INFORME DE ANÁLISIS DE BRECHA DE CONTINUIDAD DE NEGOCIO FRENTE A LA NORMA ISO 22301:2019

Medellín, octubre de 2024

CONTROLES DE VERSIONES DEL DOCUMENTO

Fecha	Versión	Descripción	Responsable	Cambios que generaron la siguiente versión
08/10/2024	V1	Elaboración del informe de análisis de brechas del SGCN frente a la norma ISO 22301:2019	ISeguras S.A.S.	

TABLA DE CONTENIDO

1. INTRODUCCIÓN 5
2. OBJETIVO DEL DIAGNOSTICO 5
3. RESULTADOS DEL DIAGNOSTICO 5
4. RESULTADO GENERAL DE LA IMPLEMENTACIÓN ISO 22301:2019 13
   4.1. Contexto Organizacional 14
   4.2. Liderazgo 15
   4.3. Planeación 15
   4.4. Soporte 17
   4.5. Operación 18
   4.6. Evaluación de desempeño 20
   4.7. Mejoramiento 21
5. CONCLUSIONES 21
6. BIBLIOGRAFIA 21
7. ANEXOS 22

ÍNDICE DE TABLAS

Tabla 1 Documentación de contexto 6
Tabla 2 Documentación de políticas 6
Tabla 3 Documentación de riesgos 6
Tabla 4 Documentación de BIA 6
Tabla 5 Estrategias de continuidad y recuperación 6
Tabla 6 Plan de continuidad del negocio 6
Tabla 7 Plan de recuperación de desastres 7
Tabla 8 Planes para manejo de crisis y procedimientos de recuperación 7
Tabla 9 Documentos de capacitación y sensibilización 7
Tabla 10 Documentación de indicadores 7
Tabla 11 Documentación de pruebas 8
Tabla 12 Documentación de nivel de madurez 8
Tabla 13 Documentación de eventos e incidentes 8
Tabla 14 Presentaciones 8
Tabla 15. Escala para valorar el nivel de madurez de los requisitos del SGCN 9
Tabla 16. Resumen de los requisitos de la norma ISO 22301:2019 13
Tabla 17. Nivel general de madurez frente a los requisitos de la norma ISO 22301:2019 13

ÍNDICE DE FIGURAS

Ilustración 1 Brechas identificadas en el SGCN del IDEA 14

1. INTRODUCCIÓN

La gestión de la continuidad del negocio es un grupo de procesos y procedimientos a lo largo y ancho de la entidad para asegurar el funcionamiento de los procesos críticos ante una interrupción. A su vez debe proporcionar planes para recuperarse de incidentes de menor importancia (por ejemplo: fallas localizadas en componentes de los procesos) a situaciones más severas ocasionadas por incendios, desastres naturales, fallas prolongadas de energía, ausencia de telecomunicaciones, ciberataques, daños en instalaciones de trabajo, entre otros.

En la literatura de gestión, el análisis de brechas implica la comparación del desempeño real con el desempeño potencial o deseado. Si una organización no hace el mejor uso de los recursos actuales, o renuncia a la inversión en capital o tecnología, puede generar productos por debajo de un potencial ideal.

En cuanto al SGCN el equipo consultor de Infraestructuras Seguras SAS realizó el **Análisis de brecha ISO 22301:2019,** para identificar la distancia existente entre las practicas actuales de continuidad del negocio del Instituto para el Desarrollo de Antioquia, en adelante IDEA y los requerimientos de la norma, y cuyos resultados se incluyen en este documento.

2. OBJETIVO DEL DIAGNOSTICO

Presentar el nivel de cumplimiento del IDEA de los requisitos establecidos en la norma ISO 22301:2019, la cual es reconocida internacionalmente para la gestión de los programas de continuidad del negocio. Específicamente se busca:

- Establecer el nivel de cumplimiento de cada uno de los requisitos de la norma.
- Identificar las principales brechas que debe abordar el IDEA para fortalecer su postura en lo relacionado con el Sistema de Gestión de Continuidad del Negocio (SGCN).

3. RESULTADOS DEL DIAGNOSTICO

La identificación de brechas respecto a la Norma ISO 22301:2019 en el IDEA tomo como punto de partida la documentación entregada al equipo consultor lo cual se complementó con entrevistas al área de riesgos y tecnología.

Documentación revisada:

Documentación de contexto
Organigrama.docx
Manual de funciones Director.pdf

Documentación de contexto
Procesos (Mapa de procesos y 15 caracterizaciones)
Resolución comité ciberseguridad 0004-2021.pdf
Resolución 0012-22 actualización manual de funciones profes especializado.pdf
Esquemático Infraestructura IDEA.pdf

Tabla 1 Documentación de contexto

Documentación de Políticas
Manual de política de seguridad de la información y ciberseguridad.pdf

Tabla 2 Documentación de políticas

Documentación de riesgos
Metodologías
Sistema de Administración de Riesgo - SARSIC.pdf
Manual SARO V07.pdf
Informe Análisis de Riesgos Continuidad Negocio RIA.pdf
Mapa-de-Riesgos-Ciberseguridad.xlsx
Mapas de riesgos Operativos.xlsx
Plan Tratamiento Riesgos de Seguridad y Privacidad Información - 2024.pdf

Tabla 3 Documentación de riesgos

Documentación de BIA
Informe de Análisis de Impacto al Negocio BIA.pdf
Anexo 1. Fuentes de Cambio.pdf
Anexo 2. Análisis Procesos Críticos.pdf
Anexo 3. Análisis Procesos No Críticos.pdf
Anexo 4. Servicios Tecnológicos.xlsx
Anexo 5. Proveedores.xlsx
Anexo 6. Cifras Análisis Cuantitativo.xlsx

Tabla 4 Documentación de BIA

Estrategias de continuidad y recuperación
Informe Estrategias Continuidad Negocio BCP-DRP.pdf

Tabla 5 Estrategias de continuidad y recuperación

Plan de continuidad del negocio (BCP)
Manual Plan Continuidad del Negocio V3 -2023 JD.pdf

Tabla 6 Plan de continuidad del negocio

Plan de recuperación de desastres DRP
Plan de Recuperación Ante Desastres DRP.pdf

Plan de recuperación de desastres DRP
Anexo 2. Requerimientos Técnicos Recuperación.xlsx
Anexo 3. Resumen del Plan DRP.pptx

Tabla 7 Plan de recuperación de desastres

Planes para manejo de crisis y procedimientos de recuperación
Plan Administración Fondos Especiales para Eventos de Interrupción.pdf
Plan de Comunicaciones en la Crisis.pdf
Plan Equipo Gerencial de Manejo de Crisis.pdf
Plan Gestión Documental para Eventos de Interrupción.pdf
Plan Gestión Financiera para Eventos de Interrupción.pdf
Plan Gestión Información Financiera para Eventos.pdf
Plan Gestión Jurídica para Eventos de Interrupción.pdf
Plan Gestión Tecnología Información Eventos.pdf
Plan Manejo de Incidentes Interrupción.pdf
Plan Otorgamiento Crédito para Eventos de Interrupción.pdf
Anexo 2. Plan de Contingencia Gestión Documental.pdf
Procedimiento Gestión de Incidentes de Seguridad - IDEA.pdf
Respaldo y restauración de información electrónica.pdf

Tabla 8 Planes para manejo de crisis y procedimientos de recuperación

Documentos de capacitación y sensibilización
Presentación -Material Soporte Jornadas de Sensibilización OCT 2022.pptx
Plan continuidad negocio capacitación feb 2023.pptx
Asistencia capacitación Presencial - Plan de Continuidad del Negocio Oct 24 y 25-2022.pdf
Asistencia capacitación Virtual Teams- Plan de Continuidad del Negocio Nov 22-2022.pdf
Material Soporte Jornadas de Capacitación - Video 1.mp4
Material Soporte Jornadas de Capacitación - Video 2.mp4
Publicación Intranet capacitacion.docx

Tabla 9 Documentos de capacitación y sensibilización

Documentación de indicadores
Anexo 2. Análisis Procesos Críticos.pdf
Anexo 3. Análisis Procesos No Críticos.pdf

Tabla 10 Documentación de indicadores

Documentación de pruebas
Informe Pruebas Continuidad de Negocio.pdf
Anexo 1. Actividades pruebas.xlsx
Anexo 2. Observaciones pruebas.pdf
Anexo 3. Reporte de Novedades Tecnología.xlsx

Documentación de pruebas
Anexo 4. Observaciones Participantes.pdf
Anexo 5. Informe Centro Alterno.pdf

Tabla 11 Documentación de pruebas

Documentación de nivel de madurez
Modelos de Madurez SGSI .xlsx

Tabla 12 Documentación de nivel de madurez

Documentación de eventos e incidentes
Activación plan de continuidad ago 29 2023.docx
Carta Incidencia 28 de agosto 2023 - Idea.pdf

Tabla 13 Documentación de eventos e incidentes

Presentaciones
PCN Comité de Gerencia may 2024.pptx
PCN Líderes de Procesos jun 2024.pptx

Tabla 14 Presentaciones

La norma se encuentra organizada en dos grandes secciones:

Generalidades: Comprende los numerales 1. Objeto y campo de aplicación, 2. Referencias Normativas y 3. Términos y Definiciones. Esta sección en sí no establece requisitos de un SGCN.
Requisitos de SGCN: Comprende los numerales 4 al 10 y presenta los requisitos de acuerdo con el ciclo PHVA (Planear, Hacer, Verificar, Actuar).

Se estableció el nivel de avance de cada uno de los requisitos especificados en las cláusulas de la 4 a la 10, los cuales son de obligatorio cumplimiento para demostrar conformidad con la Norma ISO 22301:2019. La escala utilizada para identificar el nivel de madurez de cada requisito fue la siguiente:

Nivel de Madurez	Puntaje	Descripción
1. Inicial	1 – 15	En el nivel de madurez 1 (Inicial), la organización se caracteriza por la naturaleza ad hoc de sus procesos. La organización no proporciona un entorno estable para la creación de sus productos, por lo que el éxito de sus proyectos depende exclusivamente de las habilidades de las personas dedicadas a cada uno de ellos.
2. Repetible	16 – 30	En el nivel de madurez 2 (Repetible), los proyectos de la organización realizan los procesos de acuerdo con lo planificado y definido en las políticas de la organización, empleando a personas capacitadas que poseen el conocimiento requerido, involucrando a todos los actores

Nivel de Madurez	Puntaje	Descripción
		relevantes, y monitoreando, controlando y revisando todos los procesos.
3. Definido	31 – 70	En el nivel de madurez 3 (Definido), todos los procesos son entendidos y descritos a través de estándares, procedimientos, herramientas y métodos.
4. Administrado	71 – 85	En el nivel de madurez 4 (Administrado), la organización y los proyectos establecen objetivos cuantitativos para medir la calidad de los procesos, así como su uso, y los criterios necesarios para su gestión. Se utilizan métodos estadísticos para controlar los procesos.
5. Optimizado	86 – 100	En el nivel de madurez 5 (Optimizado), la organización aplica la mejora continua de sus procesos a través de la comprensión cuantitativa de las causas de variación comunes al proceso, utilizando métodos estadísticos que avalan la mejora continua.

Tabla 15. Escala para valorar el nivel de madurez de los requisitos del SGCN

A continuación, se presenta un resumen de los requisitos evaluados:

Numeral	Aspectos que se evalúan
Numeral 4: Contexto de la organización	• El Objetivo de este capítulo es definir el Alcance del SGCN (Sistema de Gestión de la Continuidad del Negocio) y para ello se debe: **1.- Identificar los factores internos y externos que puedan ser afectados por una posible interrupción:** • Actividades de la Organización • Productos • Funciones • Servicios • Cadenas de suministro • Obligaciones Legales • Relaciones con Terceros • Otras **2.- Vincular y alinear Estratégicamente:** • Políticas de la Organización • Valores • Objetivos Estratégicos • Obligaciones Contractuales • Políticas de Gestión de Riesgos Laborales • Apetito al riesgo en la Organización.

Numeral	Aspectos que se evalúan
Numeral 5: Liderazgo	En este capítulo se definen los requisitos de la dirección de la entidad en cuanto a que debe asumir el liderazgo en las acciones de mantener, vigilar y dotar de recursos necesarios a la organización para garantizar el proceso de mejora continua. Las principales tareas de la dirección entre otras serán: • El SGCN debe formar parte de la Dirección estratégica • Garantizar los recursos necesarios para el SGCN • Comunicación a toda la empresa sobre la importancia del SGCN • Velar por el alcance de los resultados esperados • Apoyar el proceso de mejora continua • Establecer y comunicar la política de continuidad del negocio • Hay que asegurar que se establecen los objetivos y planes del SGCN • Hay que asegurar que se asignen las responsabilidades sobre el SGCN
Numeral 6: Planificación	En este capítulo se definen los Objetivos Estratégicos del SGCN como una expresión del propósito de la organización en el tratamiento de los riesgos identificados y el cumplimiento de los objetivos de la organización. Los principales objetivos del SGCN deben ser: • Estar alineados con la política de continuidad del negocio • Establecer el mínimo de productos y servicios con los que la organización alcanza sus objetivos. • Los objetivos deben ser medibles. • Los objetivos consideran requisitos aplicables • Deben ser controlados y revisados de forma periódica.
Numeral 7: Soporte	Los Recursos necesarios para la Gestión de la continuidad del negocio están contemplados en este capítulo. Estos recursos deben incluir: • Personal competente (en base a la formación específica recibida)

Numeral	Aspectos que se evalúan
	• Servicios de Soporte • Recursos de formación y toma de conciencia de la organización • Comunicaciones internas y externas (Su contenido, lugar, forma y oportunidad) • Requisitos para la creación, actualización y control de la documentación
Numeral 8: Operación	En este aparte se indaga por la puesta en marcha del SGCN teniendo en cuenta lo planificado. Los puntos fundamentales son: **1.- Realizar el Análisis de impacto en el negocio (Business Impact Analysis – BIA):** Identificar los aspectos que soportan los productos y servicios claves para la organización: • Identificar los procesos críticos • Interdependencias de todos los procesos • Recursos necesarios para el nivel mínimo **2.- Evaluación de Riesgos:** Para la evaluación de riesgos se propone la Norma ISO 31000. En todo caso se deben cumplir los siguientes requisitos: • Implantar y mantener un proceso formal de valoración de riesgos • El proceso debe ser documentado. Los Riesgos: • Deben ser Identificados, • Analizados • Evaluados sistemáticamente • En cuanto tiempo pueden causar incidentes que generan interrupciones en la organización. 3**.- Estrategia de Continuidad del Negocio:** El análisis de riesgos realizado junto a su impacto en el Negocio contribuye a desarrollar las estrategias que permitan realizar la protección y recuperación de las actividades críticas conjugando:

Numeral	Aspectos que se evalúan
	• La tolerancia de la organización al riesgo • Objetivos de tiempo de recuperación. 4.- **Procedimiento de Continuidad del Negocio:** Aquí se definen los requisitos de los procedimientos y la documentación del sistema de Continuidad del negocio para garantizar que estos procedimientos sean efectivos. Los procedimientos deben: • Establecer un adecuado protocolo de comunicaciones internas y externas. • Especificar convenientemente los pasos intermedios a dar frente a una interrupción. • Contemplar flexibilidad para responder a las amenazas no previstas. • Enfocarse en los eventos con potencialidad de causar interrupciones. • Fundamentarse en los análisis realizados y las estrategias definidas y tomando en cuenta un estudio de interdependencia de los procesos. • Implementar estrategias de mitigación adecuadas para minimizar las consecuencias de los incidentes potenciales. **5.- Ejercicios y pruebas** La consistencia de los procesos definidos debe ser probada mediante ejercicios y pruebas para validar los planes de continuidad del negocio, solo así se asegura que las estrategias seleccionadas son capaces de dar respuestas de recuperación dentro de los plazos necesarios.
Numeral 9: Evaluación de desempeño	La norma ISO 22301:2019 establece la necesidad de una permanente revisión y seguimiento del sistema para mejorar su operación. • ¿En qué medida se cumplen los objetivos y metas establecidas en el SGCN? • ¿Cuál es el desempeño de los procesos enfocados a proteger las actividades críticas? • ¿Cuál es el grado de conformidad con la Norma y los requisitos de la continuidad del Negocio?

Numeral	Aspectos que se evalúan
	• Guardar el seguimiento histórico de los puntos anteriores • Realizar Auditorías internas y planificadas • Realización de revisiones por la dirección de todos los puntos anteriores
Numeral 10: Mejoramiento continuo	La mejora continua cumple el objetivo de aumentar permanentemente la eficacia del sistema de continuidad del negocio y de todas la Organización contribuyendo a una permanente: • Mejora de la eficiencia: Costo/Beneficio. • Cumplimiento de Objetivos.

Tabla 16. Resumen de los requisitos de la norma ISO 22301:2019

En las páginas siguientes se incluye el diagnóstico de madurez encontrado del SGCN del IDEA. El detalle de la calificación otorgada a cada uno de los requisitos se encuentra en el documento anexo Análisis GAP ISO 22301: 2019.xlsx

4. RESULTADO GENERAL DE LA IMPLEMENTACIÓN ISO 22301:2019

En la tabla 17 se presenta el nivel de madurez del SGCN identificado en IDEA:

Dominio	Nivel de Madurez Actual	Nivel de Madurez Deseado
Contexto de la Organización	25,7	80
Liderazgo	36,8	80
Planeación	20,0	80
Soporte	59,6	80
Operación	46,3	80
Evaluación de desempeño	7,1	80
Mejoramiento	10,0	80

Tabla 17. Nivel general de madurez frente a los requisitos de la norma ISO 22301:2019

La brecha identificada a nivel de los diferentes requerimientos se observa en la ilustración 1:

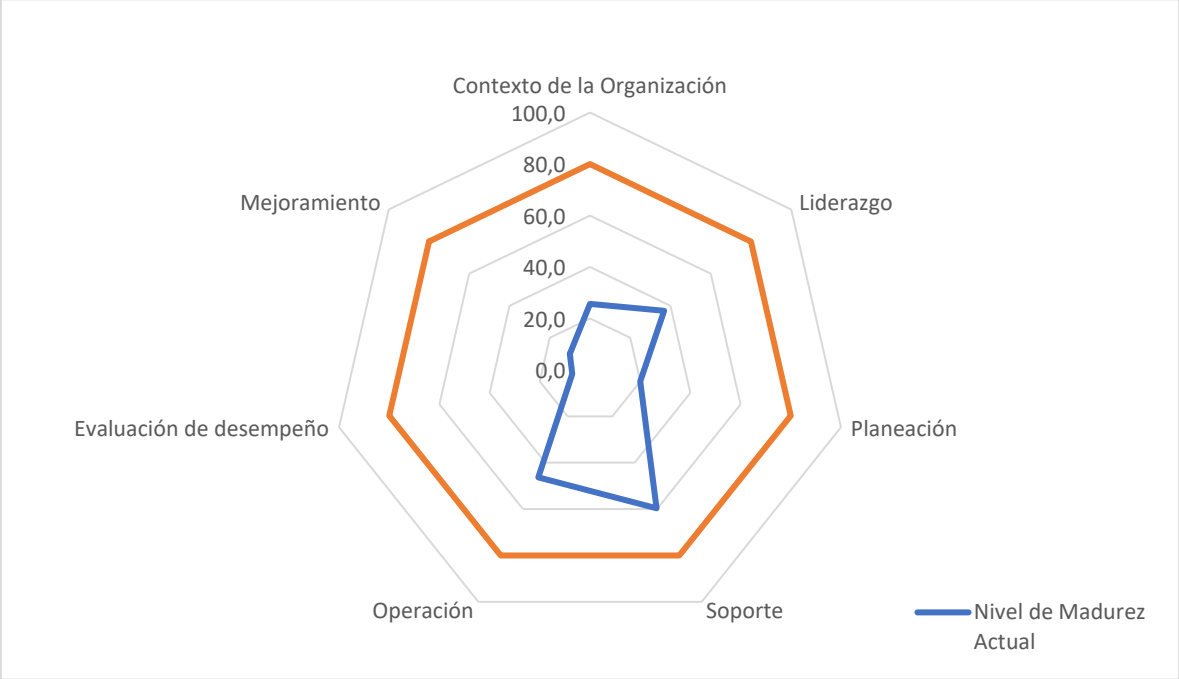


Ilustración 1 Brechas identificadas en el SGCN del IDEA

4.1. Contexto Organizacional

- En la documentación analizada se evidencia ausencia de la cuestiones internas y externas que pueden influir o afectar el Sistema de Continuidad de Negocio (organizaciones, tecnología, ambiente, personas, presupuesto, entre otros).

- Es importante además identificar y documentar las partes internas y externas definiendo las necesidades, expectativas, requisitos y requerimientos para cada parte.

- El manual del PCN indica contemplar las disposiciones, los requerimientos lineamientos establecidos por la Superintendencia Financiera de Colombia y los demás entes de control y vigilancia; así como las normas ISO aplicables, es necesario documentar estos requisitos legales y regulatorios vigentes que apliquen al Instituto, integrando actividades de revisión y actualización a este.

- Aunque el PCN contempla el alcance a nivel de procesos del instituto, es necesario identificar la interrelación externa que pueda aplicar al SGCN para la organización.

- Se evidencia documentación asociada a la planeación, implementación y mejoramiento del Plan de Continuidad de Negocio del Instituto, sin embargo, es indispensable volcar estas actividades a la estructura del ciclo PHVA de acuerdo con el marco de referencia de la ISO 22301:2019.

4.2. Liderazgo

- En el Manual del Plan de Continuidad de Negocio se expone el compromiso de la alta dirección en la implementación, mantenimiento y fortalecimiento del PCN. Es necesario definir y documentar además el compromiso de la alta dirección en cuanto a:
  - La definición de objetivos y políticas del PCN asociadas a la estrategia del Instituto.
  - Asignación de recursos para al funcionamiento.
  - Compromiso comunicando la importancia del PCN a las partes interesadas.
  - Seguimiento al cumplimiento de los objetivos del PCN.

- Se evidencia lineamientos en diferentes apartados del Manual del PCN asociados a:
  - Compromiso de la dirección
  - Aceptación del PCN por los colaboradores
  - Gestión de riesgos de interrupción
  - Capacitación
  - Divulgación
  - Actividades en las fases de operación del PCN.

De igual manera en el Manual SARO se establece la política de continuidad de negocio.

Es oportuno que todo lo anterior se estructure en un documento con la política o políticas asociadas a continuidad de negocio.

- Se observan resultados de capacitación a los colaboradores y las partes interesadas en cuanto al Plan de Continuidad de Negocio del Instituto, es indispensable también comunicar la política de continuidad de negocio.

- Se debe establecer y documentar la participación de la alta dirección en la asignación de responsabilidades y autoridad.

4.3. Planeación

- En cuanto a objetivos, políticas, roles y responsabilidades referentes al SGCN, se encuentra información general tanto en el PCN, en el manual SARO y el manual SARSIC. En la documentación revisada se encuentran los propósitos y procedimientos para la prevención, gestión, monitoreo, reacción y recuperación ante riesgos de interrupción. También se identifican objetivos generales en varios

informes y planes. Se requiere particularizar y especificar de manera más precisa y detallada lo que corresponde a la política y objetivos del SGCN, como producto de la ejecución de las siguientes tareas:

- Examinar condiciones del entorno interno y externo.
- Analizar objetivos y metas estratégicas vigentes.
- Alinear la política del SGCN con la política de Seguridad de la Información y Ciberseguridad.
- Establecer objetivos estratégicos y tácticos claros para el SGCN.
- Formular objetivos SMART e indicadores que permitan monitorear el SGCN

- La identificación de riesgos de interrupción y de pérdida de disponibilidad y vulnerabilidades de los activos de información se encuentra referida en el MANUAL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO – PCN, en el MANUAL SARO y en el manual del SISTEMA DE ADMINISTRACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - SARSIC. Sin embargo, se hace necesario establecer una planeación y articulación clara de los elementos propios de un SGCN, de tal forma que se evidencie que se cumple con los siguientes propósitos o atiende las siguientes actividades:
  - Cumplir con la estrategia, misión y visión de la entidad.
  - Asociar los elementos propios del SGCN con impactos positivos en servicios clave, satisfacción de partes interesadas y desarrollo de procesos.
  - Atender requerimientos puntuales de la SFC.
  - Identificar riesgos y oportunidades inherentes al SGCN en particular. Incorporar información clara sobre prevención y reducción de riesgos propios del SGCN.

- La gestión de incidentes, emergencias y crisis, así como las prioridades de recuperación se refieren en el PCN. Sin embargo, es necesario que se construyan y formalicen documentos que den suficiente atención a las siguientes actividades, de tal forma que se asegure su implementación y supervisión:
  - Definir roles, responsabilidades, recursos y evaluaciones del SGCN.
  - Describir actividades para direccionar, desarrollar, monitorizar y evaluar la efectividad del SGCN.
  - Establecer criterios y procedimientos para realizar las mediciones pertinentes al SGCN.

- La ejecución de pruebas y ejercicios, así como a la mejora continua, como parte de la estrategia de tratamiento de riesgos, se encuentra referida de manera general en el PCN y el SARSIC. Sin embargo, es necesario establecer una planificación detallada que satisfaga lo siguiente:
  - Disponer de un esquema de mejora continua que considere los riesgos y oportunidades del contexto interno y externo.
  - Conocer el propósito, impactos y recursos requeridos para incorporar los ajustes necesarios en el SGCN.
  - Identificar programas, proyectos e iniciativas para implementar y fortalecer el SGCN.

- Tener información precisa con respecto a los procedimientos para monitoreo y comunicación del SGCN.
- Disponer de protocolos para la incorporación de cambios en el SGCN.
- Identificar el flujo establecido para revisar y actualizar los objetivos del SGCN según sea necesario.
- Tener en consideración las exigencias y recomendaciones de auditorías y evaluaciones.

4.4. Soporte

- Se evidencia la definición general de roles, responsabilidades y recursos necesarios para la continuidad del negocio y la recuperación ante desastres. La documentación elaborada en la entidad incluye actividades para la prevención, gestión de incidentes, respuesta y recuperación, así como para la gestión de crisis. Sin embargo, es necesario que se ejecuten las siguientes actividades:
  - Establecer y comunicar una política robusta de Continuidad del Negocio a toda la entidad y asegurar que todos comprendan su contribución y las consecuencias de no atender lo definido o cumplir sus deberes en lo pertinente.
  - Definir competencias específicas para roles estratégicos, tácticos y operativos en el SGCN. Conservar información documentada con respecto a estas competencias. Fomentar el compromiso con el cumplimiento de los roles que le corresponden a cada uno.
  - Identificar claramente los recursos necesarios (financieros, humanos, técnicos, procedimentales, físicos) para el SGCN. En particular, es necesario dimensionar y especificar la vigencia de los recursos financieros.

- Se encuentran resultados asociados con los ejercicios BIA, así como actividades críticas y recursos necesarios para respuesta y recuperación ante ciertos escenarios de desastre. También se evidencia que la entidad ha definido, a nivel táctico, las estrategias y soluciones de continuidad del negocio para los escenarios de interrupción definidos. Es importante realizar ejercicios de actualización y calibración de estos análisis BIA a fin de adaptar el SGCN a las variables que se presenten en el contexto interno y externo. Es necesario que las estrategias y soluciones de continuidad y recuperación de desastres se afinen para dar atención a los resultados que arrojen los BIA revisados y ajustados.

- En la documentación se menciona la existencia de un plan y estrategia de comunicación que ha sido definido por el Equipo de Apoyo - Oficina Asesora de Comunicaciones. A pesar de que no se tuvo acceso al mismo durante el transcurso de la revisión, se asume que debe tener procedimientos para “Comunicación Externa y Mercadeo” y “Comunicación Interna”. De cualquier manera, se insiste en garantizar que se atiendan debidamente las siguientes actividades:
  - Definir con precisión el manejo de las comunicaciones, específicamente asociadas con el SGCN.

- Incluir detalles sobre qué, cuándo, a quién, cómo y quién se comunicará con las partes interesadas ante diversos escenarios de crisis.

- Se encuentra documentación referente a la ejecución de pruebas y ejercicios particulares referentes a la continuidad del negocio. En la medida que se vaya avanzando en la implementación y fortalecimiento del SGCN, es necesario que se revisen y actualicen los documentos que refieren la política, los objetivos, el alcance, los procedimientos operativos, las auditorías, las revisiones, los ejercicios de mejora, las acciones correctivas y las competencias del personal asociadas con este sistema de gestión. En consecuencia, toda esta documentación se debe mantener disponible y protegida contra los diferentes riesgos como: pérdida de confidencialidad, uso inadecuado, pérdida de integridad, desactualización, indisponibilidad, daño o destrucción.

- También se encuentran soportes de las capacitaciones y sensibilizaciones realizadas en los años anteriores, cuyas temáticas han sido de carácter general y para un entendimiento transversal en toda la entidad, como, por ejemplo, objetivos y beneficios del PCN, así como algunos aspectos particulares del diseño del PCN. Sin embargo, es preciso:
  - Establecer un plan estructurado y sostenido de formación para todos los roles del SGCN.
  - Mantener actualizadas las competencias del personal.
  - Implementar técnicas para medir la eficacia de los programas de formación.
  - Utilizar los resultados para ajustar y mejorar la formación.

4.5. Operación

Se evidencia la existencia de:

- Sistema de Administración de riesgo – SARSIC
- Manual SARO para la gestión de riesgo operativo
- Plan de manejo de incidentes de interrupción
- Plan de comunicaciones en crisis
- Plan de continuidad del negocio
- Plan de recuperación ante desastres
- Informe de análisis de riesgos de continuidad de negocio
- Mapa de riesgos de ciberseguridad
- Mapa de riesgo operativos
- Informe de análisis de impacto al negocio BIA

- Se evidencian documentos con el resultado de ejercicios de análisis de impacto al negocio y riesgos asociados a incidentes de interrupción. Estos informes corresponden al mes de enero del año 2023, no se evidencian documentos de ejercicios previos.

- Se observa desde la metodología la definición de tipologías de impacto como, afectación de la rentabilidad e ingresos, afectación al cliente, afectación de la imagen, reputación y credibilidad, incumplimiento legal, detención o afectación a otros procesos y también el análisis de impactos cuantitativos por interrupciones desde 1 día hasta 7 días.

- También se puede observar que se realizó un análisis de los procesos a nivel de procedimientos y definición de RTO para estos, es importante integrar en la próxima actualización de este ejercicio el análisis a nivel de actividades por proceso y la medición del indicador MTPD, además es vital desarrollar el análisis de los proveedores críticos para asegurar la continuidad a la operación.

- El Instituto tiene una metodología de gestión de riesgos estructurada de acuerdo con el marco de referencia ISO 31000, en la documentación revisada se evidencio ausencia del proceso de análisis de los riesgos identificados como de los planes de tratamiento que la organización debe gestionar.

- Se identificaron las estrategias de continuidad asociadas a la afectación de los componentes de infraestructura física, infraestructura tecnológica, recurso humano y proveedores. Actualmente varias de estas estrategias están redactadas para su futura implementación. Se recomienda realizar las pruebas de la estrategia de continuidad de negocio para verificar su eficacia e introducir los ajustes que sean necesarios para su mejora. Estas estrategias tienen identificadas las necesidades de recursos a nivel de: Personas, sistemas de información y servicios tecnológicos, infraestructura física, equipos, proveedores. Es relevante integrar en estas estrategias el ítem de finanzas, socios y proveedores necesarios para su funcionalidad.

- Es importante tal como lo indica la norma desarrollar procedimientos de recuperación con un nivel de detalle y especificidad de las actividades que se deben ejecutar para lograr recuperar la operación vital de cada proceso del instituto. Además de la elaboración de los procedimientos de recuperación de los sistemas de información y servicios tecnológicos, esenciales para el Plan de Recuperación de Desastres DRP.

- En la documentación se describe de manera general el manejo de las comunicaciones desde la Oficina Asesora de Comunicaciones. Adicional se menciona un documento anexo relacionado a los mensajes de comunicación externa e interna. Se recomienda actualizar el documento de manejo de crisis con los siguiente:
    - Voceros autorizados por la institución
    - Relación de convocados principales y suplentes durante una interrupción.
    - Detalle de los incidentes o impactos cuantitativos que deben convocar el comité de crisis.
    - Tipos de comunicados y que información transmitir a diferentes públicos objetivo.

- Establecer en el cronograma de pruebas para la institución los ejercicios asociados a tratar las comunicaciones por la materialización de los incidentes de interrupción.

- Se sugiere que el programa de pruebas de continuidad de negocio establezca un cronograma que organice la evaluación de escenarios de desastre de menor a mayor complejidad.

- Es importante integrar en todos los documentos el numeral de control de cambios donde se describan las mejoras o actualizaciones desarrolladas en la documentación. Es necesario mantener en los documentos la descripción de los cambios desarrollados en las últimas 2 o 3 versiones. Lo anterior permite a los lectores o personas que participen en la revisión evidenciar y entender los cambios desarrollados.

4.6. Evaluación de desempeño

- No se evidencia la existencia de mecanismos para el monitoreo de la eficiencia y/o eficacia del sistema de gestión de continuidad del negocio.

- No se evidencia la existencia de un conjunto de indicadores definido que permita medir y evaluar objetivamente el desempeño del SGCN.

- No hay evidencia de la existencia de programas o planes de auditoría orientados a evaluar el SGCN.

- No hay evidencia de la realización de ejercicios de auditoría interna o externa orientados a la evaluación del SGCN.

- No hay evidencia de la realización de revisiones y seguimiento al SGCN por parte de la dirección.

- Se evidencia la realización de ejercicios puntuales de prueba de escenarios limitados para la atención de algunas contingencias. No hay un programa de mediano y largo plazo para la realización de simulacros.

- Se recomienda definir un conjunto de indicadores que permita medir periódicamente y de forma objetiva el desempeño del SGCN, con lo cual se podrán identificar oportunidades de mejora.

- Se recomienda elaborar y ejecutar el programa y los planes de auditoría al SGCN, con lo cual se podrán identificar las acciones correctivas y las acciones de mejora necesarias para apalancar el mejoramiento continuo.

- Se recomienda implementar el mecanismo de revisión periódica por parte de la dirección, con lo cual se transmite el compromiso con la seguridad de la información y continuidad del negocio y se promueve el mejoramiento continuo.

4.7. Mejoramiento

- No se evidencia la existencia de un procedimiento documentado que oriente el ejercicio de la mejora continua.
- No se evidencia la existencia de acciones de mejora o acciones correctivas identificadas y/o ejecutadas.
- No se evidencia el seguimiento y mejora continua del SGCN.
- Se recomienda que, con base en los resultados de la evaluación del desempeño, los informes de revisión por la gerencia y los informes de auditoría, se apliquen las acciones correctivas, acciones de mejora y recomendaciones, orientadas a resolver las fallas identificadas y promover la mejora continua.

5. CONCLUSIONES

- Existen buenos esfuerzos en el desarrollo de algunos componentes pero que se emprendieron y mantienen de manera aislada y sin estar integrados bajo un programa de continuidad del negocio del Instituto.
- Una de las necesidades más sentidas en el Instituto es fortalecer las capacitaciones y formaciones de sus colaboradores en continuidad del negocio, para facilitar la implementación del SGCN como un programa y no como un proyecto puntual.
- A pesar de tener un líder de continuidad nombrado formalmente, es necesario trabajar en la implementación y puesta en marcha de las funciones que este rol exige.
- Llevar el Plan de Continuidad de Negocio del Instituto al cumplimiento de la norma 22301:2019, con el objetivo de establecer e implementar el Sistema de Gestión de Continuidad de Negocio.

6. BIBLIOGRAFIA

- ISO 22301:2019 Seguridad y Resiliencia. Sistema de Gestión de Continuidad de Negocio. Requisitos.
- DRII Disaster Recovery International Institute. Prácticas profesionales de continuidad del negocio

7. ANEXOS

- Análisis GAP ISO 22301: 2019.xlsx