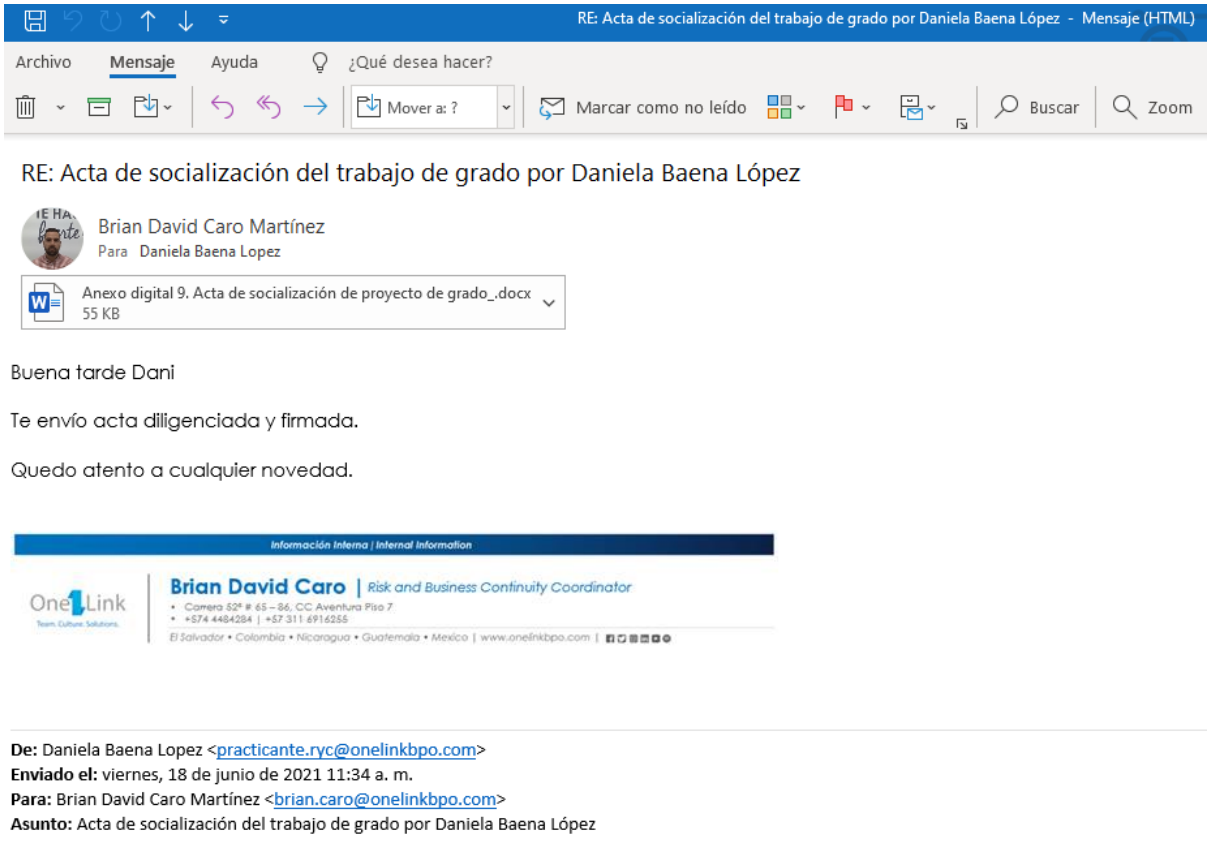
Certificado
de culminación de Nivel "Básico"

ONE LINK Certifica que Practicante Riesgos y Continuidad concluyó el 22 de mayo de 2021 el curso SEGURIDAD CORPORATIVA - BÁSICO equivalente al nivel básico y acumula 5 links educativos.

Andrea Ibarguen
Chief Human Resources Office

En este anexo se observa la evidencia de la realización del curso y fue expedido con el nombre de Practicante de Riesgos y Continuidad debido a que es el rol que tengo en la plataforma actualmente por ser genérico para la licencia. Este curso incluye un módulo de Seguridad De La Información, Gestión de Riesgos, Gestión de Continuidad de Negocio y Sistema de Gestión Integral.

Anexo 25. Evidencia de socialización proyecto de grado.



RE: Acta de socialización del trabajo de grado por Daniela Baena López - Mensaje (HTML)

Archivo Mensaje Ayuda ¿Qué desea hacer?

Mover a: ? Marcar como no leído Buscar Zoom

RE: Acta de socialización del trabajo de grado por Daniela Baena López

Brian David Caro Martínez
Para Daniela Baena Lopez

Anexo digital 9. Acta de socialización de proyecto de grado_.docx
55 KB

Buena tarde Dani

Te envío acta diligenciada y firmada.

Quedo atento a cualquier novedad.

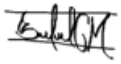
Información Interna | Internal Information

Brian David Caro | Risk and Business Continuity Coordinator
Carrera 52ª # 65 – 86, CC Aventura Piso 7
+574 4484284 | +57 311 6916255
El Salvador • Colombia • Nicaragua • Guatemala • Mexico | www.onelinkbpo.com

De: Daniela Baena Lopez <practicante.ryc@onelinkbpo.com>
Enviado el: viernes, 18 de junio de 2021 11:34 a. m.
Para: Brian David Caro Martínez <brian.caro@onelinkbpo.com>
Asunto: Acta de socialización del trabajo de grado por Daniela Baena López

Anexo 26. Acta de socialización proyecto de grado.

One1Link Team. Culture. Solutions.	Documento: ACTA DE SOCIALIZACIÓN DE PROYECTO DE GRADO Y ENTREGABLES Responsable: Daniela Baena López	Versión: 01 Fecha de Emisión: 18/06/2021

Fecha: 18/06/ 2021	Modalidad de reunión: Virtual	Medio: Microsoft Teams
OBJETIVO		
Socialización del proyecto de grado basado en la implementación del módulo de riesgos en Isolución.		
RESPONSABLE		
Daniela Baena López		
TEMAS A DESARROLLAR		
Presentación del proyecto de grado, entrega de formatos, plantillas y guías, socialización del alcance del proyecto y resultados.		
NOMBRE Y FIRMA DE LOS ASISTENTES		
Nombre completo	**Cargo**	**N° de cédula**	**Firma**
Brian David Caro Martinez	Coord. Riesgos y continuidad de negocio	1018424730	

Observaciones: Se llevo a cabo la socialización con éxito.

Anexo 27. Ejemplo riesgo en Excel.

a. Fase de identificación del riesgo

FASE DE IDENTIFICACIÓN DEL RIESGO															
PROCESO	SUBPROCESO	OBJETIVO	ÁREA/UNIDAD DE NEGOCIO	SITE	CUENTA	SERVICIO	FECHA DEL RIESGO (DD/MM/AA)	NOMBRE RIESGO	CAUSA	CONSECUENCIA	FACTORES	TIPO DE RIESGO	CONTINUIDAD NEGOCIO	ACTIVOS	CLASIFICACIÓN INFORMACIÓN
Gestión de gobierno riesgo y cumplimiento	Gestión de continuidad	Gestionar la estrategia y los planes de continuidad del negocio para prevenir la disrupción operativa.	No aplica	Todos	No aplica	No aplica	7/07/2020	Entrega inoportuna de las estrategias de continuidad	Dependencia de terceros	Multas o sanciones por incumplimientos normativos, legales y/o contractuales	Procesos	Riesgos de Administración de Procesos	No	BCP	Confidencial
									Personal insuficiente para ejecutar las actividades del proceso	Perdida de oportunidad en la Continuidad de Negocio				DRP Regional	
									Ausencia, desactualización, retraso o mala documentación de la información						
									Desactualización de contratos respecto a los servicios prestados por OneLink						

b. Fase análisis del riesgo

FASE ANÁLISIS DEL RIESGO												
INFORMACIÓN DEL RIESGO			TIPO DE EVENTO	ACTIVOS	PROBABILIDAD	IMPACTO			VALOR IMPACTO	IMPACTO	RIESGO INICIAL	EVALUACIÓN	MEDIDAS DE RESPUESTA
NUM	RIESGO	PROCESO				DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD					
CN-R-2	Entrega inoportuna de las estrategias de continuidad	Gestión de gobierno riesgo y cumplimiento	Riesgos de Administración de Procesos	BCP	Probable	Media	Baja	Baja	1	Bajo	3	Bajo	Asumir el riesgo,Compartir o transferir el riesgo,Evitar el riesgo, Reducir el riesgo

c. Fase de valoración del riesgo

VALORACIÓN DEL RIESGO																	CALIFICACIÓN GENERAL RESIDUAL		
CONTROLES EXISTENTES	RESPONSABILIDAD DEL CONTROL		TIPO DE CONTROL	NATURALEZA DEL CONTROL	FRECUENCIA DEL CONTROL		DOCUMENTACIÓN DEL CONTROL		EVIDENCIA QUE COMPONE EL CONTROL		DISEÑO DEL CONTROL	OBSERVACIONES FRENTE AL DISEÑO DEL CONTROL	EJECUCIÓN DEL CONTROL	SOLIDEZ INDIVIDUAL DEL CONTROL	IMPORTANCIA DEL CONTROL	SOLIDEZ CONJUNTO DE CONTROLES	DISMINUYE LA PROBABILLIDAD	DISMINUYE EL IMPACTO	SEVERIDAD RIESGO RESIDUAL
	ASIGNACIÓN	CARGO			FUNCIONALIDAD	PERIODICIDAD	DOCUMENTACIÓN	REFERENCIA DOCUMENTAL	EVIDENCIA QUE COMPONE EL CONTROL	DESCRIPCIÓN									
Roles y responsabilidades del sistema	Asignado	Coordinador de riesgo y continuidad del negocio	Preventivo	Manual	Adecuado	Cuando se requiera	Documentado	Gestión de continuidad de negocio	Adecuada	Formato de los BCP	Fuerte	No	Moderado	Moderado	Importante	Moderado	Moderado	Moderado	3
Análisis de presupuesto	Asignado	Coordinador de riesgo y continuidad del negocio	Preventivo	Manual	Adecuado	Anual	No documentado		Adecuada	Correo de solicitud de información	Moderado	Si	Moderado	Moderado	Importante				
Seguimiento a la partes interesadas para verificar la documentación.	Asignado	Coordinador de riesgo y continuidad del negocio	Preventivo	Manual	Adecuado	Semanal	No documentado		Adecuada	Correo de solicitud de información	Moderado	Si	Moderado	Moderado	Importante				
Revisión de contrato y actualización del mismo	Asignado	Coordinador de riesgo y continuidad del negocio	Preventivo	Manual	Adecuado	Anual	No documentado		Adecuada	Indicadores de gestion SGCN y ERM	Moderado	Si	Moderado	Moderado	Importante				

Anexo 28. Instructivo matriz de riesgo en Excel.

a. Intructivo fase de identificación del riesgo.

INSTRUCCIONES PARA EL USO DE LA MATRIZ

Esta es una matriz que va ayudarte a llevar a cabo todo el análisis de riesgo y permite tener una homologación con cada uno de los campos de la plataforma Isolución.

Fase de identificación

En esta fase se da la identificación y definición de sucesos o eventos que se pueden presentar o producir en la organización, los cuales no pueden ser controlados.

Campo	Descripción	Clasificación - Navegación
Proceso	Selecciona **uno** de los procesos del listado	Proceso
Subproceso	Selecciona **uno** de los subprocesos del listado	Subproceso
Objetivo	Buscador para seleccionar el objetivo del proceso seleccionado anteriormente	Se escoge automáticamente
Área o unidad de negocio	Selecciona tu área del listado	Área
Site	Selecciona los site que abarquen el riesgo o escoge el país si incluye todos sus sites	Site
Cuenta	Escoge la cuenta correspondiente o un no aplica encaso que no lo sea	Cuentas
Servicio	Selecciona **uno o varios** servicios del listado que apliquen al riesgo	Servicios
Fecha del riesgo	Corresponde a la definición de la fecha en la cual se identificó el riesgo	día /mes /año
Nombre del riesgo	Escoge uno del listado, en caso de no encontrar uno crea un nuevo registro. Tener en cuenta que **NO** se debe mencionar causas, consecuencias o cualquier otro campo que no se refiera específicamente a lo que no se puede controlar (riesgo), por ejemplo, daños en la infraestructura física por desastres naturales (no escribir lo señalado en rojo)	Nombreriesgo
Causas	Selecciona **una o varias** causas del listado o genera un nuevo registro. Corresponden al ¿cómo puede suceder? **Ten en cuenta que se debe tener por lo menos un control por causa** y coloca una sola causa por celda	Causas
Consecuencias	Selecciona **una o varias** consecuencias del listado o genera un nuevo registro.Corresponden a los efectos que podría tener el riesgo en caso de su materialización	Consecuencias
Factores	Selecciona **uno o varios** factores. Es el elemento o conjunto de elementos que estando presentes en una actividad o proceso pueden desencadenar o disparar las causas que generan la materialización del riesgo.	Factores
Tipo de riesgo	Selecciona solo **un** tipo de riesgo. Son el conjunto de características que se evidencian en algún evento o situación que permiten ser enmarcados en un solo concepto.	Tipos_riesgos
Continuidad de negocio	¿Se ve afectada la continuidad del proceso al materializarse el riesgo?	Responde : Sí o No
Activos	En este se hace referencia a todos los activos de información relacionados a los riesgos, es decir, aquellos que sufrirían un efecto en caso de materialización del riesgo. **Recuerde que corresponde a los que fueron levantados por ustedes con el equipo de seguridad de la información y pertenecen a su proceso.**	Activos
Clasificación de la información	Seleccione **un solo tipo** de información. Se refiere al tipo de información contenida en el activo de información e inicialmente estaba definida como pública, interna o confidencial.	Clasificación_info

b. Intructivo fase de análisis del riesgo.

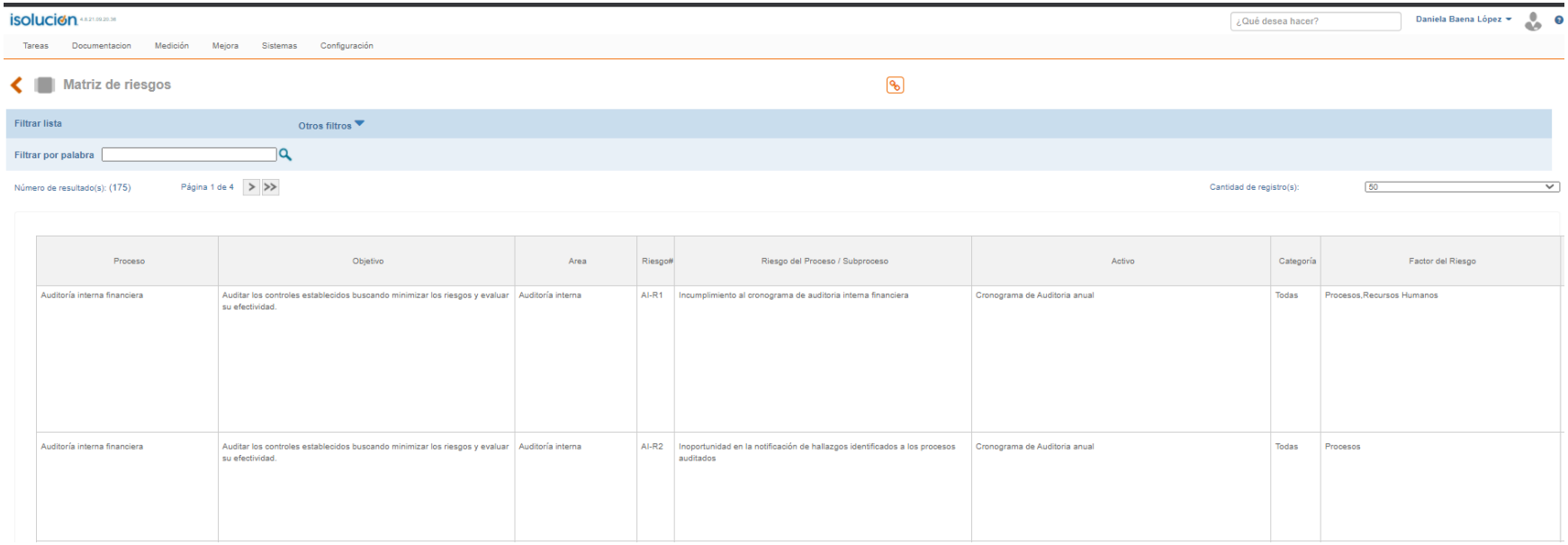
Fase de análisis del riesgo		
En esta fase se lleva acabo la valoración y priorización de los riesgos donde se hace la medición de probabilidad de ocurrencia de los riesgos y su impacto en caso de materializarse.		
Campo	**Descripción**	**Clasificación - Navegación**
Probabilidad	Seleccione **una sola** opción. Se entiende como la posibilidad de ocurrencia o materialización del riesgo	Probabilidad_ocurrencia
Impacto	Seleccione **una opción** para cada uno de los tres pilares. Se entiende como las perdidas y/o consecuencias a los tres pilares de la información de acuerdo con la disponibilidad, integridad y confidencialidad **previo a los controles que se tengan en el proceso.**	Impacto

c. Intructivo fase de valoración del riesgo.

Fase de valoración del riesgo			
En esta fase se identifican cada uno de los controles que mitigan o eliminan las causas establecidas en la identificación del riesgo, los cuales deben relacionarse directamente con cada una de las causas establecidas en el riesgo.			
Campo	**Descripción**	**Clasificación-Navegación**	
Controles existentes	Selecciones un control del listado o escriba el nombre del control SOA en caso de ser aplicable o describa si tiene un control operativo en su proceso.	Controles_ope	SOA
Responsabilidad del control	Una o varias personas encargadas por velar del cumplimiento del control.		
Cargo	Escoja el o los cargos responsables del listado.	Cargos	
Tipo de control	Seleccione **un solo** tipo de control. Corresponde a la evaluación de la acción.	Clasif_controles	
Naturaleza del control	Selección **un solo** tipo de naturaleza. Corresponde al tipo de control de acuerdo con la forma en que es ejecutado.	Naturaleza_control	
Funcionalidad	Seleccione **una opción**. Corresponde a como se encuentra el control actualmente, es decir, si se está llevando a cabo de forma adecuada o inadecuada.		
Periodicidad	Seleccione **una opción** que sea coherente con la periodicidad de las evidencias que se tendrían del control. Corresponde a la frecuencia con la cual se lleva a cabo el control.		
Documentación	Solo se encontrará documentado si existe el documento en la plataforma, en caso contrario seleccionar como no documentado.		
Referencia documental	Seleccione la referencia donde se encuentra documentado el control de acuerdo al listado, en caso de no encontrarla colocar como **no documentado**. Corresponde al soporte del control de acuerdo con la documentación que se encuentran dispuesta en la plataforma, es decir, solo puede estar documentando si ya existe un documento cargado en la plataforma. Suministra información para hacer la realización del control, estas son necesarias para los procesos de auditorías y sirven de prueba acerca del control.	Referencia_documental	
Evidencia que compone el control	Selecciones si las evidencias que se tienen de la ejecución del control si son adecuadas o inadecuadas teniendo en cuenta que estas serán necesarias como un soporte en posibles auditorias y deben ser coherente con la periodicidad.		
Descripción	Describa cada una de las evidencias como formatos, correos, solicitudes, procedimientos, entre otros.		
Ejecución del control	Selecciona una sola opción conforme a la aplicación del control y si este se lleva a cabo de forma fuerte, moderada o débil.	Ejecución_control	
Importancia del control	Debido a cuestiones de parametrización se decidió colocar **importante** en todos los casos.		
CALIFICACIÓN GENERAL RESIDUAL			
En esta fase se determina de forma subjetiva si los controles definidos disminuyen la probabilidad de ocurrencia del riesgo y su impacto. Obteniéndose de esta manera el nivel de riesgo que permanece en la organización tras mitigar, reducir o eliminar los riesgos (riesgo residual). Exige que se tomen medidas previas para que de manifestarse, su efecto sea mínimo.			
Campo	**Descripción**		
Disminuye la probabilidad	Seleccione **una opción** desde su punto de vista que responda si la aplicación de todos los controles definidos disminuye la probabilidad de ocurrencia del riesgo de forma débil, modera o fuerte.		
Disminuye el impacto	Seleccione **una opción** desde su punto de vista que responda si la aplicación de todos los controles definidos disminuye impacto del riesgo de forma débil, modera o fuerte.		

Anexo 29. Matriz de riesgo en ISOlución®.

En el siguiente anexo se muestra la matriz generada por ISOlución® para los riesgos y se muestra en diferentes imágenes debido a su extensión.



Proceso	Objetivo	Area	Riesgo#	Riesgo del Proceso / Subproceso	Activo	Categoría	Factor del Riesgo
Auditoría interna financiera	Auditar los controles establecidos buscando minimizar los riesgos y evaluar su efectividad.	Auditoría interna	AI-R1	Incumplimiento al cronograma de auditoria interna financiera	Cronograma de Auditoria anual	Todas	Procesos,Recursos Humanos
Auditoría interna financiera	Auditar los controles establecidos buscando minimizar los riesgos y evaluar su efectividad.	Auditoría interna	AI-R2	Inoportunidad en la notificación de hallazgos identificados a los procesos auditados	Cronograma de Auditoria anual	Todas	Procesos

Continuación de Matriz de riesgo en ISOlución®.

Consecuencias	Afecta la Continuidad del Negocio	Tipo de Riesgo	Probabilidad	Impacto	Severidad del Riesgo Inherente	Respuesta / Tratamiento de los riesgos	Causa o Falla	Control #
Inoportunidad en la notificación de riesgos,Materialización de riesgos,Falta de recursos (Humanos, tecnológicos, físicos , inmobiliarios, financieros,etc)	NO	Riesgos de Administración de Procesos	Raro	Bajo	1,00 - Bajo	Asumir el riesgo Compartir o transferir el riesgo Evitar el riesgo Reducir el riesgo	Asignación de presupuesto insuficiente	CO
							Cambio de prioridades de la administración a otras actividades	CO

Descripción del Control Asociado a la Causa o Falla	Responsabilidad del Control		Tipo de Control	Naturaleza del Control	Frecuencia del Control		Documentación del Control		Evidencia que Compone el Control.		Diseño de Control
	Asignacion	Cargo			Funcionalidad	Periodicidad	Documentacion	ReferenciaDocumental	Evidencia	Descripcion	
Análisis de presupuesto	Asignado	Gerente de Auditoria interna	Preventivo	Manual.	Adecuado	Anual	No Documentado.		Adecuadas	Correos electrónicos con la información de presupuesto	Moderado
Seguimiento recurrente a la plantilla de cronograma de Auditoria	Asignado	Gerente de Auditoria interna	Preventivo	Manual.	Adecuado	Anual	Documentado	Auditoria Interna Financiera	Adecuadas	Plantilla de cronograma de Auditoria (AI-T-F-003)	Fuerte

Observaciones frente al diseño del Control	Ejecución del Control	Solidez Individual del Control	Solidez del Conjunto de Controles	Disminuye Probabilidad	Disminuye Impacto	Riesgo Residual	Acciones
SI	Moderado	Moderado	Moderado	Moderado	Moderado	1 - Bajo	
NO	Moderado	Moderado					