Programa de Continuidad de Operaciones de las Unidades de Inteligencia Financiera

Julio 2021

El GAFILAT agradece la asistencia técnica brindada por la Cooperación Alemana para el Desarrollo, implementada por la Deutsche Gesellschaft für Iternationale Zusammenarbeit (GIZ), para la elaboración del presente documento, que contó además con el apoyo del Sr. Oscar Moratto. El contenido de esta publicación es completa responsabilidad del Grupo de Acción Financiera de Latinoamérica (GAFILAT).

Copyright © GAFILAT. Reservados todos los derechos, queda prohibida la reproducción o la traducción de esta publicación sin permiso previo por escrito. Las solicitudes de permiso de reproducción o de traducción de cualquier parte o de la totalidad de esta publicación deben dirigirse a la siguiente dirección: Florida 939 - 10º A - C1005AAS - Buenos Aires, Argentina – Teléfono (+54-11) 5252-9292; correo electrónico: contacto@gafilat.org.

ÍNDICE

LISTADO DE TABLAS

LISTADO DE FIGURAS

INTRODUCCIÓN

1. La pandemia del COVID-19 ha tenido impactos en todos los niveles y en diversas actividades económicas, tanto de sector público como privado. En lo que respecta al sector público, en particular, a las Unidades de Inteligencia Financiera – UIF, estos impactos se ven representados particularmente en:

    a. Necesidad de implementar estrategias de trabajo remoto como producto de las medidas de confinamiento y distanciamiento social, en la medida en que "los sistemas de tecnología de información y seguridad lo permitan"[1].
    b. Reducción o pausa en las operaciones y actividades desarrolladas por las UIF.
    c. Reducción de staff designado a análisis o investigación[2].
    d. Reducción en el número de Reportes de Operaciones Sospechosas – ROS[3] y/o solicitud de extensiones de plazos en la entrega de ROS[4].
    e. Retrasos en la obtención de información adicional requerida a los Sujetos Obligados (SO) para el análisis de operaciones o investigaciones en curso.
    f. Demoras en la recepción y procesamiento de información remitida por los SO[5].
    g. Afectación en las capacidades de cooperación internacional (p. ej. respuesta de requerimientos por parte de otras UIF a través del canal seguro Egmont)[6].
    h. Dificultades en los procesos de difusión de información a autoridades competentes (p.ej. fiscalía, procuraduría o equivalentes) debido a las afectaciones de dichas instituciones producto del Covid-19, así como del aparato judicial[7].

2. Teniendo en cuenta lo anterior, y primordialmente la implementación de estrategias de trabajo remoto por parte de las UIF, éstas pueden verse expuestas a riesgos de ciberseguridad y de continuidad de negocio de diversa índole. En este sentido, el GAFILAT planteó el desarrollo de herramientas que permitan a las UIF adoptar programas efectivos para la continuidad de sus actividades y operaciones en contextos de crisis.

[1] FATF (2020). COVID-19-related Money Laundering and Terrorist Financing. http://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf
[2] GAFILAT (2020). Comunicado del GAFILAT sobre Covid-19 y sus riesgos asociados de LA y FT. https://www.gafilat.org/index.php/es/espanol/19-noticias/102-comunicado-del-gafilat-sobre-Covid-19-coronavirus
[3] Ibid
[4] FATF (2020). COVID-19-related Money Laundering and Terrorist Financing
[5] Ibid
[6] Ibid
[7] Ibid

3. El presente documento se encuentra dividido en diversos capítulos. El primero, incluye un marco teórico descriptivo de carácter general relativo al funcionamiento de las UIF. En este sentido, se describen sus objetivos, funciones y particularmente, la importancia de las UIF en los sistemas de prevención del lavado de activos y financiamiento del terrorismo (LA/FT). El segundo, aborda el marco teórico del plan de continuidad de negocio (PCN), sus componentes y etapas. El tercer capítulo se establece un diagnóstico del PCN en los países del GAFILAT, mientras que el capítulo cuatro se centra en describir la metodología para realizar el análisis de riesgos y el análisis de impacto al negocio (business impact analysis, BIA, por sus siglas en inglés), así como su aplicación en el entorno de las UIF. Además, se hace una sugerencia respecto al tiempo objetivo de recuperación (recovery time objective, RTO por sus siglas en inglés) y del punto objetivo de recuperación (recovery point objective, RPO por sus siglas en inglés) de los servicios críticos de una UIF; y se presenta una propuesta de priorización de procesos críticos de una UIF. El último capítulo se centra en las recomendaciones relativas a la implementación del PCN en las UIF asociado a los procesos de mayor criticidad, incluyendo estrategias, medidas de seguridad y estrategias de implementación.

4. Debe tenerse en cuenta que los elementos abordados en este informe, en particular, las recomendaciones, podrán ser analizados por cada UIF con el objetivo de evaluar su factibilidad de implementación y priorización en función de las realidades de cada una de las instituciones. En este sentido, este producto no implica ninguna ampliación de las obligaciones contenidas en el estándar internacional, sino que aspira a brindar herramientas y elementos que pueden resultar de utilidad para las UIF de la región, y cuya valoración y eventual implementación será voluntaria. Toda medida que complemente o amplíe lo previsto en el estándar debe ser entendido como una recomendación orientativa.

RESUMEN EJECUTIVO

5. De acuerdo con la Recomendación 29 del Grupo de Acción Financiera Internacional (GAFI, la Unidad de Inteligencia Financiera (UIF) se encuentra definida como "un centro nacional para la recepción y análisis de: (a) reportes de operaciones sospechosas; y (b) otra información relevante al lavado de activos, delitos determinantes asociados y el financiamiento del terrorismo, y para la comunicación de los resultados de ese análisis"[8]. Se trata de un actor fundamental en los sistemas de prevención ALA/CFT/CFADM.

6. Esta importancia se soporta primordialmente por (i) la capacidad de la UIF de recolectar información, incluso, adicional a la remitida por los SO; (ii) la velocidad con la cual accede a información, incluyendo información financiera, administrativa y del orden público[9]; (iii) la capacidad de generar inteligencia financiera (operativa y estratégica) y; (iv) la capacidad de comunicar los resultados de su análisis. Estos elementos corresponden a las funciones primordiales de una UIF (recepción, análisis y comunicación de información).

7. De igual forma, las capacidades de una UIF se ven potenciados al contar con independencia y autonomía operativa, que parten de la premisa que la UIF tenga autoridad y capacidad para llevar a cabo sus funciones libremente, incluida la decisión autónoma para analizar, solicitar y/o comunicar información específica[10].

8. En este sentido, ante la ocurrencia de eventos internos o externos de alto impacto que impidan la utilización de los medios habituales, se torna fundamental contar con mecanismos que permitan que los procesos críticos de negocio que desarrolla la UIF puedan seguir operando de manera oportuna a través de medios alternos para realizar sus funciones normales, máxime bajo las condiciones actuales de pandemia.

9. De esta forma, contar con estrategias de continuidad de negocio en las etapas de notificación, análisis y comunicación de información, así como para las tareas complementarias que desarrolla la UIF (p. ej., supervisión de SO), se vuelve un requisito fundamental que incluso puede ser entendido como parte de la capacidad de independencia y autonomía operativa de una UIF.

[8] Recomendación 29 de los Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva del Grupo de Acción Financiera (GAFI)
[9] Ibid
[10] Egmont (2018). Entendiendo la Independencia Operativa y Autonomía de las UIF. Resumen Ejecutivo. https://egmontgroup.org/en/filedepot_download/1661/107

10. Es relevante resaltar que estos mecanismos alternos de continuidad de negocio deben cumplir con los parámetros de seguridad y confidencialidad de información, tal y como lo establece la Recomendación 29 (R.29) del GAFI. Asimismo, las falencias en la protección de información, según el Grupo Egmont de Unidades de Inteligencia Financiera se considera como un Criterio de Incumplimiento con los Estatutos y/o los Principios de Intercambio de Información entre Unidades de Inteligencia Financiera[11].

11. Las UIF, como todas las entidades, deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes que puedan afectarles y que podrían impactar la ejecución de sus operaciones. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permitan a la UIF operar tras un incidente o una situación grave como la pandemia del COVID-19[12] en un plazo de tiempo que no comprometa la continuidad de sus operaciones. La necesidad de actuar frente a esta situación implicó que las instituciones públicas y privadas se vieran en la necesidad de desplegar sus planes de continuidad de negocio (PNC) implementando estrategias como el trabajo remoto, ya sea de forma parcial o total.

12. La continuidad de negocio se define como "capacidad de una organización de continuar la oferta de productos y servicios dentro de un periodo de tiempo aceptable a una capacidad predefinida durante una interrupción"[13]. En este sentido, es fundamental que una UIF cuente con un PCN que asegure una operación ante situaciones de interrupción inesperadas, al menos de sus actividades críticas, dada la importancia estratégica de estas organizaciones en los sistemas de prevención y lucha contra el lavado de activos y la financiación al terrorismo.

13. Un PCN involucra diversos aspectos y su nivel de detalle y alcance depende de distintas variables dentro de las cuales se encuentran, el ambiente normativo y de funciones que ejerza la UIF.

14. Sin embargo, un pilar fundamental para el correcto diseño e implementación de un PCN es el apoyo de la alta dirección.

15. Una vez se haya establecido el alcance del sistema, incluyendo los procesos y activos de información críticos deberá realizarse un análisis de impacto de negocio con el fin de clasificar los procesos según criticidad y dependencia de los activos tecnológicos. De igual

[11] Egmont (2014). Proceso de Apoyo y Cumplimiento.
[12] Declarada oficialmente como pandemia por la Organización Mundial de la Salud el 11 de marzo 2020
[13] Norma ISO 22301. Definiciones

forma, es fundamental realizar un análisis de riesgo, donde se evalúe en términos de impacto y frecuencia las amenazas a las cuales está expuesta la UIF. De esta forma, se estará en capacidad de diseñar la estrategia y la respuesta a incidentes.

16. Con el fin de asegurar la pertinencia y eficiencia del PCN es necesario implementar un proceso de pruebas, mantenimiento y revisión al mismo. En este marco, la norma ISO 22301 es un estándar internacional que sirve de referencia para el diseño e implementación de sistemas de gestión de continuidad de negocio (SGCN).

17. Otro aspecto fundamental que debe ser analizado a la par del diseño del PCN, y máxime a la naturaleza y confidencialidad de la información que recolecta, analiza y comunica una UIF, es el relativo a la seguridad de la información, el cual puede enmarcarse en la norma ISO 27001.

18. En virtud de lo anterior, a fin de realizar el diagnóstico del programa de continuidad de operaciones de las UIF de los países miembros del GAFILAT, se recolectó información por medio de un cuestionario online y se realizaron entrevistas con algunas de las UIF de la región para poder ampliar el análisis y la información recibida.

19. A través de estos métodos de recolección de información se obtuvieron datos que permitieron contar con una visión de las medidas y acciones implementadas por las UIF de la región para dar continuidad a las operaciones propias de sus unidades. A saber, se tuvieron como principales conclusiones:

    a. En el 55% de los países, el número de ROS en el periodo de 2020 (parcial) se encuentra entre el 50% y el 79% de los ROS del 2019. Se presentaron casos de aumentos en el número de ROS y de reducción superior al 50% al comparar estos dos periodos de tiempo.
    b. También se presentaron algunos casos con reducciones en los volúmenes de requerimientos de información a través del canal seguro Egmont, tanto en recepción como en solicitud.
    c. En lo referente a casos de inteligencia financiera, al comparar el 2019 y el 2020 (parcial), no todas las UIF analizadas presentaron reducciones en el número de casos difundidos a autoridades competentes, y en donde se presentaron reducciones, en la mayoría de los países dichas reducciones no fueron drásticas.
    d. Se observa que todas las UIF entrevistadas, en mayor o menor medida, implementaron estrategias de adaptación en los procesos de recepción, análisis y difusión de información, ya fuese a través de medidas de trabajo remoto y/o la

implementación de protocolos de bioseguridad y modificaciones de horarios laborales o turnos, para el desempeño de sus labores desde las instalaciones de la institución; así como ajustes en los procesos de negocio, con el fin de adaptarlos a las nuevas condiciones.

e. A pesar que no todas las UIF de la región cuentan con un PCN explícito (83%), durante la pandemia implementaron en su gran mayoría, en función de la intensidad de las cuarentenas decretadas, medidas rápidas y efectivas que permitieran una operación continua de las actividades de inteligencia financiera y de supervisión en donde fuera aplicable, de tal forma que el impacto en las operaciones fuera mínimo.

20. Dentro de los principales aspectos a resaltar de las entrevistas no estructuradas se mencionan los siguientes:
    a. Varias UIF de la región venían implementando procesos de transformación digital, enfocados primordialmente a la digitalización de los mecanismos de comunicación, ya sea con los SO y/o los receptores de información de inteligencia financiera.
    b. Las UIF realizaron importantes ajustes a sus procesos internos con el fin de permitir que sus actividades se vieran impactadas lo menor posible.
    c. Dependiendo de las acciones diseñadas, se permitieron mayores o menores grados de conectividad remota de funcionarios de la UIF, diseñando diversas medidas de ciberseguridad.
    d. Varias UIF implementaron estrategias de capacitación de funcionarios y SO.

21. Dentro de las principales oportunidades de mejora y fortalecimiento de las capacidades de continuidad de operaciones de las UIF se encuentran:
    a. Designar un equipo con claras responsabilidades en términos del diseño e implementación del PCN.
    b. El formalizar un Plan de Manejo de Crisis.
    c. Contar con Sistemas de Gestión de Información y Eventos de Ciberseguridad – SIEM, y con un Centro de Operaciones de Seguridad (SOC), así como la ampliación de la adopción de Sistemas de Gestión de Seguridad de la información (ISMS) basados en una norma/estándar internacional, pueden apoyar de forma importante los esfuerzos de continuidad de operaciones de las UIF.

22. En el análisis de riesgos y BIA, se identificaron como principales amenazas las relativas a cinco (5) contextos: i. desastres naturales; ii. ataques informáticos; iii. fallos tecnológicos; iv. errores internos no intencionales; v. problemas sociales y de salud pública.

23. De esta forma, se identificaron como amenazas con nivel inherente extremo los ataques informáticos, los daños tecnológicos y los problemas sociales y de salud pública; como de nivel alto, los desastres naturales y los errores internos no intencionales. En la definición de procesos críticos de las UIF, se identificaron los asociados a las tareas de i. notificación; ii. análisis de información; iii. comunicación de resultados y; iv. actividades de supervisión (para aquellas UIF que desarrollan este aspecto).

24. Finalmente, con base en estos hallazgos identificados, se establecen una serie de medidas y recomendaciones para los procesos críticos de las UIF que fueron identificados con relación al PCN. Estas recomendaciones incluyen las estrategias, medidas de seguridad y herramientas de implementación.

METODOLOGÍA

25. El programa de continuidad de operaciones de UIF parte de la base de un conocimiento del contexto de las mismas. En este sentido, se determinó qué es una UIF, cuáles son sus funciones y se establecieron los procesos funcionales de mayor relevancia, los cuales corresponden a las actividades de recepción, análisis y comunicación de información, así como, en donde sea aplicable, las funciones de supervisión de SO.

26. Posteriormente, el proceso metodológico incluyó el entendimiento de los PCN y su adaptabilidad a las UIF.

27. Adicionalmente, se procedió a realizar un proceso de recolección de información primaria, con el fin de realizar un diagnóstico de las estrategias de continuidad de operaciones de las UIF de los países del GAFILAT. Este diagnóstico parte del diseño de un instrumento que consta de ciento setenta y dos (172) preguntas de diversa índole que cubren temas tales como:

    a. Información general: ubicación, número de funcionarios de la UIF, entre otros.
    b. Información operativa: volumetrías de información (ROS, requerimientos, etc.), metodología de lectura y clasificación de ROS, canales de recepción y difusión de información.
    c. Información de impacto COVID-19 en las operaciones de la UIF: impacto de aislamiento o confinamiento (de existir), implementación de medidas de trabajo remoto, etc.
    d. Plan de Continuidad de Negocio (PCN): elementos correspondientes al PCN (análisis de impacto de negocio, análisis de riesgos, seguridad de información, etc.)
    e. Personal: PCN y el personal de UIF.
    f. Oficinas: PCN y ambiente físico.
    g. Tecnología de información: PCN y aplicativos de tecnología de información y medidas de ciberseguridad básicas.
    h. Seguridad de la red: elementos de ciberseguridad, tanto políticas de ciberseguridad como mecanismos de protección.
    i. Administración y monitoreo de información: manejo de información, clasificación y uso de estándares internacionales.
    j. Circunstancias adicionales: otros elementos importantes relativos al PCN.

28. Con las respuestas obtenidas, se planteó un diagnóstico inicial de la situación de continuidad de operaciones de las UIF participantes en el instrumento de recolección de información.

29. De forma complementaria, se realizaron entrevistas no estructuradas con algunas UIF con el objetivo de ampliar la información recabada a través del instrumento de recolección.

30. Posterior al análisis de información, se llevaron a cabo las actividades tendientes a realizar la identificación y valoración de amenazas en términos de PCN aplicables a UIF y a ejecutar una evaluación del riesgo inherente. Esto, tomando como base los estándares ISO 22301, ISO 27001 e ISO 31000.

31. A partir de dicha evaluación, se identificaron los procesos críticos de las UIF, se priorizaron y se realizaron recomendaciones relativas a las estrategias, medidas de seguridad y herramientas de implementación asociadas a los procesos críticos identificados previamente.

GLOSARIO

ALA/CFT	Antilavado de activos y contra el financiamiento del terrorismo
AOP	Autoridades de orden público
BIA	Análisis de impacto de negocio (Business Impact Analysis)
BYOD	Traer su propio dispositivo (Bring your own device)
CDN	Red de entrega de contenidos (Content Delivery Network)
CISO	Chief Information Security Officer
Cobit	Objetivos de control para la información y tecnologías relacionadas (Control Objectives for Information and related Technology)
DLP	Prevención de pérdida de datos
DRP	Plan de Recuperación de desastres (Disaster Recovery Plan)
DMZ	Zona desmilitarizada o red perimetral (Demilitarized zone)
DNS	Sistema de nombres de dominio (Domain names system)
FPADM	Financiamiento de la proliferación de armas de destrucción masiva
FT	Financiamiento del terrorismo
GAFI	Grupo de Acción Financiera Internacional
GAFILAT	Grupo de Acción Financiera de Latinoamérica
IPS	Sistema de prevención de intrusiones (Intrusion prevention system)
ISMS	Sistemas de Gestión de Seguridad de la información
LA	Lavado de activos
MTD	Tiempo máximo tolerable de caída (Maximum Tolerable Downtime)
NAS	Dispositivo de almacenamiento conectado en red (Network attached storage)
NIST	Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology)
OTP	Contraseña de un solo uso (One time password)
PMC	Plan de manejo de crisis
RDP	Protocolo de escritorio remoto (Remote desktop protocol)
ROL	Nivel mínimo de recuperación de servicio (Revised Operating Level)
ROS	Reporte de Operación Sospechosa
RPO	Punto objetivo de recuperación o grado de dependencia de actualidad de los datos (Recovery Point Objective)
RTO	Tiempo de recuperación objetivo (Recovey Time Objective)
SAN	Red de área de almacenamiento (storage area network)

SGCN	Sistema de Gestión de Continuidad de Negocio
SIEM	Sistema de Gestión de información y eventos de seguridad
SO	Sujetos obligados
SOC	Centro de operaciones de seguridad (Security operations center)
SSL/TLS	Certificados de servidor seguro
UIF	Unidad de Inteligencia Financiera
UPS	Fuente de poder ininterrumpida (Uninterruptible power supply)
VPN	Red privada virtual (Virtual private network)

CONCEPTOS[14]

i. **Continuidad de negocio**: Es la capacidad de una organización de continuar la oferta de productos y servicios dentro de un periodo de tiempo aceptable a una capacidad predefinida durante una interrupción.

ii. **Plan de continuidad de negocio**: Se define como la información documentada que orienta a una organización para responder ante una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio.

iii. **Análisis de impacto al negocio (BIA)**: proceso en el que se analiza el impacto de una interrupción conforme avanza el tiempo en la organización.

iv. **Interrupción**: incidente bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización.

v. **Máximo tiempo de caída tolerable (MTD)**: Tiempo que determina el tiempo que puede estar caído un proceso antes de que se produzcan efectos desastrosos en la compañía y repercuta en el negocio.

vi. **Punto objetivo de recuperación (RPO)**: Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

vii. **Punto Tiempo objetivo de tiempo de recuperación (RTO)**: Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

viii. **Resiliencia**: Capacidad de una organización para resistir cuando es afectada por una interrupción.

[14] Norma ISO 22301, 2019

1. MARCO GENERAL DE LAS UNIDADES DE INTELIGENCIA FINANCIARA

1. Las UIF son actores fundamentales en los sistemas ALA/CFT/CFPADM. Entender sus características, funciones primordiales y la relevancia de los procesos de continuidad de operaciones para este tipo de instituciones es fundamental para abordar los programas de continuidad de operaciones en UIF.

1.1. Contexto histórico

2. La lucha contra el crimen organizado es una actividad que los Estados han desarrollado por décadas. El atacar estructuras asociadas al lavado de activos, el financiamiento del terrorismo y más recientemente, el financiamiento de la proliferación de armas de destrucción masiva (LA/FT/FPADM) ha tomado particular relevancia, en el entendido que al "privar a los elementos delictivos del producto de su actividad"[15] criminal se ataca su sostenimiento en el largo plazo. Conforme a lo anterior, se podría considerar lo siguiente:

    a. El impacto y afectación sobre el orden económico y social, así como la integridad de los mercados financieros que este tipo de actividades generan.
    b. Los efectos sobre la seguridad nacional asociadas a estos delitos.
    c. El alcance transnacional de este tipo de estructuras.
    d. La creciente necesidad de cooperación internacional con el objetivo de desmantelar eficientemente estas organizaciones.

3. Como parte de las medidas de los países para combatir y prevenir estos delitos, se ha desarrollado una arquitectura jurídica e institucional encaminada a "prevenir y contener los fenómenos de crimen organizado transnacional asociados"[16] al LA/FT/FPADM. De esta forma, los "Estados que se suscriben a estos acuerdos manifiestan un compromiso político a aplicar jurídica y operativamente, como mínimo, aquellas directrices del derecho internacional público y de estándares internacionales sobre política pública, creados sobre la base de corresponsabilidad en la resolución de asuntos que atañen al concierto mundial de naciones"[17].

4. Dentro de este marco jurídico internacional se encuentran, entre otros, la Declaración de Principios de Basilea (1988); la Convención de las Naciones Unidas contra el Tráfico Ilícito

[15] FMI (2004). Unidades de Inteligencia Financiera. Panorama General. P. 1.
[16] UIAF (2014). Introducción al marco jurídico y estándares internacionales antilavado de activos y contra la financiación del terrorismo. P 11
[17] Ibid p. 8.

de Estupefacientes y Sustancias Sicotrópicas (1988); el Convenio de Estrasburgo contra el Blanqueo de Capitales (1990); las 40 Recomendaciones del Grupo de Acción Financiera Internacional (GAFI); el Convenio de Naciones Unidas para la Supresión de la Financiación del Terrorismo (1999); la Convención de Palermo contra la Delincuencia Organizada Trasnacional (2000) y la Convención de las Naciones Unidas contra la Corrupción (2003). En América, son de destacar el Reglamento modelo de la Comisión Interamericana Contra el Abuso de Drogas de la OEA (reformado en 2002); la Declaración de Caracas (1990), de Cartagena (1991); la Convención Interamericana contra la Corrupción (1996); la Convención Interamericana contra el Terrorismo (2002); y los lineamientos del del Grupo de Acción Financiera de Latinoamérica (GAFILAT).

5. En este contexto, surgen las UIF ante la necesidad de acceder a información financiera por parte de las fuerzas del orden. Inicialmente, se incluyó al sistema financiero con el objetivo de abordar la problemática de LA[18]. Se llegó entonces a la conclusión que, si el sistema de lucha contra el LA y el FT exigía a las instituciones financieras comunicar operaciones sospechosas, se necesitaba una oficina o un organismo central encargado de evaluar y procesar los datos correspondientes[19].

6. Las UIF surgen aisladamente a principios de los años noventa, como consecuencia de la necesidad de un organismo central que recibiera, analizara y divulgara información financiera provechosa para combatir el LA[20]. De esta forma, las UIF tienen un incremento importante, a tal punto que el Grupo Egmont, la asociación internacional que las congrega informalmente, tenía 94 miembros en 2004[21] y en la actualidad cuenta con 166 miembros[22].

1.2. ¿Qué es una UIF y cuáles son sus funciones?

7. En primera instancia, los Estados requieren contar con servicios o cuerpos de Inteligencia, con capacidad operativa, tecnológica y humana, con el objetivo de diseñar escenarios futuros y proponer posibles alternativas para la toma de decisiones gubernamentales, previniendo de esta forma amenazas delictivas[23]. En este sentido, el contar con capacidades de inteligencia financiera resulta estratégico para poder complementar otras

[18] Gilmore, W. (1999). Dirty Money: The Evolution Of Money-Laundering Counter-Measures, segunda edición. (Estrasburgo: Council of Europe Press). P. 103
[19] Grupo Egmont (1995). The First International Meeting of Organizations Devoted to Anti-Money Laundering (Bruselas). P. 1
[20] FMI (2004). Unidades de Inteligencia Financiera. Panorama General. P. 1.
[21] Ibid
[22] https://egmontgroup.org/en/content/about
[23] UIAF (2014). Las unidades de Inteligencia Financiera.

capacidades de inteligencia con el objetivo de desmantelar, no solo operativamente, sino financieramente las estructuras de crimen organizado.

8. De acuerdo con los Estándares Internacionales del GAFI, la Recomendación 29 (R.29) – Unidad de Inteligencia Financiera[24], dispone que los "países deben establecer una Unidad de Inteligencia Financiera (UIF) que sirva como un centro nacional para la recepción y análisis de: (a) reportes de operaciones sospechosas; y (b) otra información relevante al lavado de activos, delitos determinantes asociados y el financiamiento del terrorismo, y para la comunicación de los resultados de ese análisis. La UIF debe ser capaz de obtener información adicional de los SO, y debe tener acceso oportuno a la información financiera, administrativa y del orden público que requiera para desempeñar sus funciones apropiadamente".

9. Por su parte, la Nota Interpretativa de la R.29 explica que dentro de las funciones de una UIF se debe realizar las siguientes tareas[25]:

    a. Recepción: ser la agencia central de recepción de información remitida por los SO, incluyendo: i. los reportes de operación sospechosa en cumplimiento de las Recomendaciones 20 y 23; ii. cualquier otra información que exija la legislación nacional. Además, se podría considerar obtener información complementaria (incluyendo, por ejemplo, fuentes abiertas, información recopilada y/o mantenida por otras autoridades, entre otra) de índole financiero, administrativo y de orden público que sea necesaria para desempeñar sus funciones.
    b. Análisis: la UIF realiza dos (2) tipos de análisis. A saber:
        i. Análisis operativo que utiliza la información disponible, ya sea a través de ROS o reportes objetivos[26], así como aquella que la UIF esté en capacidad de obtener, para identificar objetivos específicos, seguir el rastro de actividades o transacciones y determinar los vínculos entre esos objetivos y los posibles productos del delito, el LA, los delitos determinantes o precedentes, el FT y el FPADM.
        ii. Análisis estratégico, por el cual la UIF utiliza información disponible y que se pueda obtener, incluyendo datos proporcionados por otras autoridades

[24] GAFILAT (2019). Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva. R.29

[25] GAFILAT (2019). Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva. Nota interpretativa R.29.

[26] Reportes sobre operaciones que superan un umbral determinado pero que de por sí, no constituyen una Operación Sospechosa. Esta información es valiosa como fuentes complementarias de información en el proceso de generación de inteligencia financiera. FMI (2004). Unidades de Inteligencia Financiera.

competentes para identificar tendencias y patrones relacionados con el LA, el FT y el FPADM. Este tipo de análisis suele ser un insumo para definir políticas y metas para la UIF.

c. Comunicación: la UIF debe comunicar, ya sea de forma espontánea o por solicitud, la información y los resultados de los análisis realizados a las autoridades competentes y "a las UIF de otros países"[27], de conformidad con los estándares internacionales y siempre que cumpla con la legislación establecida por el país. Para tal fin, debe emplear canales dedicados, seguros y protegidos.

10. De igual forma, se advierte que, en la región de América Latina, algunas UIF realizan algunas funciones complementarias, tales como:
    a. Capacitación de SO.
    b. Capacitación de autoridades del orden público (AOP), supervisores y otras autoridades competentes.
    c. Participación en el diseño de política pública relacionada con el combate del LA/FT/FPADM.
    d. Colaborar en el marco regulatorio y/o emitir regulación a ciertas actividades económicas.
    e. Supervisión de SO[28].
    f. Bloqueo de operaciones y congelamiento de cuentas relacionadas con maniobras de LA o FT.
    g. Fomento de interés público en cuestiones de prevención de LA/FT/FPADM y actividades o campañas de sensibilización.
    h. Establecer herramientas o aplicativos para la consulta online de las listas de individuos u organizaciones terroristas de la Resolución del Consejo de Seguridad de las Naciones Unidas (RSCNU) 1267.
    i. Ser la instancia ejecutiva o secretaría técnica del comité o comisión nacional ALA/CFT del país.

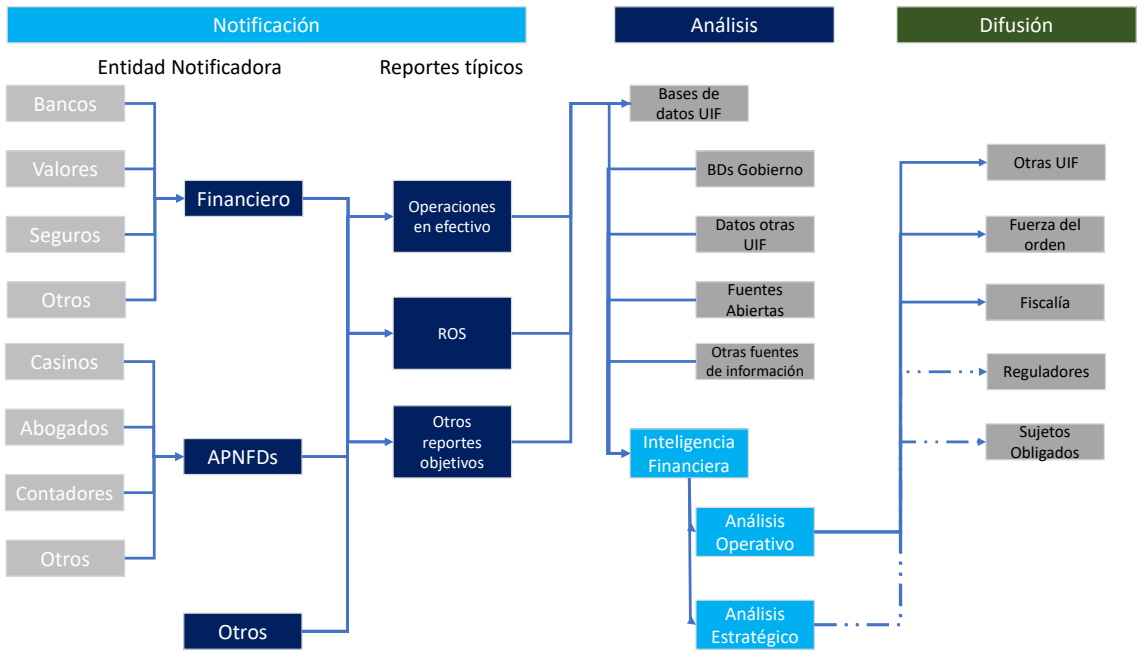
11. Existe también, en varios países del GAFILAT, una función de particular importancia en los procesos de evaluación mutua de las 40 Recomendaciones del GAFI, y es el de servir como institución articuladora en dichos procesos.

12. En resumen, y de manera esquemática, el flujo de información en una UIF se presenta en la siguiente figura. Cabe señalar que esta figura representa únicamente las funciones

[27] FMI (2004). Unidades de Inteligencia Financiera. Panorama General. P. 4.
[28] Particularmente, sectores residuales de supervisión.

tradicionales de las UIF, de acuerdo con lo requerido por el estándar del GAFI. En las UIF que cuentan con funciones complementarias este flujograma puede presentar variaciones.

Figura 1 - Flujo esquemático de información de una UIF



Fuente: Elaboración propia con base en FMI (2004). Unidades de Inteligencia Financiera. Panorama General. Figura 1

13. Las UIF generalmente se pueden clasificar dentro de uno de cuatro (4) modelos de funcionamiento. Es importante mencionar que teniendo en cuenta este aspecto, la Recomendación 29 del GAFI no prejuzga la elección del modelo de UIF que haga cada país ni tiene preferencia por un modelo en particular, dado que los requisitos se aplican a todos los modelos por igual. La selección del modelo depende de factores tales como los objetivos misionales que le han sido asignados a la UIF, el marco de supervisión, los sistemas jurídico y administrativo y las capacidades técnicas y financieras del país[29]. Los modelos típicos de UIF son[30] [31]:
    a. Modelo Judicial: la UIF se establece dentro de la rama judicial del Estado, usualmente la Fiscalía o su equivalente, de tal forma que la información relacionada a actividades sospechosas es acopiada por agencias de investigación de tal forma que los poderes judiciales pueden ser desplegados (p. ej., confiscación de fondos,

[29] FMI (2004). Unidades de Inteligencia Financiera. Panorama General. P. 5.
[30] https://egmontgroup.org/en/content/financial-intelligence-units-fius
[31] FMI (2004). Unidades de Inteligencia Financiera. Panorama General. PP 10 – 19.

congelamiento de cuentas, realización de interrogatorios, arresto de personas, etc.). La ventaja principal de este tipo de sistema es que la información proporcionada pasa directamente de los SO a un organismo del poder judicial para fines de análisis y procesamiento.

b. Modelo policial o fiscalizador (*law enforcement*): implementa las medidas de lucha con el LA/FT/FPADM dentro de un sistema policial existente, apoyando los esfuerzos de múltiples autoridades del ejercicio de la ley con autoridad concurrente y en algunos casos de competencia, para investigar estos delitos. Bajo este modelo, la UIF tendrá una relación más estrecha con otras entidades encargadas de la aplicación de la ley —por ejemplo, la unidad de delitos financieros— que podrán aprovechar los conocimientos y las fuentes de información de la UIF, permitiendo un intercambio de información más ágil al utilizar las redes existentes de intercambio de información, tanto nacionales como internacionales.
c. Modelo Administrativo: bajo este esquema, la UIF es una autoridad administrativa centralizada e independiente que recibe y procesa información y transmite los resultados de su análisis a las autoridades de cumplimiento de la ley para su judicialización. Las UIF de este tipo suelen formar parte de la estructura o el ámbito de supervisión de una administración u organismo distinto de las autoridades judiciales o policiales A veces constituyen un organismo separado, sujeto a la supervisión de un ministerio (típicamente Hacienda) o una administración - UIF "autónoma" (p. ej. el Banco Central) o al margen de ella (UIF "independiente"). De esta forma, la UIF funciona como un puente o filtro entre los SO y las AOP a cargo de la investigación y el enjuiciamiento de los delitos financieros. La información que recibe la UIF es analizada al interior y de encontrarse elementos que permitan corroborar o complementar la información remitida por los SO, se comunica dicho análisis a las autoridades encargadas de las investigaciones y los procesos penales.
d. Modelo Mixto: la UIF sirve como un intermediario y vínculo entre las ramas judiciales y de cumplimiento de ley combinando así características de al menos dos modelos de UIF.

14. Indistintamente del modelo adoptado, una cualidad fundamental que deben cumplir las UIF es la denominada "Independencia y Autonomía Operativa"[32]. Estos dos elementos son una condición fundamental para lograr un sistema efectivo ALA/CFT y parten de la premisa

[32] GAFILAT (2019). Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva. Nota interpretativa R.29.

que la UIF tiene autoridad y capacidad para llevar a cabo sus funciones, incluida la decisión autónoma para analizar, solicitar y/o comunicar información específica[33]. Dentro de los elementos que enmarca dicha independencia y autonomía se mencionan los siguientes[34]:

a. La UIF tiene la autoridad y la capacidad de llevar a cabo sus funciones de manera independiente, incluida la decisión autónoma de analizar, solicitar y/o comunicar información específica.
b. La UIF tiene protección funcional que la protege de responsabilidad civil o penal.
c. La UIF recibe recursos técnicos, humanos y financieros adecuados, que le permiten garantizar y promover su autonomía e independencia, así como cumplir con su mandato de manera efectiva.
d. La UIF obtiene y hace uso de los recursos necesarios para desempeñar sus funciones en forma individual o rutinaria, sin influencias o interferencias políticas, gubernamentales o sectoriales indebidas que puedan poner en riesgo su independencia operativa.
e. La UIF tiene la autoridad para decidir cuándo y dónde viajar en función de sus necesidades operativas.
f. La designación y la destitución del Director de UIF deben ser apolíticas, oportunas y sobre la base del mérito.
g. La justificación para destituir al Director de UIF es transparente y se basa en un desempeño insatisfactorio o incumplimiento de una obligación, lo cual debe estar debidamente pormenorizado y documentado.
h. El personal de la UIF no puede recibir tareas que estén por fuera del mandato de la UIF.
i. La UIF debe poder decidir o involucrarse en forma independiente con otras autoridades nacionales competentes o entidades homólogas extranjeras en relación con el intercambio de información.

15. Adicionalmente, todas estas funciones se deben ejecutar bajo altos estándares seguridad y confidencialidad de la información. En este sentido, la Nota Interpretativa de la Recomendación 29, junto con el criterio 29.6 establecen tres elementos para tener en cuenta:

a. Seguridad y confidencialidad de información: establecer mecanismos, procedimientos y normas relativos a la seguridad y confidencialidad de la

[33] Grupo Egmont (2018). Entendiendo la Independencia Operativa y autonomía de las UIF.
[34] Ibid

información que reposa en la UIF. Estos deben incluir el almacenamiento, divulgación y protección de la información, así como su acceso.

b. Acceso a la información: contar con niveles de autorización de acceso a información a los funcionarios de la UIF y proveer mecanismos para que los funcionarios entiendan las responsabilidades que les atañen con respecto al manejo y comunicación de información delicada y confidencial.
c. Seguridad de acceso: tanto a las instalaciones físicas de la UIF, como a los sistemas de información y a la información en general que reposa en la entidad.

16. Aunado a lo anterior, con el fin de proteger la información que acopian las UIF, estas deben "implementar normas que rijan la seguridad y confidencialidad de la información, incluidos los procedimientos de manejo, almacenamiento, divulgación y protección de la información, y de acceso a la información; garantizar que el personal de la UIF cuente con los niveles de autorización necesarios en cuanto a la seguridad y que entiendan sus responsabilidades en el manejo y comunicación de información delicada y confidencial; y asegurar el acceso limitado a sus instalaciones y a la información, incluyendo los sistemas de tecnología de la información". De igual forma, el Grupo Egmont ha establecido que la UIF debe proteger la información que recibe, así como la inteligencia financiera y otra información que genera[35] y ha determinado como un criterio de incumplimiento con los Estatutos y/o los Principios de Intercambio de Información entre las UIF las infracciones de seguridad y/o confidencialidad de información[36].

1.3. Importancia de las UIF en el sistema ALA/CFT

17. La existencia de organismos nacionales especializados en la recolección y análisis de información ALA/CFT resulta fundamental para cualquier Estado. Ello se debe, entre otros factores, a los siguientes[37]: a) los Estados enfrentan amenazas asociadas con el LA/FT; b) las dinámicas criminales son cambiantes; c) hay convergencia criminal y una motivación fundamental para cooperar y delinquir, buscando entre otros objetivos, el lucro; d) los delincuentes buscan vulnerabilidades en diversos sectores económicos, no solo el sector financiero con el objetivo de realizar operaciones de LA/FT; e) la ejecución de este tipo de operaciones requiere cada vez más de conocimientos especializados, de tal forma que se establecen organizaciones dedicadas exclusivamente a, por ejemplo, realizar operaciones de LA (lavado de activos por terceros), sin que estos se encuentren involucrados con la

[35] Egmont Group (2018). Entendiendo la Independencia Operativa y autonomía de las UIF.
[36] Egmont Group (2014). Proceso de Apoyo y Cumplimiento. P. 7.
[37] UIAF (2014). Lo que debe saber del lavado de activos y la financiación al terrorismo.

comisión del delito subyacente o precedente[38], tanto así que existen los lavadores profesionales de dinero, los cuales ofrecen sus servicios por una comisión, quienes usan sus conocimientos y experiencia para explotar vacíos legales, encontrar oportunidades para criminales y ayudar criminales a retener y legitimizar los ingresos producto del delito[39].

18. Esta relevancia e importancia del establecimiento de UIF se observa a través de diversos instrumentos internacionales tales como:
    a. La Convención de las Naciones Unidas contra el Crimen Organizado Transnacional (2000).
    b. La Convención de las Naciones Unidas contra la Corrupción (2003).
    c. Las Recomendaciones del GAFI, en particular, la R.29.

19. En este orden de ideas, las UIF cumplen un rol fundamental en los sistemas de prevención, detección, investigación y de represión, tanto nacionales como internacionales del LA/FT, incluyendo otras actividades delictivas, tales como la lucha contra la corrupción, tanto pública como privada[40]. Esta importancia de las UIF se da por diversos aspectos, tales como:
    a. Capacidad de recolectar información de parte de SO, relativa tanto a ROS como a reportes objetivos de diversa índole.
    b. Capacidad de generar inteligencia financiera, tanto en análisis operativo como estratégico que sirva a los Estados en los procesos de toma de decisiones.
    c. Contar con personal especializado en inteligencia financiera que permita el análisis de operaciones complejas, en diversos sectores económicos e incluso, que involucren múltiples jurisdicciones.
    d. Comunicar los resultados de inteligencia financiera a las autoridades competentes con el objetivo de desmantelar estructuras de crimen organizado involucradas en actividades de LA/FT.
    e. Comunicar y recibir información a nivel de inteligencia, a y de parte de otras UIF.
    f. Identificar tipologías y estrategias utilizadas por grupos criminales para llevar a cabo operaciones de LA/FT y así, informar a los sectores económicos

[38] Metodología del GAFI de 2013, nota al pie del Resultado Inmediato 7.
[39] FATF (2018). Professional Money Laundering. http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html
[40] Transparencia Internacional (2019). Financial intelligence units (FIUs): Effective institutional design, mandate and Powers. https://knowledgehub.transparency.org/helpdesk/financial-intelligence-units-fius-effective-institutional-design-mandate-and-powers

potencialmente vulnerados, para que estén en capacidad de diseñar estrategias de mitigación de estos riesgos y así, fortalecer los sistemas de prevención del LA/FT.

g. Brindar capacitación especializada a jueces, fiscales, policías y demás organismos de ley, relativa a la lucha contra el LA/FT.
h. Apoyar o dirigir estrategias de supervisión basada en riesgos en temáticas relacionadas con LA/FT.
i. Fungir como institución articuladora en los procesos de evaluación mutua de las 40 Recomendaciones GAFI.
j. Brindar cooperación nacional e internacional en aspectos relacionados a LA/FT.

20. Por todo lo anterior y conforme a lo mencionado anteriormente, contar con una UIF robusta técnicamente y que tenga Independencia y Autonomía Operativa es un pilar fundamental de los sistemas ALA/CTF.

1.4. Relevancia de contar con un modelo de continuidad de negocios para las UIF

21. Debido a la relevancia estratégica de las UIF en la lucha contra el LA/FT es crítico que este tipo de instituciones cuenten con mecanismos que les aseguren que, ante eventos internos o externos de alto impacto, los procesos críticos puedan seguir operando de manera oportuna a través de medios alternos para realizar sus funciones normales cuando los medios habituales no están disponibles debido a una contingencia.

22. En este sentido, contar con estrategias de continuidad de negocio[41] en las etapas de recepción, análisis y comunicación de información se hace un requisito fundamental que incluso puede ser entendido como parte de la capacidad de independencia y autonomía operativa de una UIF.

1.4.1. Recepción de Información

23. Durante este proceso se debe asegurar la disponibilidad de las aplicaciones mediante las cuales se reciben los reportes por parte de los SO, manteniendo la misma confidencialidad e integridad de los datos reportados.

24. En este sentido, bajo un contexto de continuidad de negocio, en un escenario extremo en el cual no se pueda acceder a la ubicación principal o de existir, a la(s) ubicación(es)

[41] Conjunto de procedimientos y medidas que adopta una institución para garantizar que las funciones esenciales puedan continuar durante y después de cualquier incidente y que su operación no se vea afectada. Fuente: https://bsginstitute.com/area/Continuidad-del-Negocio

alterna(s), como en el caso de mantener la operación bajo confinamientos como aquellos presentados al inicio de la pandemia del COVID-19, se deben implementar estrategias de trabajo remoto. Algunas de las estrategias para el trabajo remoto son:

a. Aplicaciones de acceso público o en la nube, que permitan al SO realizar la entrega de información y garantice la autenticidad del sujeto y trazabilidad de la información entregada.
b. Acceso remoto seguro a las aplicaciones requeridas por los funcionarios encargados de recibir y tramitar la información entregada en otros medios por parte de los SO.
c. Procedimiento seguro de recepción de información recibida en medio físico y entrega para el trámite del responsable.
d. Entrega de computadores en préstamo para los funcionarios que lo requieran.

25. De permitirse, la UIF deberá implementar medidas de seguridad para el trabajo remoto de sus funcionarios, dentro de las cuales se encuentran:
    a. Las aplicaciones públicas o en la nube para recepción de información, deben permitir al reportante auto gestionar todo el proceso de entrega de información y a nivel de seguridad contar mínimo con un canal seguro de comunicación que permita que la información viaje cifrada y con un mecanismo de autenticación multifactor para validar la identidad del reportante.
    b. Es necesario que los funcionarios que requieran acceder a los sistemas de información para el cargue de reportes, utilicen una conexión segura VPN e igualmente cuenten con un mecanismo de doble autenticación para validar su identidad. El acceso a los repositorios de documentos de trabajo deberá realizarse a través de VPN[42] únicamente, deberán estar alojados en un sistema de almacenamiento centralizado administrado por perfiles y usuarios y si es posible, se debe restringir la salida de información de la red interna de la organización.
    c. Establecer un protocolo de préstamo de computadores a empleados, con controles de seguridad para la entrega, el uso y devolución.

26. En este sentido, existen algunas herramientas que pueden ser implementadas para tal fin, dentro de las cuales se encuentran:

[42] Tecnología que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet, de esta forma, permite al ordenador en la red enviar y recibir datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

a. Para garantizar la comunicación segura de las aplicaciones públicas o en la nube, se debe implementar un certificado de servidor seguro SSL[43]/TLS[44].
b. Para la autenticación multifactor, se pueden emplear distintos métodos como: token de seguridad o una contraseña única basada en tiempo OTP[45].
c. Para la creación de VPN de acceso remoto, se requiere de la infraestructura tecnológica para su gestión, comúnmente los productos de seguridad como cortafuegos traen incluida esta característica.
d. Para el almacenamiento de información, se recomienda contar con infraestructura tipo SAN[46] o NAS[47] y controlar su acceso y uso mediante políticas de dominio. Para evitar temas de fuga de información, si es posible implementar una solución de prevención de perdida de información DLP[48].
e. Para el préstamo de computadores se recomienda realizar copia de seguridad del equipo antes de su salida, instalarles un software de cifrado de disco y antimalware, si es posible implementar una solución de prevención de perdida de información DLP o en su defecto inhabilitar puertos USBs u otro medio que sirva para la copia de información.

1.4.2. Análisis de Información

27. Durante este proceso, se debe garantizar que los analistas de información tengan acceso a las herramientas y datos necesarios para realizar su labor de forma remota, manteniendo la confidencialidad e integridad de la información de la organización. Para esta etapa, las estrategias para el trabajo remoto son:
    a. Acceso remoto seguro a las aplicaciones y documentos requeridos por los funcionarios analistas de información para realizar adecuadamente su labor.

[43] Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https
[44] El protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL. Ibid.
[45] Contraseña de un solo uso OTP, es una contraseña válida solo para una autenticación. La OTP soluciona una serie de deficiencias que se asocian con la contraseña tradicional (estática).
[46] Es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos: a) Una red de alta velocidad de canal de fibra o iSCSI; b) Un equipo de interconexión dedicado (conmutadores, puentes, etc); c) Elementos de almacenamiento de red (discos duros)
[47] Tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador/ordenador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado.
[48] Sistema que está diseñado para detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitoreo, detección y bloqueo de información sensible mientras está en uso (acciones de extremos), en movimiento (tráfico de red) y en reposo (almacenamiento de datos).

b. Autenticación multifactor para validar la identidad del analista, especialmente cuando acceda a sistemas con información sensible o confidencial.
c. Mecanismos de seguridad para monitorear y controlar el acceso, uso y comunicación de la información sensible gestionada por los analistas de información
d. Entrega de computadores en préstamo para los funcionarios que lo requieran.

28. Dentro de las medidas de seguridad para el trabajo remoto se encuentran:
    a. Es necesario que los funcionarios que requieran acceder a los sistemas de información misionales utilicen una conexión segura VPN e igualmente cuenten con un mecanismo de doble autenticación para validar su identidad.
    b. El acceso a los repositorios de documentos de trabajo deberá realizarse a través de VPN únicamente, deberán estar alojados en un sistema de almacenamiento centralizado administrado por perfiles y usuarios y si es posible, se debe restringir la salida de información de la red interna de la organización.
    c. Contar con sistemas de monitoreo, que permitan la visibilidad, auditoria y trazabilidad de las actividades de los analistas de información.
    d. Establecer un protocolo de préstamo de computadores a empleados, con controles de seguridad para la entrega, el uso y devolución.

29. Finalmente, algunas herramientas para su desarrollo son:
    a. Para la creación de VPNs de acceso remoto, se requiere de la infraestructura tecnológica para su gestión, comúnmente los productos de seguridad como cortafuegos traen incluida esta característica.
    b. Para la autenticación multifactor, se pueden emplear distintos métodos como: token de seguridad o una contraseña única basada en tiempo OTP.
    c. Para el almacenamiento de información, se recomienda contar con infraestructura tipo SAN o NAS y controlar su acceso y uso mediante políticas de dominio. Para evitar temas de fuga de información, si es posible implementar una solución de prevención de perdida de información DLP.
    d. Para el monitoreo de las actividades de los usuarios, se recomienda la implementación de un sistema de Gestión de información y eventos de seguridad SIEM.
    e. Para el préstamo de computadores se recomienda realizar copia de seguridad del equipo antes de su salida, instalarles un software de cifrado de disco y antimalware, si es posible implementar una solución de prevención de perdida de información

DLP o en su defecto inhabilitar puertos USBs u otro medio que sirva para la copia de información.

1.4.3. Comunicación del resultado del análisis de la información

30. Durante este proceso se debe garantizar que la comunicación y diseminación de los casos e informes respectivos, se realice de forma segura a los receptores competentes, utilizando medio digitales, pero manteniendo la confidencialidad e integridad de la información.

31. Es así que, dentro de las estrategias para el trabajo remoto se encuentran:
    a. Establecer un protocolo seguro para la entrega de informes de casos a las autoridades competentes.
    b. Utilizar medios digitales para la entrega de informes de casos, garantizando la identidad del emisor y receptor, la confidencialidad e integridad de los archivos comunicados.

32. Algunas medidas de seguridad para el trabajo remoto que pueden implementarse en esta etapa son:
    a. Establecer un protocolo seguro para la entrega de informes de casos a las autoridades competentes.
    b. Utilizar medios digitales para la entrega de informes de casos, garantizando la identidad del emisor y receptor, la confidencialidad e integridad de los archivos comunicados.

33. Dentro de las herramientas para el desarrollo de la etapa se encuentran:
    a. Comunicaciones cifradas, e-mail firmado digitalmente, herramientas de software de cifrado de archivos y documentos.
    b. Se deben adquirir firmas digitales para aquellos funcionarios autorizados a remitir los informes de casos a las autoridades competentes, estas firmas son suministradas por entidades certificadoras oficiales en cada país y se utilizan para firmar digitalmente un archivo y comprobar su validez.

2. PLAN DE CONTINUIDAD DE NEGOCIOS: MARCO TEÓRICO

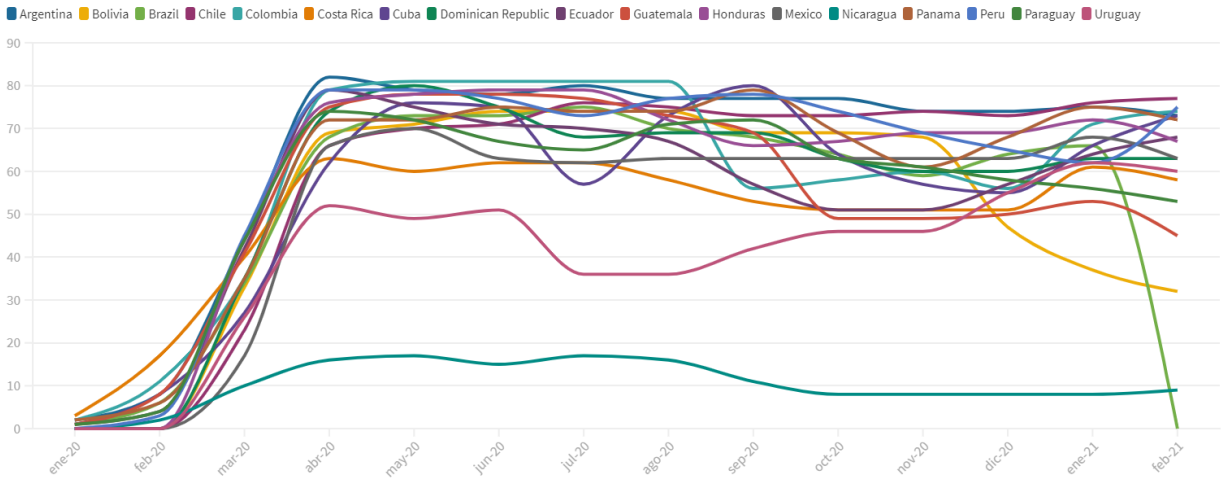
34. Las Unidades de Inteligencia Financiera, al igual que todas las entidades, deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes que puedan afectarles y que podrían impactar la ejecución de sus operaciones. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permitan a la UIF operar tras un incidente o una situación grave como la pandemia del COVID-19[49] en un plazo de tiempo que no comprometa la continuidad de sus operaciones. Lo anterior, permitirá que las UIF puedan tomar acciones oportunamente, además de mitigar el impacto en los tiempos de recolección, análisis y procesamiento de la información crítica y la oportunidad de entrega de información a las autoridades competentes.

35. Derivado de la pandemia del COVID-19, la comunidad internacional se vio en la necesidad de implementar medidas y aplicar recursos a fin de mitigar en la medida de lo posible el impacto de este fenómeno en la población. Como parte de estas medidas, los países tomaron acciones tales como, distanciamiento social y particularmente, el diseño de cuarentenas o *lockdowns* de duración e intensidad[50] heterogénea, que incluyeron medidas de índole diversa[51].

36. En particular, entre los países miembros del GAFILAT se tuvieron medidas diferenciales de severidad de las cuarentenas, presentándose los picos de restricción entre los meses de marzo a agosto de 2020, tal como muestra el índice de contención y cierre desarrollado por la Universidad de Oxford[52], el cual mide factores como el cierre de establecimientos públicos, de sitios de trabajo, cancelación de eventos públicos, restricciones de congregación de personas, cierre de transporte público, requerimientos de permanecer en casa, restricciones de movimiento dentro del país y restricciones a viajes internacionales.

[49] Declarada oficialmente como pandemia por la Organización Mundial de la Salud el 11 de marzo 2020
[50] https://ig.ft.com/coronavirus-lockdowns/
[51] https://www.bsg.ox.ac.uk/research/research-projects/coronavirus-government-response-tracker
[52] https://www.bsg.ox.ac.uk/sites/default/files/2020-12/BSG-WP-2020-032-v10.pdf

Figura 2 - Índice de contención y cierre. Universidad de Oxford. Países miembros del GAFILAT



37. Lo anterior implicó que las instituciones públicas y privadas se vieran en la necesidad de desplegar sus planes de continuidad de negocio (PNC) implementando estrategias como el trabajo remoto, ya sea de forma parcial o total. Las empresas, en la mayoría de los casos, no estaban preparadas para este tipo de estrategias, lo cual ha afectado el desarrollo normal de sus funciones.

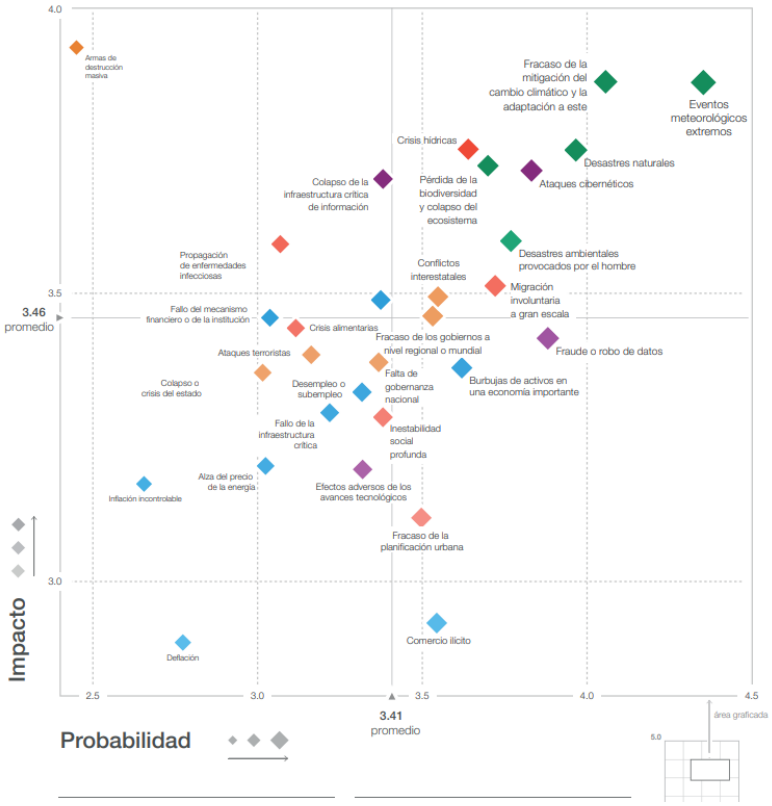
38. En especial, en múltiples PCN no se contemplaba el escenario de una pandemia que implicara la implementación de medidas de trabajo remoto a la totalidad o gran parte del personal. Sin embargo, este tipo de escenarios ya habían sido pronosticados, por ejemplo, el Foro Económico Mundial (FEM), en diversos informes de riesgos mundiales y en particular, en la versión del año 2019[53], planteaban la "propagación de enfermedades infecciosas" como uno de los principales riesgos mundiales en términos de impacto.

39. En dicho informe el FEM establecía que "la debilidad de la preparación básica en los distintos países es un obstáculo importante para responder a una pandemia"[54], de tal

[53] Foro Económico Mundial (2019). Informe de Riesgos Mundiales. https://www.weforum.org/reports/the-global-risks-report-2019
[54] Ibid, pág. 48

forma que "cuando surja un brote, es posible que no se cuente con las respuestas apropiadas o que se apliquen con retraso, y se contará con recursos limitados para tratar con cualquier otro evento epidémico que pudiera surgir"[55], como en efecto, ocurrió con la pandemia de COVID-19.

Figura 3 - Foro Económico Mundial. Informe Mundial de Riesgos 2019. Principales riesgos



40. En el caso específico de las UIF esta problemática, según el comunicado emitido por el GAFILAT en abril de 2020[56], puede tener repercusiones en sus principales actividades misionales, tales como la reducción o pausas de las actividades, reducción del personal, disminución en el número de reportes recibidos y en general dificultades para el desarrollo de las actividades de análisis, procesamiento y reporte de información. Ante esta situación se vuelve fundamental el desarrollo de un plan de continuidad del negocio que garantice la preparación y planeación de las UIF para enfrentar este tipo de situaciones y permitirles operar o reanudar las actividades de una forma "normal".

[55] Ibid
[56] GAFILAT (2020). Comunicado del GAFILAT sobre Covid-19 – Coronavirus. 8 de abril de 2020.

41. El objetivo de este capítulo es presentar los conceptos relacionados con la gestión de la continuidad del negocio, enfocados principalmente en los riesgos tecnológicos y los procesos críticos de una UIF para que sirvan de marco y guía en la planeación y diseño de estrategias de trabajo para enfrentar incidentes, desastres o situaciones que afecten su normal operación.

2.1. Proyectos de continuidad de negocio

42. El diseño de un sistema de gestión de continuidad de negocio (SGCN) debe corresponder a la intensidad y tipo de impacto que la organización, en este caso, la UIF, pueda o no pueda asumir luego de una interrupción.

43. De esta forma, según la norma ISO 22301 – Seguridad y resiliencia, sistema de gestión de continuidad de negocio, el SGCN dependerá de diversos aspectos, tales como el análisis del contexto interno y externo de la organización, el alcance que tendrá el SGCN, incluyendo las partes que serán incluidas en el mismo, así como los productos y servicios que se incluirán en el SGCN. En este sentido, teniendo en cuenta las características legales, funcionales y de otra índole que enmarcan el desarrollo de los objetivos misionales de una UIF, podrán influenciar el alcance del mismo.

44. En línea con otras normas de gestión de riesgo, en particular el estándar ISO 31000[57], un pilar fundamental para un SGCN exitoso, es demostrar, por parte de la alta dirección, específicamente el Director de UIF, "Liderazgo y compromiso"[58], a través de acciones tales como:
    a. Asegurando que los recursos necesarios para el SGCN se encuentren disponibles.
    b. Dirigiendo y apoyando el personal que contribuye a la eficacia del SGCN.

45. En este orden de ideas, es deseable que las UIF documente y mantengan planes y procedimientos para la continuidad de negocio, que brinden orientación e información a los equipos para tener la capacidad de reaccionar ante una interrupción y ayudar a la organización en la respuesta y recuperación. Según el alcance se pueden distinguir 3 tipos de planes de continuidad de negocio
    a. **Plan de Continuidad de Negocio (PCN)**: Establece la continuidad de una organización desde múltiples perspectivas: infraestructura TIC, recursos humanos,

[57] Familia de normas relativas a la gestión de riesgo, codificada por la International Organization for Standardization ISO. El propósito de la norma ISO 31000 es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo. La norma se basa en tres (3) componentes. Los principios, el marco de referencia y el proceso de la gestión de riesgo.
[58] ISO 22301, 5.1.

mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo el impacto de una inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores o como lo es recientemente el confinamiento por una pandemia.

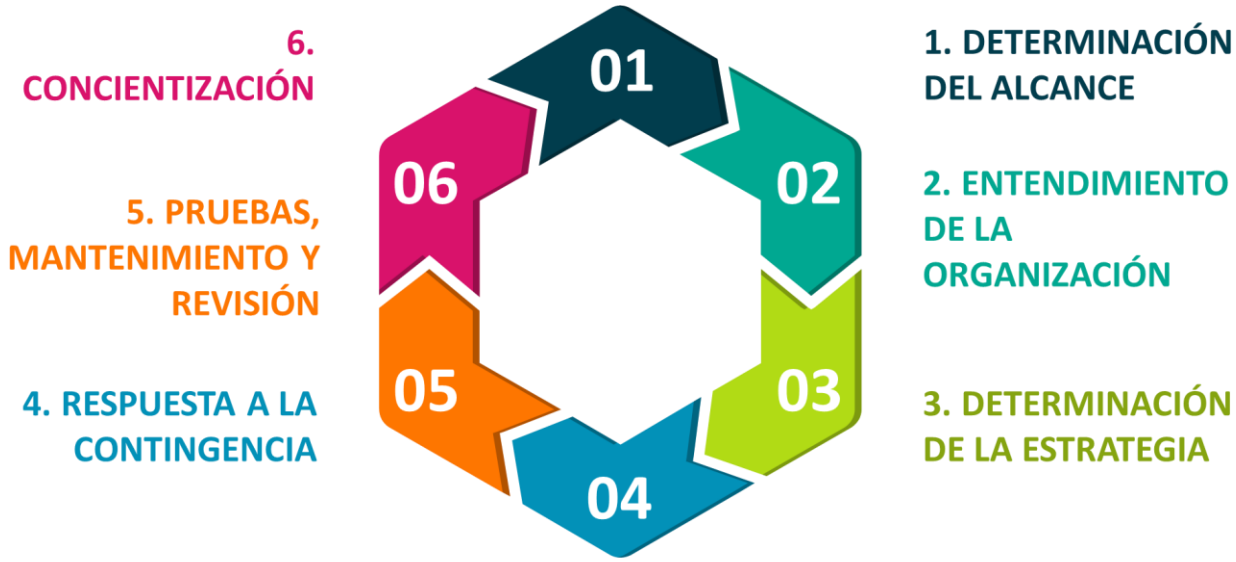
b. **Plan de Continuidad TIC (o Plan de Contingencia TIC, PCTIC)**: Es uno de los planes que forman el plan de continuidad de negocio de la organización, pero restringido al ámbito de las tecnologías de información y comunicación. Mientras que un PCN sirve de disparador para los diferentes planes de contingencia, un PCTIC se limita al ámbito tecnológico.
c. **Plan de Recuperación ante Desastres (DRP)**: En este caso, su fase de análisis es menos profunda y se enfoca al ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe. Por ejemplo, si se tiene un plan de desastres para la página web de comercio electrónico, el DRP contendrá todos los pasos para la recuperación de la aplicación.

46. La implementación de un PCN presenta varias ventajas, a continuación, se destacan las más importantes:
    a. Mantener el nivel de servicio en límites predefinidos.
    b. Determinar la capacidad que puede tener la empresa en caso de materializarse un riesgo de alto impacto.
    c. Mitigar permanentemente el riesgo de interrupción de servicios.
    d. Administrar una eventual crisis, protegiendo principalmente la integridad de las personas y activos de la empresa.
    e. En caso de crisis garantizar un efectivo flujo de las comunicaciones internas y externas.
    f. Garantizar el principio de la "empresa en marcha" logrando la recuperación de la operación crítica en el menor tiempo posible.
    g. Minimizar las pérdidas, contener el impacto y minimizar la probabilidad de cometer errores.

2.2. Fases de la continuidad de negocios

47. Como toda estrategia organizacional, existe un proceso y buenas prácticas definidas para el desarrollo e implementación de un SGCN. El objetivo es obtener, como parte de los resultados del SGCN, el PCN de la organización. En la siguiente gráfica se observan las fases generales de este proceso.

Figura 4 - Fases de la gestión de continuidad de negocio.



48. Estas fases se describen a continuación:

2.2.1. Determinación del alcance

49. Esta es una fase preliminar en la que se debe clasificar cada una de las áreas de la organización dándole una prioridad a cada una de ellas, con el fin de determinar cuáles son las más vulnerables y de esta manera establecer lineamientos iniciales relativos a la continuidad de negocio. En este punto, como se expuso previamente, es clave la participación de la alta dirección.

50. Se busca así, determinar los elementos de la organización van a ser el foco de la mejora de la continuidad. Por tanto, estará implicado el personal, los activos de información, los sistemas informáticos, y otros servicios y procesos de la organización.

51. Se puede plantear el enfoque desde el punto de vista del activo, o del proceso:
    a. El enfoque por activo asume la mejora de la continuidad de un conjunto de activos, y a partir de estos obtiene la información de los procesos que los utilizan. Este enfoque es más propio de un DRP o cuando el proyecto será abordado por parte del departamento técnico.

b. El enfoque por proceso pretende mejorar la continuidad de un determinado proceso, con independencia de los activos de informática que le den soporte. Este enfoque es más propio del negocio.

2.2.2. Entendimiento de la organización

52. Siguiendo los lineamientos de la ISO 22301, se debe determinar los aspectos externos e internos que sean relevantes para el cumplimiento de los propósitos de la UIF y que afecten su capacidad para lograr el(los) resultado(s) deseado(s) de su SGCN[59].

53. De igual forma, comprender y evaluar los requisitos legales y reglamentarios vigentes relacionados con la continuidad de sus productos o servicios, actividades y recursos[60].

54. Durante esta primera fase se debe recolectar toda la información de la organización con el fin de identificar cuáles son los procesos de negocios críticos (activos), cómo se les dará soporte y cuáles son las necesidades que se presentan.

55. La primera tarea es determinar los usuarios finales del proceso que se han seleccionado en el alcance como parte del PCN. El siguiente paso, es recopilar toda la información sobre las aplicaciones que se han identificado en el paso anterior, para obtener los detalles de su funcionamiento, instalación, proveedor, etc.

56. Asimismo, es relevante establecer, asignar y comunicar, por parte de la alta dirección, la responsabilidad y autoridad para los roles importantes asociados al SGCN[61].

2.2.2.1. Análisis de impacto del negocio (BIA)

57. Es uno de los ejes principales del PCN, al contener las necesidades de los procesos que se han definido dentro del alcance. La UIF deberá usar los procesos para analizar el impacto dentro de una situación de interrupción del proceso y determinar así, los requisitos y prioridades de la continuidad de negocio[62]. Así se podrá clasificarlos según su criticidad y su dependencia de los activos tecnológicos.

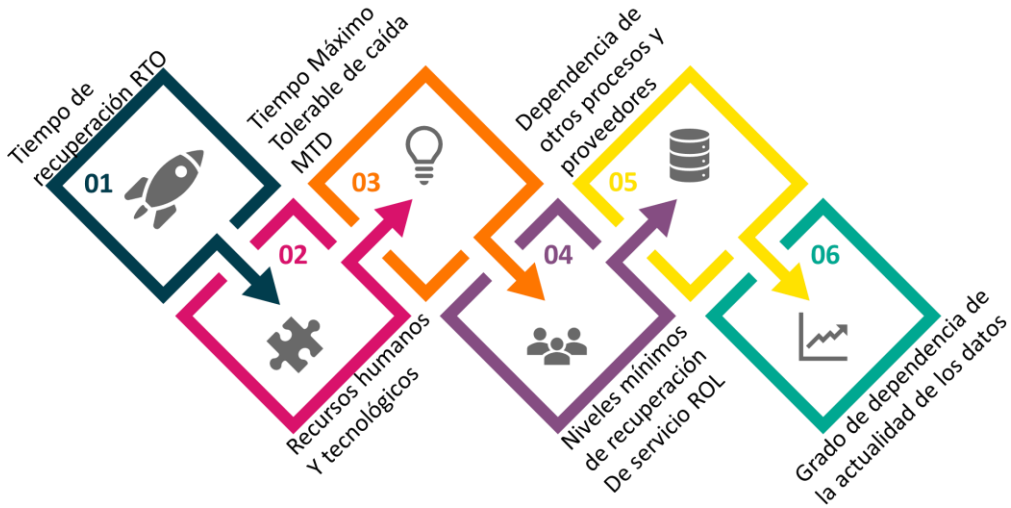
58. En la determinación del BIA, cada proceso debe[63]:

[59] ISO 22301. 4.1 Comprender la organización y su contexto.
[60] Ibid. 4.2.2. Requisitos legales y reglamentarios
[61] Ibid. 5.2.3 Funciones, responsabilidades y autoridad.
[62] Ibid. 8.2.2 Análisis de impacto al negocio
[63] Ibid

a. Definir los tipos de impacto y criterios relevantes para el contexto de la organización.
b. Identificar las actividades que soportan la provisión de productos y servicios.
c. Evaluar el impacto a lo largo del tiempo que resulte de una interrupción de dichas actividades.
d. Identificar el periodo de tiempo dentro del cual el impacto de no reanudar las actividades sería inaceptable para la UIF.
e. Priorizar los periodos de tiempo dentro del periodo identificado en el numeral anterior para reanudar las actividades interrumpidas en una capacidad mínima aceptable.
f. A partir de lo anterior, identificar actividades prioritarias.
g. Determinar los recursos que se requieren para soportas las actividades prioritarias.
h. Determinar las dependencias, incluyendo contrapartes. Por ejemplo, en el caso de una UIF, SO, autoridades competentes y de orden público, organismos judiciales o entidades de inteligencia, entidades análogas u homólogas del exterior; así como las interdependencias de las actividades prioritarias.

59. De esta forma, el BIA contiene los requisitos temporales y de recursos de los procesos dentro del alcance y, junto con el Análisis de Riesgos, define las iniciativas a implantar para recuperar los procesos en situación de contingencia. La siguiente figura muestra los elementos principales a identificar durante el análisis de impacto de negocio

Figura 5 - Elementos para elaboración del BIS. Fuente: (INCIBE, 2020).



60. Estos conceptos se presentan a continuación:
    a. Tiempo de recuperación o RTO (Recovery Time Objective). Este es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. Este valor tiene un gran componente de subjetividad.
    b. Tiempo máximo tolerable de caída o MTD (Maximum Tolerable Downtime). Este es el tiempo que un proceso puede permanecer caído antes de que se produzcan consecuencias desastrosas para la organización.
    c. Niveles mínimos de recuperación de servicio o ROL (Revised Operating Level). Este es el nivel mínimo de recuperación que debe tener una actividad para que la consideremos como recuperada, aunque el nivel de servicio no sea el óptimo.
    d. Grado de dependencia de la actualidad de los datos o RPO (Recovery Point Objective). Este valor determina el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de copias de la organización, y no guarda relación con el RTO visto anteriormente

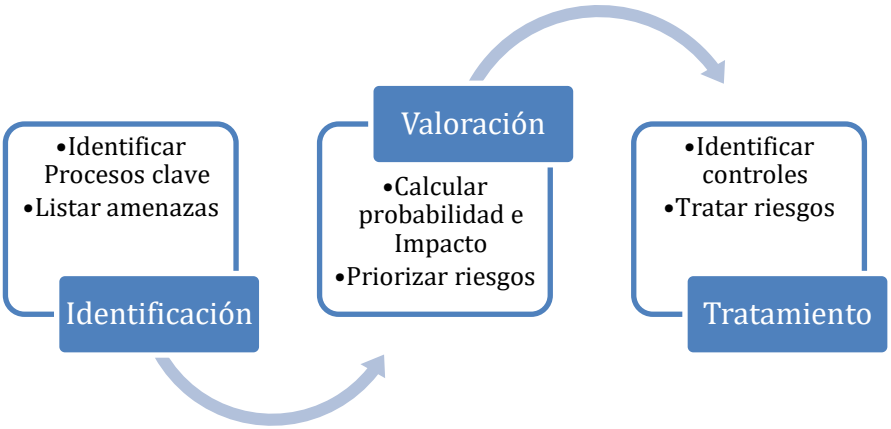
2.2.2.2. Análisis de riesgo

61. El análisis de riesgo consiste en determinar las amenazas a las que está expuesta la organización: robo de información sensible, desastre natural, pérdida de suministro eléctrico, caída del servidor de correo, pandemia, etc. A diferencia de otros casos, en este tipo de proyectos, el análisis de riesgo se centra en aquellas amenazas que implican una indisponibilidad de los procesos del alcance. En el análisis de riesgo[64] se identifica el riesgo de interrupción de las actividades prioritarias y de los recursos requeridos, se analizan y evalúan los riesgos identificados y se determinan cuáles riesgos requieren de un tratamiento[65].

62. De una forma más detallada, una vez se obtiene el listado de las amenazas, se determina la probabilidad y el impacto de cada una de estas. Esto puede hacerse utilizando una escala variable cualitativa, por ejemplo, de uno a cinco: de "Muy baja" a "Muy alta". Luego se realiza el producto de la probabilidad por el impacto de cada amenaza, con el fin de obtener el nivel de riesgo de la amenaza y que pueda servir como criterio de priorización de riesgos. De esta manera se obtiene un listado de los riesgos de la organización, donde cada registro será una amenaza, un valor de impacto y uno de probabilidad. En la siguiente gráfica se muestra el proceso general de análisis de riesgo.

[64] Ibid 8.2.3. Análisis de riesgos.
[65] Existen diversas opciones de tratamiento, dentro de las cuales están la aceptación, transferencia, mitigación o eliminación del riesgo. ISO 31.000

Figura 6 - Etapas del análisis de riesgo



63. Por último, se establece el tratamiento de los principales riesgos identificados, es decir aquellos con mayor impacto se deben tratar de manera adecuada mediante una de las siguientes estrategias: Transferir, Eliminar, Asumir, Mitigar.

2.2.3. Determinación de la estrategia

64. Una vez estén definidos los procesos críticos de negocio, se debe establecer que, si se presentara una amenaza, la UIF estaría en la capacidad de recuperar estos procesos en corto plazo, o si, por el contrario, requiere de un tiempo mayor, para lo cual, se deben establecer estrategias para la continuidad de negocio.

65. Estas estrategias deben considerar[66] opciones para el antes, durante y después de una interrupción a partir de los resultados del análisis de impacto al negocio y la evaluación de riesgos.

66. La determinación de estrategias y soluciones involucra aspectos tales como[67] el logro de los requisitos para continuar y recuperar las actividades prioritarias dentro del tiempo identificado y la capacidad acordada y; los costos y beneficios de la estrategia.

67. En este sentido, para la determinación de la estrategia, se debe disponer de la siguiente información:
    a. Los procesos críticos del negocio, sus tiempos necesarios de recuperación y sus requisitos de pérdida de datos.

[66] Ibid. 8.3.1 Generalidades.
[67] Ibid. 8.3.2. Identificación de estrategia y soluciones

b. Los recursos implicados en cada uno de los procesos: aplicaciones, infraestructura, etc.
c. Los tiempos de recuperación de cada uno de los recursos que puede garantizar el personal técnico.
d. Los riesgos a los que se encuentra sometida la infraestructura TI.

68. A partir de esta información, se puede determinar cuál es la diferencia entre las necesidades de los procesos de negocio incluidos en el alcance y las capacidades de los recursos que utilizan. De este modo, se identifica si los recursos actuales y sus estrategias de recuperación permitirían cubrir el MTD establecido para cada proceso. Algunos elementos potencialmente afectables por una contingencia son los siguientes:
    a. Personal. Según el personal crítico identificado en el BIA, se debe evaluar las diferentes opciones para mitigar su ausencia.
    b. Locaciones. Deben evaluarse situaciones en las que no se disponga de ubicación para trabajar.
    c. Tecnología. Para las diferentes tecnologías implicadas en los activos que dan soporte al proceso se deben valorar posibles alternativas de funcionamiento o medidas complementarias.
    d. Información. Considerar todos aquellos aspectos relacionados con la disponibilidad y salvaguarda de la información relacionada con los procesos críticos.
    e. Proveedores. Garantizar que los proveedores críticos tienen unos tiempos de respuesta acordes a las necesidades de nuestra empresa, y que no estamos expuestos a que nos trasladen sus posibles contingencias

2.2.4. Respuesta a la contingencia

69. En esta fase se elegirán las estrategias necesarias que se pondrán en marcha en caso de presentarse un incidente o un desastre y se creará un plan de crisis en donde se documentará toda la información. Los esquemas de respuesta permiten[68] una "advertencia oportuna y la comunicación a las partes interesadas relevantes" para que, de esta forma, se brinde a la UIF procedimientos para gestionar la organización durante la interrupción, incluyendo los equipos responsables para responder durante dicha interrupción.

70. Este proceso comienza con la implantación de las iniciativas identificadas en la fase anterior, y seguirá una fase de clasificación y priorización de medidas, en función del proceso afectado por su implantación y la criticidad de éste.

[68] Ibid 8.4 Planes y procedimientos para la continuidad de negocios.

71. Esta documentación se ejecuta en forma de árbol jerárquico, donde el elemento superior gestiona el momento crítico inmediatamente posterior a la crisis, los elementos intermedios ponen las bases para la recuperación de la infraestructura, y los nodos inferiores establecen los procedimientos técnicos detallados para dicha recuperación.

72. Este proceso es organizado en torno a los siguientes elementos:
    a. Plan de Crisis: Este documento es el elemento central en la gestión de la situación de crisis, cuyo objetivo es evitar tomar decisiones improvisadas que puedan empeorar la crisis o que, simplemente, no se tomen.
    b. Planes Operativos de Recuperación de Entornos: Estos documentos pueden abarcar uno o más entornos independientes y contienen información específica sobre el entorno al cual aplican. Por ejemplo, un entorno puede ser un ERP, el correo electrónico. Tras el disparo de los diferentes Planes Operativos, cada una de las infraestructuras afectadas comenzará su proceso de recuperación, tomando como base para ello el elemento último de la ejecución de la estrategia de continuidad: los procedimientos técnicos de trabajo
    c. Procedimientos Técnicos de Trabajo: Esta es toda documentación que describe cómo se debe llevar a cabo las tareas necesarias para la gestión y recuperación de una aplicación, sistema, infraestructura o entorno. Aunque intrínsecamente no son parte de la continuidad del negocio sino de la operación diaria, es en una situación de crisis, cuando se vuelven más importantes. Por lo tanto, estos documentos contienen gran cantidad de información específica a cada uno de los entornos: direcciones IP, versionado de programas, listado detallado de comandos, tablas de enrutamiento, recuperación de copias de base de datos, puesta en marcha de aplicaciones, etc.

73. Es así que sería recomendable que cada plan incluya[69]:
    a. Propósito, alcance y objetivos.
    b. Funciones y responsabilidades del equipo que implementará el plan.
    c. Acciones para implementar las soluciones.
    d. Información de soporte necesaria para activar, operar, coordinar y comunicar las acciones de los equipos.
    e. Requisitos de los recursos y reportes.
    f. Proceso para darse de baja.

[69] Ibid 8.4.4.3

2.2.5. Pruebas, mantenimiento y revisión

74. La UIF puede implementar un programa de ejercicios y pruebas para validar la eficacia de las soluciones y estrategias de continuidad de negocio planteadas[70], así como la revisión tanto por auditoría[71] como por la alta dirección[72], con el objetivo de asegurar la pertinencia, idoneidad y eficacia del PCN.

75. Para esto, será necesario contar con recursos humanos y tecnológicos que permitan crear planes de prueba, mantenimiento y revisión, para identificar cuáles son las buenas prácticas y en qué se debe mejorar. Se deben llevar a cabo diferentes pruebas sobre los entornos definidos en el alcance, con diferentes grados de complejidad y elaboración.

76. Entre todas las pruebas, se deben realizar pruebas de todos los entornos al menos una vez al año para cubrir el conjunto de amenazas definidas como potencialmente catastróficas. En la ejecución de las pruebas, es necesario llevar a cabo una planificación previa que tenga en cuenta los siguientes aspectos:
    a. Personal técnico implicado en las pruebas.
    b. Usuarios del aplicativo o proceso implicado en las pruebas.
    c. Personal externo implicado en las pruebas: clientes, proveedores, etc..
    d. Descripción de las pruebas a realizar.
    e. Descripción del resultado esperado tras la ejecución de las pruebas.
    f. Hora y fecha de realización de las pruebas.

77. El proceso de mantenimiento del PCN implica entre otros aspectos, el mantener actualizada toda la documentación cada vez que se produzca un cambio significativo en la organización, a nivel de infraestructuras TIC, de personal, o de cualquier otro aspecto implicado en los procesos críticos.

78. Por su parte, las pruebas buscan mostrar los distintos tipos de escenarios de contingencia que deben ser testeados. A pesar de que el plan de mantenimiento contiene aquellos eventos que deben disparar una revisión o modificación del sistema (por ejemplo, el cambio de un proveedor, atravesar con éxito una fase de crisis), en la ejecución de los planes de prueba es vital para garantizar la salud del PCN.

[70] Ibid. 8.5 Programa de ejercicios.
[71] Ibid. 9.2 Auditoría interna.
[72] Ibid. 9.3. Revisión por la dirección

2.2.6. Concientización

79. Se estima que resulta relevante crear una cultura dentro de la UIF para que todos los empleados conozcan el plan de acción y se apropien de la situación, al igual que entiendan cuál será su rol dentro de este plan. Es importante, a estos efectos, plantear un proceso de concienciación que contemple la descripción de los elementos que utilizamos en la continuidad (análisis de impacto sobre el negocio, plan de crisis, estrategias de recuperación, etc.). Además, deben de considerarse aspectos como las responsabilidades, pruebas que se deben realizar, etc.

80. El público objetivo en este caso deberá ser tanto el personal técnico como el personal de negocio que tenga algún tipo de relación con los procesos críticos que han sido establecidos del alcance.

2.3. ISO 22301: Sistema de gestión y continuidad de negocio

81. La norma técnica ISO 22301 es una estándar internacional de gestión de continuidad de negocio que proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de la organización. Se usa para asegurar a las partes interesadas clave de la empresa estén totalmente preparadas y que puedan cumplir con los requisitos internos, regulatorios y del cliente.

82. Esta norma proporciona a las organizaciones un marco que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y comercializando[73]. En el entorno de una UIF, la ISO 22301 busca que las operaciones críticas misionales, tales como recepción, análisis y comunicación de información, así como en aquellas UIF que realicen actividades de supervisión, puedan continuar bajo un estándar mínimo aceptable.

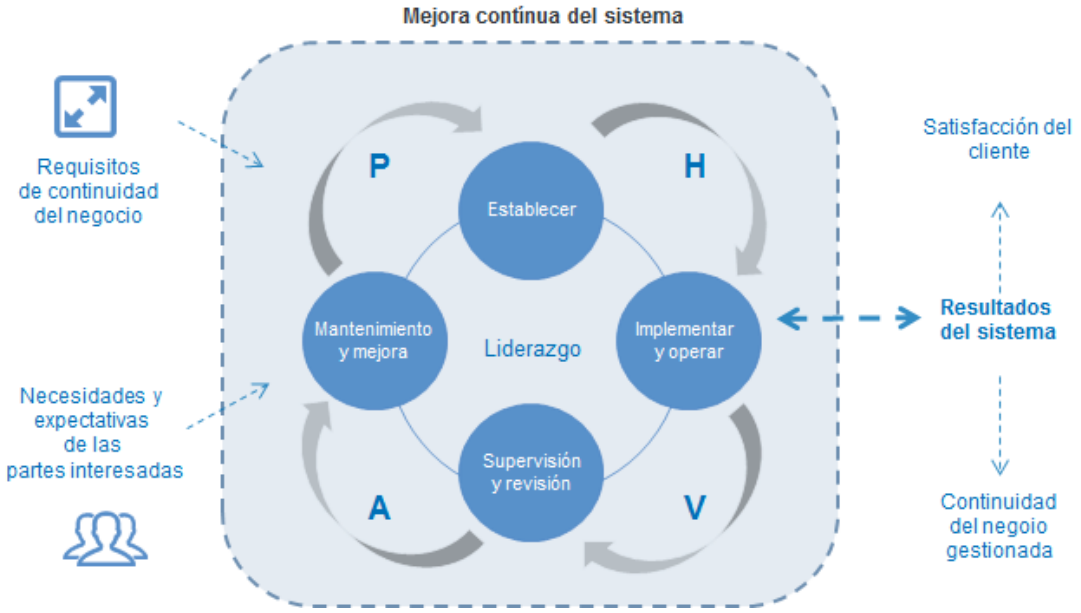
83. Según la norma (ISO 22301, 2019) los planes para la continuidad del negocio deben incluir:
    a. Propósito, alcance y objetivos.
    b. Funciones y responsabilidades del equipo que implementara el plan.
    c. Acciones para implementar las soluciones.
    d. Información de soporte necesaria para activar, operar, coordinar y comunicar las acciones de los equipos.
    e. Interdependencias internas y eternas.

[73] https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301

f. Requisitos de los recursos.
g. Requisitos para los reportes.
h. Un proceso para darse de baja.

84. La norma ISO 22301:2019 – Plan de Continuidad de Negocio, cuyo esquema general se presenta a continuación, es el estándar internacional más reconocido relativo a continuidad de operaciones.

Figura 7 – Esquema general norma ISO 22301



Fuente: http://www.agoraconsultores.es/iso-22301-continuidad-del-negocio/

85. Este estándar incorpora los elementos presentados previamente de forma que su implementación pueda ser realizada de manera exitosa por una organización, en este caso, una UIF. Por lo anterior, se adoptará como referente metodológico.

86. Además, se incorporarán elementos de la ISO 27001: 2017, Sistemas de gestión de seguridad de la información – Requisitos, e ISO 27002: 2017, Técnicas de seguridad – Código de prácticas para la gestión de seguridad de la información. Esto debido a que la continuidad de operaciones debe asegurar la confidencialidad y seguridad de la información que recibe y disemina la UIF.

87. En este sentido, debe tenerse en cuenta la Nota Interpretativa de la R. 29 del GAFI que establece que las UIF deben "implementar normas que rijan la seguridad y confidencialidad de la información, incluidos los procedimientos de manejo,

almacenamiento, divulgación y protección de la información, y de acceso a la información; garantizar que el personal de la UIF cuente con los niveles de autorización necesarios en cuanto a la seguridad y que entiendan sus responsabilidades en el manejo y comunicación de información delicada y confidencial; y asegurar el acceso limitado a sus instalaciones y a la información, incluyendo los sistemas de tecnología de la información".

88. Cabe anotar que las falencias en la protección de información, según el Grupo Egmont se considera como un Criterio de Incumplimiento con los Estatutos y/o los Principios de Intercambio de Información entre Unidades de Inteligencia Financiera[74]. Es más, para tal fin, el Grupo Egmont ha desarrollado el Manual de Seguridad de Unidades de Inteligencia Financiera[75] (*Securing Financial Intelligence Units Manual*) el cual incluye "medidas comprehensivas requeridas por una UIF incluyendo físicas, personal, manejo de información y seguridad de tecnologías de información.

89. El documento contiene una guía detallada para los miembros actuales y futuros de Egmont para ayudar a evaluar y abordar cualquier elemento de seguridad al interior de la UIF". Esto debido a que el grupo Egmont que "debido a la naturaleza confidencial de la información intercambiada entre UIF, la seguridad física, de personal y de información es suprema"[76].

Figura 8 – Esquema general norma ISO 27001

[74] Egmont (2014). Proceso de Apoyo y Cumplimiento.
[75] Egmont (2014). Annual Report 2012 – 2013. P. 14
[76] Ibid.

90. Como puede observarse, múltiples aspectos, como por ejemplo el establecimiento del contexto, la determinación del alcance, el liderazgo y compromiso, la evaluación de desempeño y mejora, coinciden con otros estándares ISO como la ISO 31000 y en particular, la ISO 22301, aunque analizados desde perspectivas diferentes.

3. DIAGNÓSTICO DE PLAN DE CONTINUIDAD DE OPERACIONES EN PAISES MIEMBROS DEL GAFILAT

91. Con el objetivo de tener un diagnóstico relativo al impacto en las operaciones de las UIF como producto de la pandemia de COVID-19, de las medidas implementadas por las UIF durante este periodo y los planes programados de continuidad de operaciones, se realizaron dos (2) acciones
    a. Diseño y aplicación de un instrumento de recolección de información (64.7% de los países del GAFILAT participaron)
    b. Entrevistas semiestructuradas con UIF de la región (41% de los países del GAFILAT).

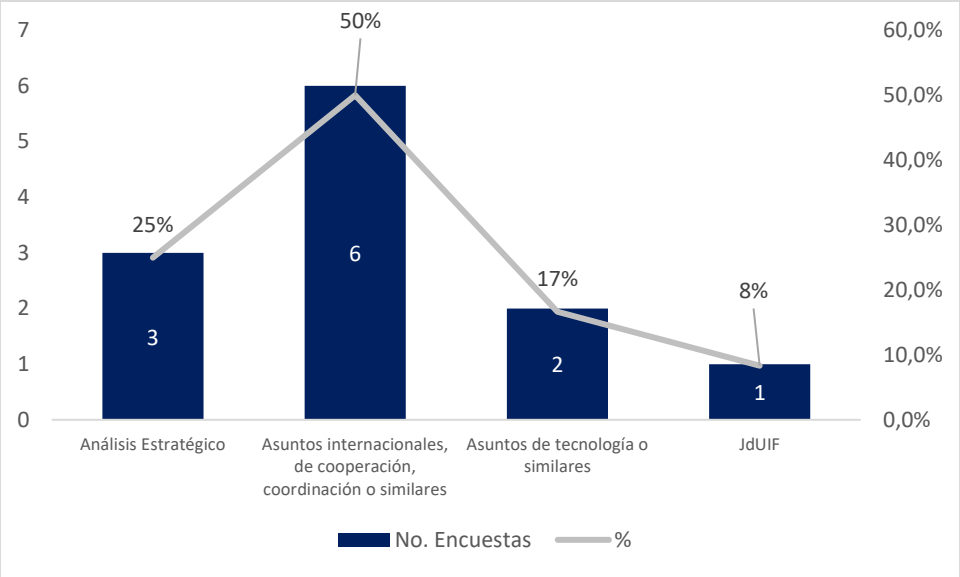
92. A continuación, se presentan las principales conclusiones producto del proceso de aplicación del instrumento y realización de las entrevistas. Se cubrirán diez (10) aspectos i. información general de la UIF; ii. información operativa; iii. de impacto COVID-19 en las operaciones de la UIF; iv. PCN; v. Personal y PCN; vi. Oficinas, PCN y ambiente físico; vii. tecnología de información de apoyo al PCN; viii. seguridad de la red; viii. administración y monitoreo de información y; ix. otros elementos importantes del PCN; x. circunstancias adicionales; xi. Actividades de supervisión y; xii. aspectos relativos a las entrevistas no estructuradas

93. Cabe anotar que, en lo subsecuente, se hace referencia a los países que respondieron el instrumento de recolección de información. Por lo tanto, **las estadísticas y porcentajes se calcularán sobre esa base** y no sobre todos los países miembros de GAFILAT.

3.1. Información general de la UIF

94. Las encuestas fueron diligenciadas por funcionarios con diferentes roles dentro de la UIF. La mayor proporción de encuestas (50%) fueron diligenciadas por personal de asuntos internacionales, de cooperación, coordinación o similares, seguidos de análisis estratégico (25%), asuntos de tecnología o similares (13%) y en el caso de una de las encuestas (8%), por el Director de UIF. En el siguiente gráfico se presenta el resumen de diligenciamiento de información por rol.

Figura 9 - Roles que diligenciaron el instrumento



95. En términos del número de funcionarios, existe heterogeneidad respecto a este factor, variando de UIF con cerca de 200 funcionarios a UIF con algo más de 20. Esta variable es relevante en el momento de desplegar un PCN y en particular, medidas de trabajo remoto. A mayor número de funcionarios, mayor complejidad en implementar dicha estrategia.

96. De igual forma, también se presentan variaciones con relación a la proporción de funcionarios de la UIF respecto al total de funcionarios. Esto, entre otras variables, depende a su vez que la UIF desempeñe labores adicionales a las tradicionales (análisis estratégico y análisis operativo), por ejemplo, de supervisión de SO.

3.2. Información operativa

97. Se recolectó información respecto a la volumetría de los ROS en los periodos enero – diciembre de 2019 y enero – octubre 2020. A pesar que los dos periodos no son equivalentes, puede establecerse tendencias relativas a la remisión de ROS por parte de los SO. En valores absolutos, el número de ROS remitidos en el periodo enero – diciembre de 2019 varía entre los 166 y los 590.682, mientras que para el periodo enero – octubre de 2020 dicha variación fluctúa entre los 157 y los 344.976 ROS.

98. Dentro de las UIF que diligenciaron el instrumento, el sector financiero es el sector preponderante en la remisión de ROS. En el periodo enero – diciembre de 2019, la

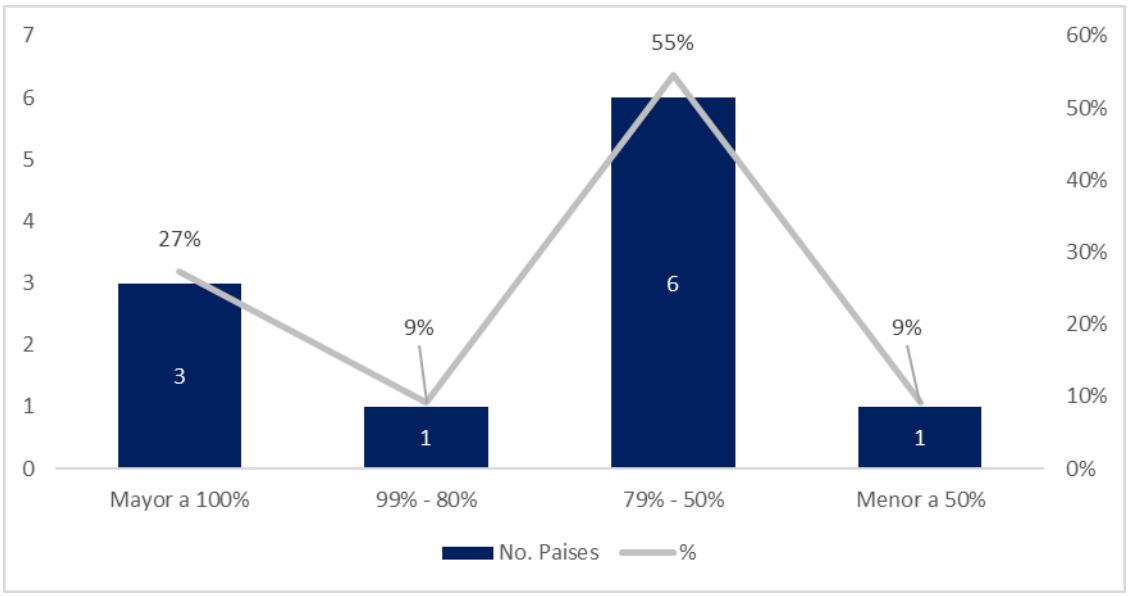
proporción de ROS remitidos por sector financiero estuvo entre el 51 y el 100%; en el periodo de enero – octubre de 2020, estas proporciones estuvieron entre el 47 y 100%.

99. El 82% de los países indican que la proporción de ROS remitidos por el sector financiero aumentó o se mantuvo igual en el periodo enero – octubre del 2020 versus el periodo enero – diciembre de 2019. El mayor incremento en proporciones presentó un 27% de ROS del sector financiero remitidos en el periodo indicado. El 18% de los países que diligenciaron el instrumento presentaron una reducción de la proporción de ROS remitidos por el sector financiero, sin que fuera extremadamente significativa dicha reducción (4% como máximo).

100. En términos generales, dentro de las razones para que el sector financiero, en su mayoría, presentara aumentos en la proporción de ROS puede deberse a factores como que bajo las medidas de confinamiento en aquellos países que las adoptaron, este sector se consideró como prioritario y mantuvo su operación de negocio. Igualmente, puede ser debido a la regulación a la que son sometidas usualmente este tipo de instituciones, que cuentan con planes de continuidad de operaciones que facilitan en alguna medida la implementación de acciones de trabajo remoto, entre otras.

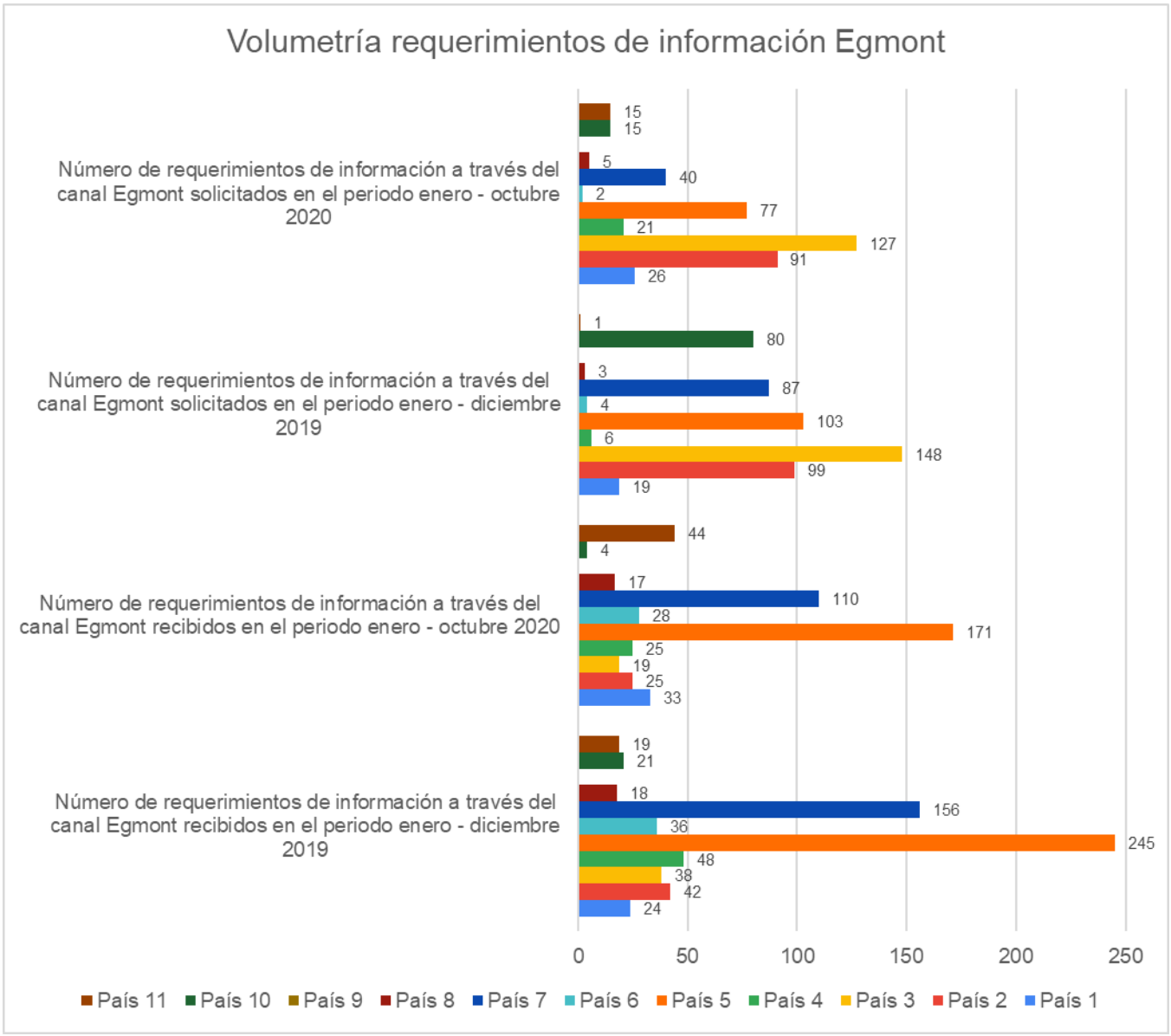
101. Un resultado interesante es el hecho que, a pesar que el periodo de 2020 corresponde al 83% del periodo de tiempo del año 2019 y a que en algunas jurisdicciones pueden darse picos de reporte hacia final de año, en el 27% de los encuestados, al compararse los ROS remitidos en el 2020 (parcial) versus el 2019, **se presentó un aumento de ROS en este periodo**. Estos aumentos en los volúmenes de ROS también se evidenciaron en el 30% de las entrevistas realizadas. En el 10% de las encuestas (un país), los ROS del 2020 representan entre 80 y el 99% de los ROS remitidos en el 2019, lo cual de manera preliminar podría indicar niveles de ROS similares entre los años 2019 y 2020. El 55% de los países, el número de ROS en el periodo de 2020 (parcial) versus el 2019 se encuentra entre el 50 y el 79%. En el 10% de los países (un caso), se presenta una proporción inferior al 50% al comparar el número de ROS del año 2020 y el 2019.

Figura 10 – Comparación porcentual de volumetría de ROS entre los periodos enero – noviembre de 2020 y enero – diciembre de 2019.



102. Respecto a los requerimientos de información a través del canal seguro Egmont, tanto recibidos como realizados, se tienen también diferencias importantes entre los países del GAFILAT. En el periodo enero – diciembre de 2019 dependiendo del país, se tuvieron entre 18 y 245 requerimientos de solicitud de información por parte de otras UIF, mientras que en el periodo enero – diciembre de 2020 dichas solicitudes se redujeron a niveles de entre 4 y 171 requerimientos. En lo que respecta con los requerimientos realizadas por la UIF, en totales se pasó de entre 1 y 148 requerimientos en el 2019 a entre 2 y 127 requerimientos en el 2020.

Figura 11 – Volumetría requerimientos de información recibidos y enviados a través del canal Egmont

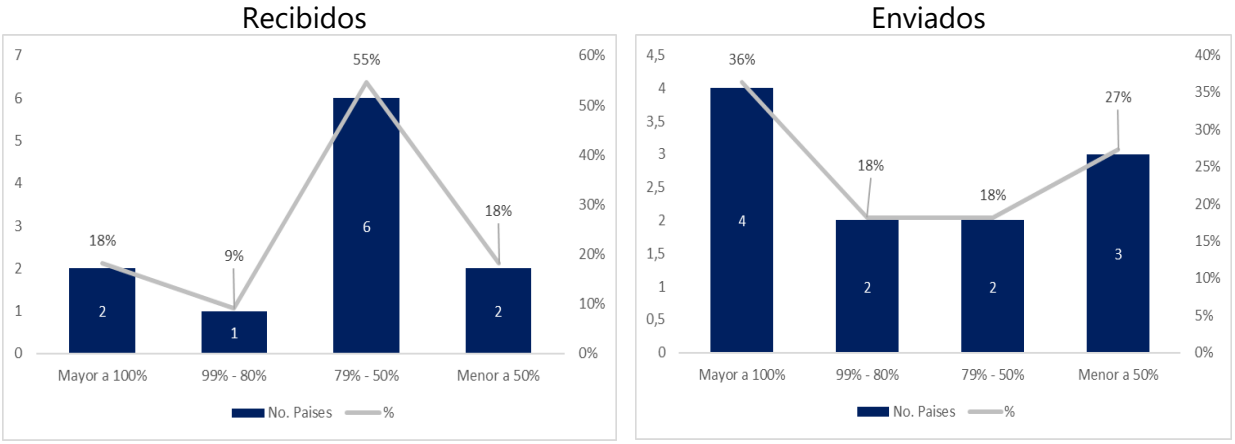


103. Al comparar país por país tanto en la recepción como la solicitud de requerimientos de información a través del canal seguro Egmont, se encuentra que, en el caso de requerimientos recibidos, el 18% de los encuestados presentaron incrementos en el número de requerimientos en el periodo enero-octubre 2020 en comparación con el periodo enero-diciembre de 2019; en el 9% la proporción de requerimientos recibidos en el 2020 estuvo entre el 80 y el 99% del número de requerimientos recibidos en el 2019, en la mayor proporción de países, equivalentes al 55% de los encuestados, la reducción

de requerimientos recibidos estuvo entre el 50 y el 79% de los requerimientos del año previo, mientras que el 18% presentó una reducción de solicitudes de información mayor al 50%.

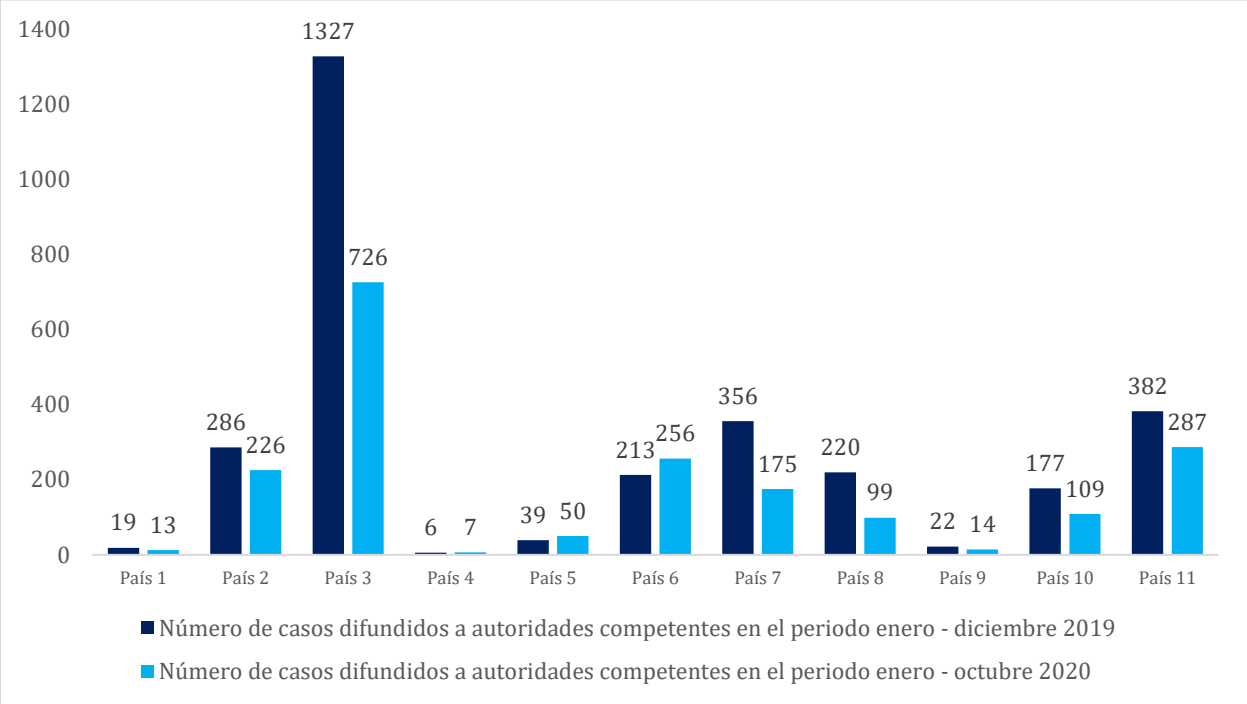
104. En relación con los requerimientos enviados por los países encuestados en los periodos de tiempo analizados, el 36% de los casos, aumentaron el número de solicitudes de información a través del canal Egmont. En el 18%, en lo corrido del 2020 se presentó una volumetría entre el 80 y el 99% del año 2019, lo que podría llevar a pensar que al menos en estos países los volúmenes de solicitudes que realizarán durante el 2020 se encontrarán en niveles cercanos a los del 2019. En dos países el nivel de requerimientos solicitados en lo corrido del 2020 se encuentra entre el 50% y el 79% de los requerimientos del año 2019.

Figura 12 – Comparación porcentual de volumetría de requerimientos a través del canal Egmont entre los periodos enero – octubre de 2020 y enero – diciembre de 2019.



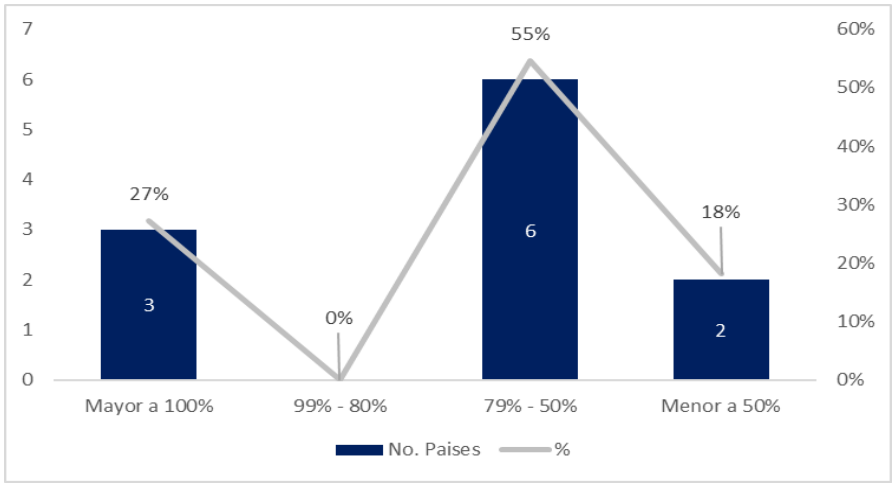
105. Al comparar el incremento o decrecimiento en el número de casos de inteligencia financiera difundidos por las UIF participantes, se encuentra que en el 27% de los países, a pesar de que el periodo analizado del 2020 no corresponde a la totalidad del año, se presentaron incrementos en el número de casos difundidos respecto al 2019. La mayor proporción de UIF (55%) presentaron reducciones entre el 21% y 50% de los casos difundidos. Sin embargo, como se expuso previamente, el periodo de tiempo analizado en el año 2020 no corresponde a la totalidad del año, por lo que podría pensarse que los volúmenes pueden estar ligeramente inferiores o cercanos a los alcanzados en el 2019. Solo el 18% de los encuestados, presentaron reducciones mayores al 50% en la difusión de casos de inteligencia financiera.

Figura 13 – Comparación de volumetría de casos de inteligencia financiera difundidos a autoridades competentes en los periodos enero – octubre de 2020 y enero – diciembre de 2019



106. Con esto, se observa que, en lo referente a **casos de inteligencia financiera, no todas las UIF analizadas presentaron reducciones en el número de casos difundidos a autoridades competentes, y en donde se presentaron reducciones, en la mayoría de los países dichas reducciones no fueron drásticas.**

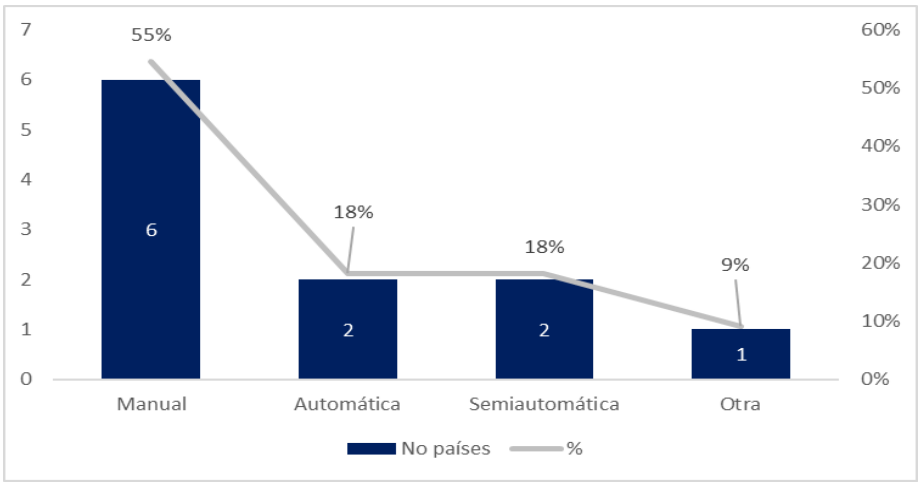
Figura 14 – Comparación porcentual de volumetría de casos de inteligencia financiera difundidos a autoridades competentes en los periodos enero – octubre de 2020 y enero – diciembre de 2019



107. En relación con la metodología utilizada para la lectura y clasificación de los ROS, más de la mitad de los encuestados (55%) ejecutan dicho proceso de manera manual, un 18% de manera totalmente automática, un 18% de manera semiautomática, donde se combinan procesos de manuales y automáticos y el restante 9%, una lectura y clasificación similar a una semiautomática.

108. El que se cuente con mecanismos que permitan automatizar, parcial o totalmente la lectura y clasificación de ROS, siendo esta una actividad crítica de una UIF, es un aspecto favorable para apoyar los procesos de continuidad de operaciones de la entidad

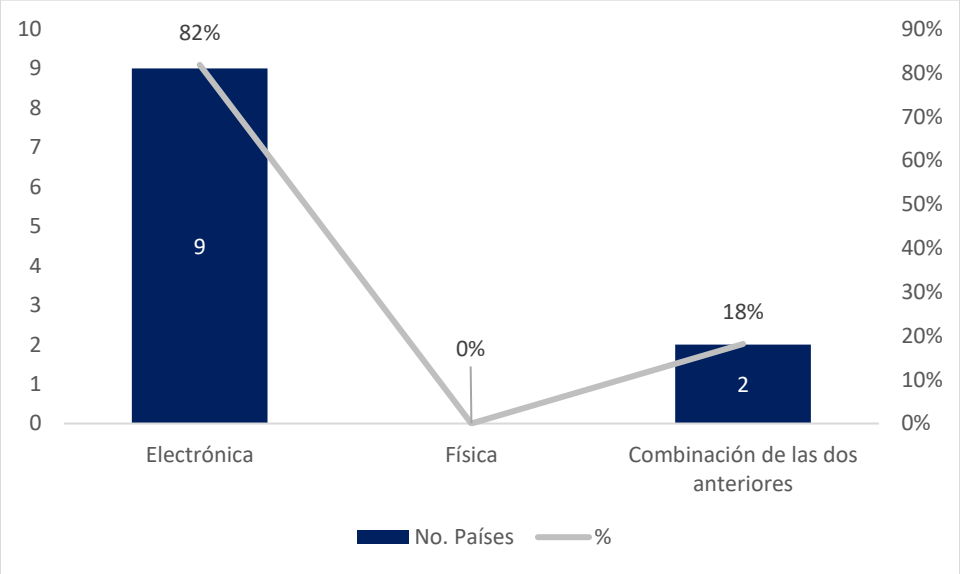
Figura 15 – Proceso de lectura y clasificación de ROS



109. La recepción de ROS se realiza por diversos mecanismos. El 82% de los encuestados realizan una recepción totalmente electrónica, mientras que el 18% restante

tienen una combinación de recepción electrónica y en medio físico. Ningún encuestado manifestó que la recepción de ROS se realizaba exclusivamente de manera física. Esta capacidad de **permitir la recepción electrónica de ROS facilita el proceso de notificación de información y hace que esta labor no se vea impactada de forma crítica ante eventos como los sucedidos bajo COVID-19**.

Figura 16 – Mecanismo de recepción de ROS



110. Para la recepción de información, el 64% de las UIF participantes manifestaron contar con mecanismos de autenticación fuertes (p.ej. dos factores) por parte de los SO para acceder a las plataformas de reporte de información, mientras que el 36% no cuenta con dichas medidas de seguridad.

111. Otro proceso fundamental es la comunicación de información a destinatarios naturales, como puede ser la Fiscalía o Procuraduría. En este sentido, el 36% de los entrevistados realizan la difusión de manera electrónica, el 9% por medio físico, el 45% en

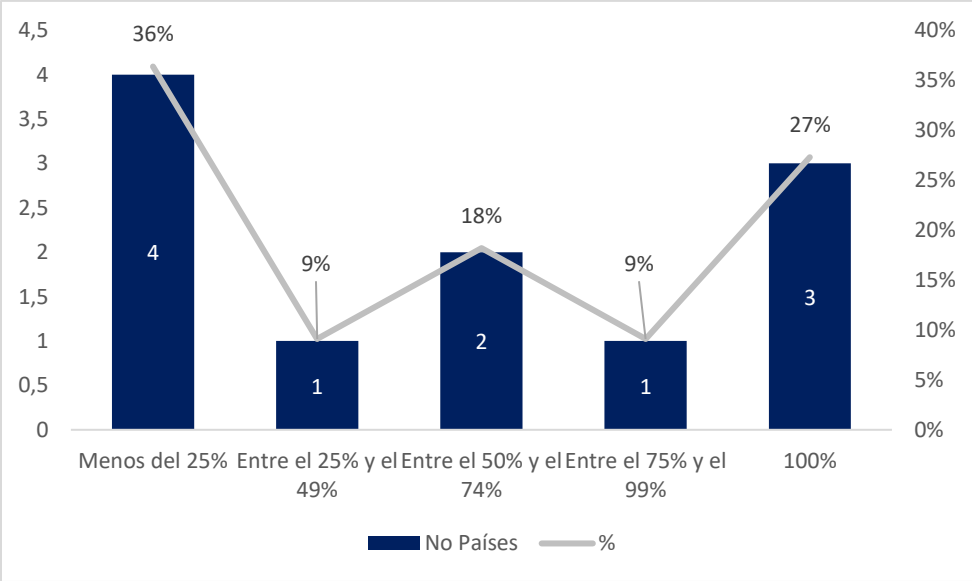
una combinación de medio físico y electrónico y el 9% restante a través de otro mecanismo (CD encriptado).

112. Para la remisión electrónica de información, se dividió en partes iguales entre aquellos que cuentan y los que no cuentan con mecanismos de validación de los receptores para asegurar el acceso sólo a personal autorizado.

113. **El que la comunicación de información se haga por medios electrónicos y con mecanismos de autenticación, provee otro factor que fortalece las capacidades de las UIF a soportar eventos inesperados**.

114. Solo el 27% de los encuestados manifestaron que el 100% de los funcionarios cuentan con accesos remotos a la red corporativa, en un caso se indica que el 75% al 99% de sus funcionarios tienen este acceso. El 18% de los encuestados respondieron que entre el 50% y el 74% de sus funcionarios tienen acceso remoto, mientras que el 9% le otorga dicho acceso a entre el 25% y el 49% de sus funcionarios. Finalmente, la mayor proporción de UIF, manifestaron que menos del 25% de sus funcionarios tienen acceso a su red corporativa.

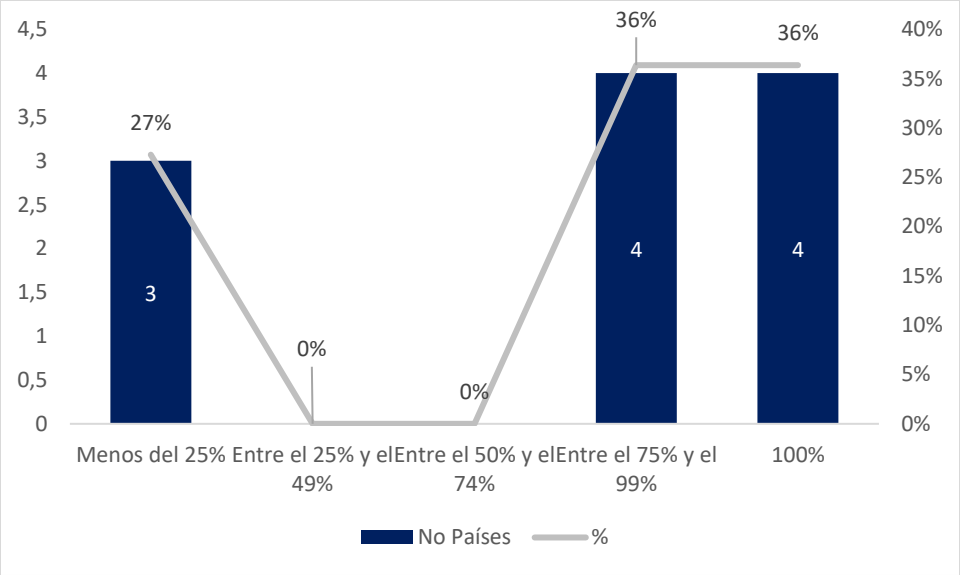
Figura 17 – Porcentaje del personal que tiene acceso remoto a la red corporativa



3.3. Impacto COVID-19 en las operaciones de la UIF

115. El 72% de los encuestados manifestaron que al menos el 75% de los funcionarios de análisis operativo tiene acceso remoto a la red corporativa. Es más, el 36% de los encuestados expusieron que la totalidad de los funcionarios de análisis operativo cuentan con la capacidad de trabajar de forma remota. Solo el 27% de los encuestados tienen capacidades de conexión remota a la red por parte de los funcionarios de análisis operativo, menores al 25% de los mismos.

Figura 18 – ¿Qué porcentaje del personal de Análisis Operativo tiene acceso remoto a la red corporativa?



116. El 91% de los encuestados estipularon que el personal de análisis operativo cuenta con mecanismos para acceder de forma remota a la plataforma de lectura y clasificación de ROS. Sin embargo, el porcentaje de países que manifestaron que los analistas de Análisis de Operaciones tienen acceso remoto a las bases de datos y aplicativos para poder desarrollar casos se redujo al 73%.

117. El 82% de las UIF proveen de acceso remoto a los responsables de dar respuesta a requerimientos de información de parte de autoridades nacionales competentes, mientras que el 73% de las UIF encuestadas conceden este acceso a los responsables de dar respuesta a requerimientos de información de parte de otras Unidades de Inteligencia Financiera (p.ej. a través de Egmont).

118. El 73% de los encuestados disponen de mecanismos de acceso remoto para el personal de análisis estratégico, en particular, a las bases de datos requeridas para desarrollar sus objetivos misionales.

119. El impacto operacional del brote de COVID-19 en las UIF participantes, obedeció a diversos factores, dentro de los que se encuentran, la intensidad y extensión de los confinamientos, p.ej., uno de los países participantes no presentó confinamiento; la activación de actividades económicas a partir de los primeros confinamientos y; las capacidades de respuesta de cada UIF.

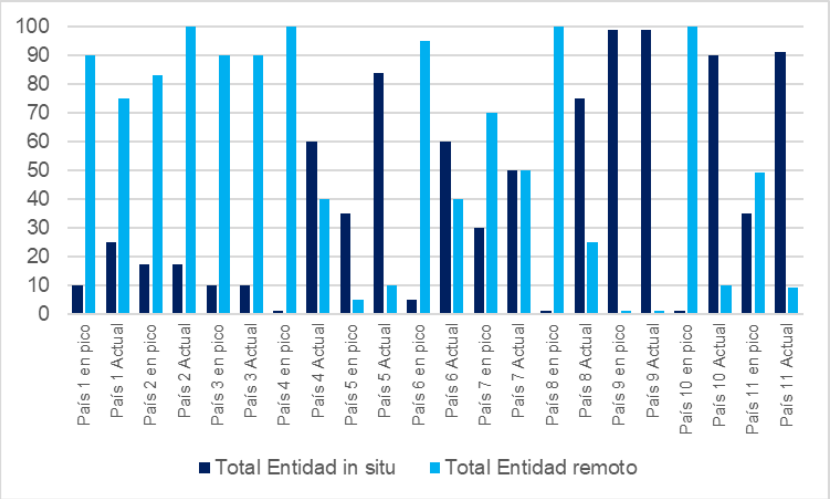
120. Sin embargo, se observa que todas las UIF entrevistadas, en mayor o menor medida, **implementaron estrategias de adaptación en los procesos de recepción, análisis y difusión de información**, ya fuese a través de medidas de trabajo remoto (incluyendo políticas de ciberseguridad) y/o la implementación de protocolos de bioseguridad y modificaciones de horarios laborales o turnos, para el desempeño de sus labores desde las instalaciones de la institución. Se requirieron, en muchos casos, **ajustes en los procesos de negocio**, con el fin de adaptarlos a las nuevas condiciones.

121. Diversos participantes expusieron el enfoque en una **mayor articulación con los SO**, a través del uso de canales digitales, brindando información de diversa índole, incluyendo señales de alerta y otra información de interés para los SO. De igual forma, en algunos casos, **se tomaron medidas administrativas**, tales como la extensión de plazos de reporte, régimen sancionatorio especial, para SO, implementación de supervisión extra-situ en aquellas que cumplen labores de supervisión, entre otras.

122. En un 9% de los países se informó el despliegue de actividades de inteligencia financiera ante casos de corrupción, en particular de compra de insumos y medicamentos contra el COVID-19.

123. Uno de los aspectos donde se observa el impacto de las medidas de confinamiento es en la proporción de funcionarios realizando tareas de forma remota o in situ. Se observa que, en la mayoría de UIF, se llegó a proporciones bastante altas, incluso, cercanas al 100%.

Figura 19 – Porcentaje de personal insitu vs remoto. Comparación entre pico de pandemia y situación actual



124. La proporción de funcionarios de análisis estratégico que se encontraban in situ, en la mayoría de UIF encuestadas, aumentó una vez se relajaron las medidas de confinamiento producto de la pandemia, en algunas UIF esta situación se dio en sentido contrario. Durante el pico de la pandemia, en el 9% de las instituciones se presentó una proporción de funcionarios de análisis estratégico bajo modalidad remota, igual a la proporción de personal total de la UIF en modalidad remota. En el 36% de los encuestados, esta proporción es menor y en el 55% mayor.

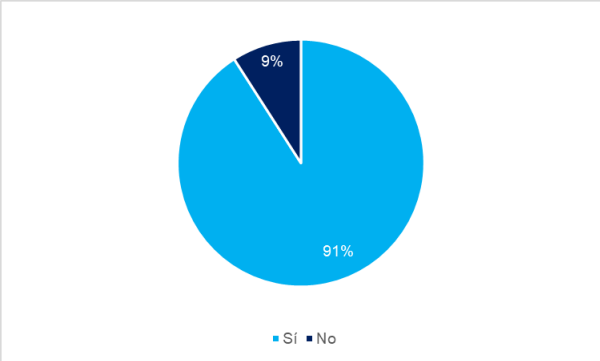
125. En la actualidad, el 27% de las UIF reportaron que la proporción de personal de análisis estratégico en modalidad remota es igual a la proporción de la totalidad de funcionarios en modalidad remota, en el 36% restante la de UIF, esta proporción es mayor. Se puede observar una tendencia asociada a que **la proporción de funcionarios de análisis operativo es mayor o igual a la proporción de funcionarios de análisis estratégico bajo conexión remota,** en tres países reportó una tendencia inversa.

126. Las proporciones de personal de tecnología in situ y remoto en el pico de la pandemia actualmente presentan comportamientos similares a los del personal de análisis operativo y estratégico en el sentido que, en la mayoría de los casos, se observa un aumento de la proporción de empleados in situ, una vez han bajado los niveles de contagio y medidas de confinamiento.

127. De esta forma, el 91% de las UIF entrevistadas y el 100% de las UIF con las cuales se sostuvieron entrevistas mas no diligenciaron el instrumento de recolección,

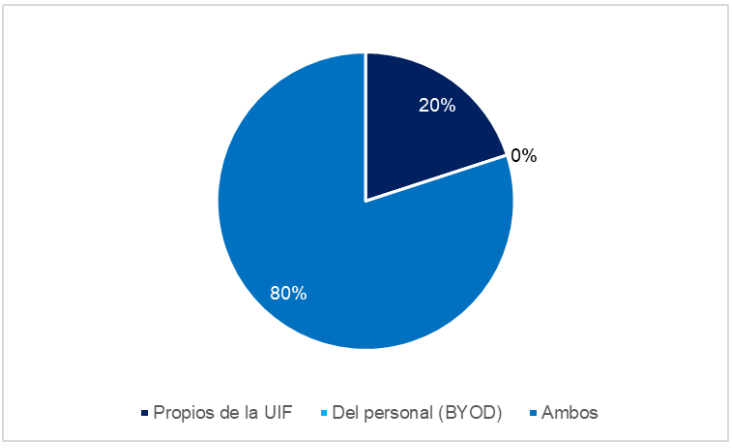
manifestaron el haber implementado medidas de trabajo remoto como respuesta a la coyuntura generada por la pandemia del COVID-19. De igual forma, el 64% de los encuestados realizaron confirmaciones o pruebas de capacidad de red para que todo el personal trabaje de forma remota.

Figura 20 – Adopción de medidas de trabajo remoto en la UIF



128. En relación con la disponibilidad de equipos para la conexión remota, el 20% de los encuestados manifestaron que la conexión a los sistemas de la UIF se realiza a través de equipos propios de la UIF, el 80% en una combinación de equipos de la UIF y propios del personal, mientras que en ninguna UIF entrevistadas la conexión se realiza exclusivamente con equipos personales de los funcionarios de la entidad.

Figura 21 – Proporción fuente de equipos utilizados en conexiones remotas en UIF



129. El 91% de las UIF que diligenciaron el instrumento y el 100% de las UIF con las que se sostuvieron entrevistas abiertas indicaron que cuentan con mecanismos de conexión remota segura tales como VPN y RDP.

130. Cerca del 50% de los encuestados diligenciaron el instrumento con información relativa a que las políticas de copias de seguridad no sufrieron modificaciones como producto de la contingencia.

131. La implementación de estrategias de capacitación a funcionarios de la UIF en relación con riesgos de ciberseguridad que puedan generarse en el contexto del COVID-19, fue llevada a cabo por el 91% de las UIF que diligenciaron el instrumento. En las entrevistas abiertas realizadas, tanto a una muestra de países que diligenciaron el instrumento como a un grupo de países que no lo diligenciaron, la concientización del personal y la capacitación en medidas de protección y resguardo de información, incluyendo temáticas de ciberseguridad, fue un aspecto de particular importancia que fue expresado regularmente.

132. Sin embargo, el 82% de quienes diligenciaron el instrumento implementaron entrenamientos o capacitaciones adicionales para funcionarios, relacionados con la nueva situación de trabajo remoto y del COVID-19.

3.4. PCN

133. Más que establecer si se cuenta con un PCN como tal, se busca identificar las medidas de continuidad de operaciones que han sido implementadas.

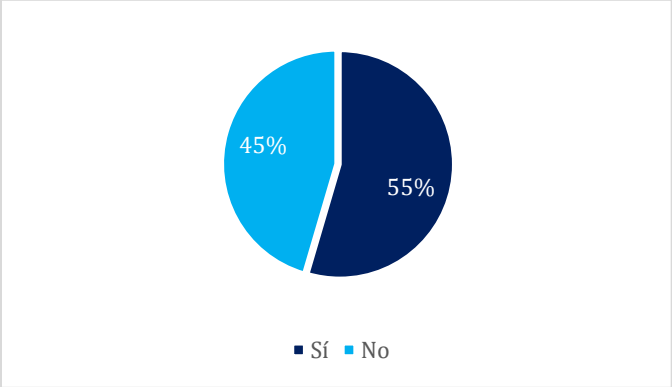
134. Uno de los elementos primordiales de un PCN es el desarrollo de un BIA. Este elemento se utiliza como herramienta complementaria en el proceso de estimación de la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.

135. A diferencia de una evaluación de riesgos, que se enfoca en cómo podría verse afectada una organización a través de la identificación, análisis y valoración de amenazas en términos de continuidad de operaciones, con base en su impacto y su probabilidad de ocurrencia, el BIA es un proceso más especializado en la identificación de los tipos de impacto, orientado en conocer qué podría verse afectado y las consecuencias sobre los procesos de negocio. De esta forma, el BIA se convierte en una fase importante en el desarrollo del Plan de Recuperación de Desastres (DRP), y por lo tanto, del PCN, debido a que permite a las organizaciones estimar la magnitud del impacto operacional y financiero asociado a una interrupción.

136. De las UIF entrevistadas, el 55% han realizado un BIA, mientras que el 45% aún no han realizado esta acción. Esto es relevante, puesto que **para dar mayor fortaleza al**

PCN, es fundamental contar con un BIA. La totalidad de UIF que han realizado un BIA lo actualizaron en el último año y han diseñado a su vez, indicadores relativos al BIA, incluso un país ha desarrollado indicadores a partir del BIA a pesar de no tener completamente implementado su BIA.

Figura 22 – ¿Ha realizado un análisis de impacto de negocio (Business Impact Analysis "BIA")?



137. Durante el proceso de fortalecimiento de las capacidades de respuesta ante incidentes, el 73% de las UIF que diligenciaron el instrumento han identificado los procesos críticos de negocio, mientras que el 27% aún no han realizado esta tarea.

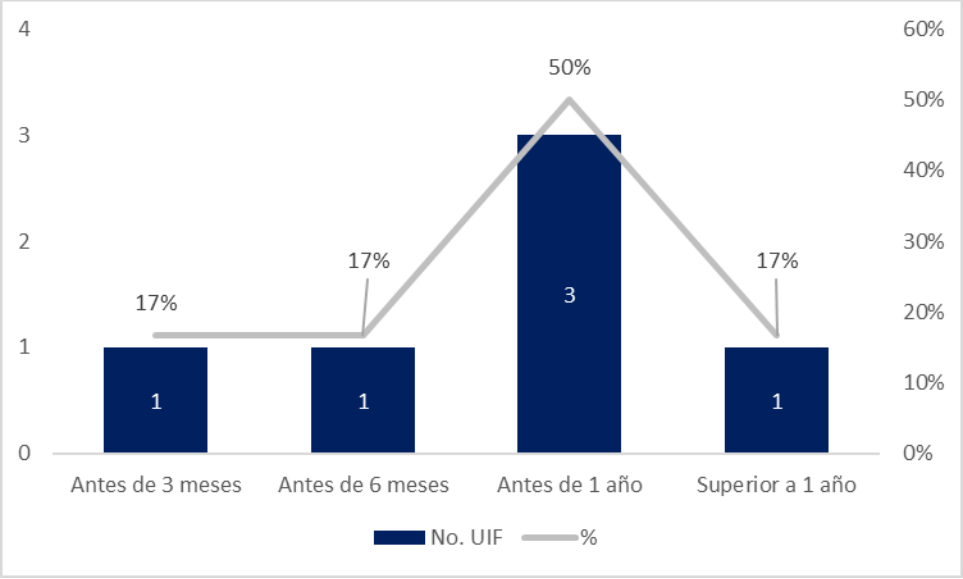
138. De igual forma, dentro de las UIF consultadas, el 64% manifestaron haber considerado los impactos de los riesgos directos en la operación, como pueden ser fallas de tecnología, fallas de equipos, pérdida de energía, incendio, ausencia de personal crítico, entre otras.

139. Ante la pregunta de si cuenta con un PCN oficial, el 64% de las UIF que respondieron el instrumento no cuentan con este tipo de plan, mientras que el 34% si cuentan con un PCN. Sin embargo, **a pesar que no todas las UIF de la región cuentan con un PCN explícito, durante la pandemia implementaron en su gran mayoría, en función de la intensidad de las cuarentenas decretadas, medidas rápidas y efectivas**

que permitieran una operación continua de las actividades de inteligencia financiera y de supervisión en donde fuera aplicable, de tal forma que el impacto en las operaciones fuera mínimo. Dentro de las UIF que cuentan con un PCN, este se encuentra contemplado ya sea dentro de los planes de acción de la ENR, en un plan estratégico de la organización y contempla en términos generales los aspectos contenidos en la norma ISO 22301.

140. En relación con el plazo que las UIF que en la actualidad no cuentan con un PCN per se, el 50% contempla tener diseñado el PCN en menos de un año, el 17% antes de 6 meses y el 17% antes de 3 meses. De esta forma, **una proporción importante de las UIF (83%) que en la actualidad no cuentan con un PCN, tienen programado su diseño en un plazo de máximo un año.** De esta forma, se potenciarán y fortalecerán las estrategias de continuidad de operaciones que a la fecha ya han sido implementadas.

Figura 23 – En caso de no contar con un plan de continuidad de negocio, ¿se ha contemplado implementar uno en los siguientes periodos de tiempo?



141. En cuanto a la participación de la alta dirección de la entidad en aspectos relevantes y críticos del diseño y actualización del PCN, puntualmente, en la revisión y aprobación de elementos tales como su alcance y frecuencia, el 50% de quienes respondieron esta pregunta manifestaron que la dirección realiza estas acciones. **En este sentido, se crea una importante oportunidad el que los JdUIF participen activamente en la aprobación y revisión de los PCN.**

142. Aunque se puede afirmar que todas las UIF que diligenciaron el instrumento de recolección y las que sostuvieron entrevistas no estructuradas, aún sin diligenciar el formulario, implementaron medidas diversas de continuidad de operaciones, que permitieron que las labores de las UIF se vieran impactadas lo menos posible, tan solo el 13% de quienes diligenciaron la encuesta actualizaron sus PCN como consecuencia de la coyuntura provocada por el COVID-19.

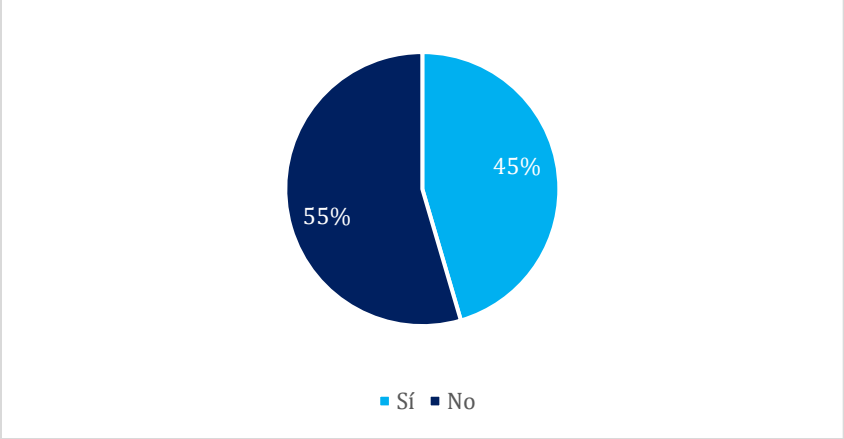
143. Entre las UIF que diligenciaron el instrumento de recolección de información, la mitad que aquellas que han implementado o están en proceso de implementar un PCN, han designado un responsable o coordinador del mismo. De esta forma, **una estrategia para fortalecer las iniciativas de continuidad de operaciones en las UIF es que se cuente con un equipo con claras responsabilidades en términos del diseño e implementación del PCN.**

144. Un elemento que puede afectar la rapidez con la que se puede desplegar un PCN es el que en el 63% de quienes respondieron esta pregunta, el coordinador del plan no cuenta con poder de decisión respecto al PCN ni recursos para su desarrollo.

145. Entre los encuestados, el 45% no cuenta con copias offsite del PCN, el 18% sí cuenta estas copias del plan y el 36% no respondió la pregunta. En este sentido, es **recomendable contar con copias offsite del PCN con el objetivo que, ante un evento de interrupción abrupta se cuente con acceso a los mecanismos de recuperación debidamente documentados.**

146. Una estrategia de particular importancia para ampliar las capacidades de recuperación ante un evento externo que afecte la continuidad de operaciones, en particular, aquellas que impactan los sistemas físicos y de almacenamiento de datos, es el contar con un centro alterno de datos. El 45% de las UIF encuestadas cuentan con centros alternos de datos, mientras que el 55% no cuentan con esta capacidad. **Dentro de las medidas de fortalecimiento del PCN, contar con un centro alterno de datos potencia las capacidades de respuesta de la UIF ante situaciones adversas.**

Figura 24 – ¿Cuenta con un centro alterno de datos?



147. Aunque, como se expuso previamente, el 64% de las UIF participantes del instrumento no cuentan con un PCN, el porcentaje de UIF que **cuentan con un DRP** aumenta al 55%, lo cual **sienta una base importante para el PCN.** La importancia del DPR radica, como lo expresó una UIF, en que pueda "servir de guía y referencia para recuperar y mantener las aplicaciones y servicios de TI requeridos por los procesos críticos de la [UIF], en el caso de una interrupción de fuerza mayor que afecte la continuidad de dichos recursos".

148. Dentro de los componentes que hacen parte del DRP de las UIF, se encuentran:

a. Contar con políticas de Respaldo de la información para mitigar los posibles riesgos por desastre.
b. Contar con políticas y procesos de Recuperación de la información en caso de desastre.
c. Replicación on line de los principales sistemas y su posterior recuperación en el sitio remoto.
d. Procedimientos de copias diarias de seguridad de los datos críticos offsite.
e. Plan de manejo de la crisis en una forma organizada y efectiva
f. Entrenamiento al personal con los procedimientos de emergencia.

149. A pesar de los importantes esfuerzos que han realizado las UIF de la región en estrategias para responder a los retos planteados por la pandemia, el 73% de las UIF que diligenciaron el instrumento no han cuantificado los recursos mínimos necesarios para la recuperación de desastres.

150. En concordancia con lo expuesto previamente, relativo a que el 64% de las UIF no cuentan con un PCN, la misma proporción de entidades no han designado personal de la institución con roles específicos dentro del plan de recuperación. Por lo tanto, **una vez**

se diseñen los PNC se debe designar personal con roles y responsabilidades claramente definidas dentro de los mismos.

151. A pesar que el PCN cubre diversos escenarios adversos, que afectan la continuidad de operaciones, ante una situación para la cual la entidad no se encuentra preparada, que afecta directamente a contrapartes interesadas (p.e. órganos judiciales, SO, etc.), y que la obliga a establecer acciones estratégicas rápidas para resolverla, se configura una situación de crisis.

152. En este sentido, y dada la importancia de las UIF en los sistemas ALA/CFT, contar con un **Plan de Manejo de Crisis**, en el cual se implementen tácticas de comunicación específicas ante las partes con las que interactúa y que durante el transcurso de la crisis se tomen decisiones estratégicas para reducir su impacto, configura un elemento complementario valioso al PCN.

153. Asimismo, **en las entrevistas llevadas a cabo con diversas UIF de la región, se encontró que todas desplegaron estrategias de comunicación con sus partes de interés**, con el objetivo de informar diversos aspectos asociados a las medidas que se iban implementando a raíz de la crisis provocada por el COVID-19. De esta forma, es importante formalizar este tipo de respuestas, dado que, de las encuestas recolectadas, el 82% de las UIF no cuentan con un PMC. Dentro de las UIF que tienen implementado un PMC, Dentro de quienes respondieron la encuesta, un elemento a resaltar del PMC, es que busca "Promover la credibilidad e imagen positiva de la organización".

154. Independientemente de los planes que se tengan diseñados, su actualización y revisión periódica asegura su vigencia ante situaciones externas. El 45% de quienes diligenciaron el instrumento indicaron que los planes diseñados (PCN, PMC, DRP, etc.) se revisan de manera anual, mientras que el restante 55% no han realizado acciones de actualización.

155. Una menor proporción de UIF, correspondiente al 36% de los encuestados, han realizado simulacros o test al PRN.

156. En relación con las responsabilidades asignadas a la ejecución y supervisión de los planes relacionados con continuidad de operaciones, tales como el PCN, DRP, entre otros, esta recae principalmente, en el área de tecnología (50%). Seguida de Ptro (30%) y el equipo de recuperación de desastres (20%).

157. De forma complementaria, el 64% de los encuestados cuenta con personal responsable para realizar una evaluación de daños ante un evento inesperado que afecte el PCN.

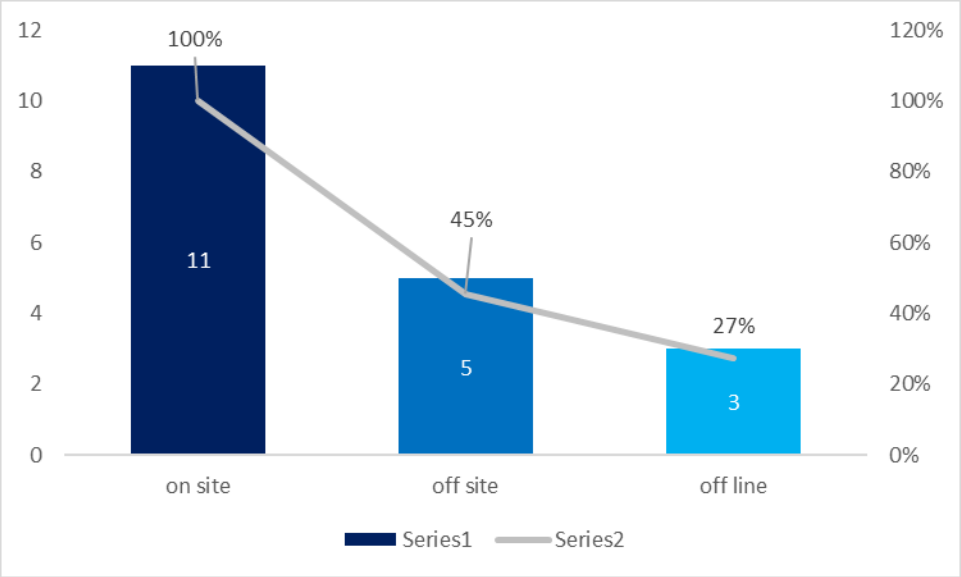
158. Un pilar fundamental en el aseguramiento del correcto funcionamiento, en este caso, de los PCN, es que éstos sean sometidos a procesos de auditoría. De entre quienes diligenciaron el instrumento de recolección de información, el 36% somete sus sistemas tecnológicos a auditorías trimestrales, en el 27% de los casos dicha auditoría se realiza a nivel anual y el 9% de manera semestral. Solo en el 27% de las UIF encuestadas, los sistemas tecnológicos no se han sometido a procesos de auditoría.

159. Aunado a lo anterior, la evaluación de vulnerabilidades de los sistemas de la UIF proporciona fortalezas a los PCN y pueden servir como elementos que apoyen los procesos de priorización de estrategias. **Los análisis de vulnerabilidades externas de los sistemas de las UIF es uno de los aspectos que muestra fortaleza entre las UIF que diligenciaron el instrumento.** En su mayoría, éstos han sido realizados en el último trimestre (50%), seguidos por el último año (38%). Solo el 13% de los encuestados no han realizado análisis de vulnerabilidades externas.

160. Otro aspecto que presenta importantes fortalezas en relación con el PCN está asociado a las políticas de respaldo de información. El 100% de los entrevistados realizan **copias de seguridad de los sistemas críticos, como lo es la base de datos de ROS, adicionalmente, estos procesos son totalmente automáticos**, lo que reduce la posibilidad que se presenten eventos de riesgo operativo en su desarrollo. De igual forma, las UIF **toman variadas acciones para preservar la información, tales como backups incrementales, respaldo externo e incluso, respaldo externo en bóveda bancaria. Así mismo, los backups tienen periodicidades disimiles, desde diarios hasta anuales, con políticas de respaldo tales como cintas en backups semanales**.

161. En ese sentido, **el 100% de las UIF que diligenciaron el instrumento, poseen sistemas de backup onsite. Sin embargo, el 55% de las estas cuentan con mecanismos alternos de backup**. En este sentido, el 45% cuenta con backup offsite y el 27% cuenta con backup offline. También es importante resaltar que el 18% cuenta con más de dos mecanismos de backup. Todos estos aspectos relativos a los backups de información **proveen importantes capacidades a las UIF para reaccionar de forma rápida y eficiente ante eventos adversos**.

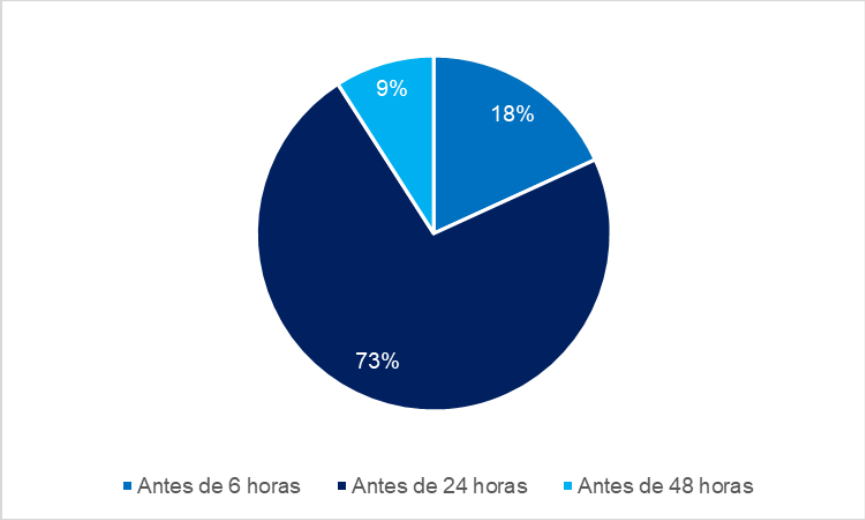
Figura 25 – Almacenamiento de copias de seguridad



162. El 73% de las UIF que diligenciaron el instrumento han estimado su RPO, mientras que solo el 23% no han realizado esta labor. El 82% de los encuestados consideran que son capaces de restaurar copias de seguridad de datos lo más rápidamente posible y con el menor impacto.

163. Se encontró que los RPO de los encuestados son relativamente bajos. En el 18% de los casos, se tienen periodos entre dos copias de seguridad de menos de 6 horas, el 73% menos de 24 horas en el 9% menos de 48 horas.

Figura 26 – ¿Cuánto tiempo estima usted para su RPO, el periodo entre dos copias de seguridad con una pérdida aceptada /aceptable de datos?



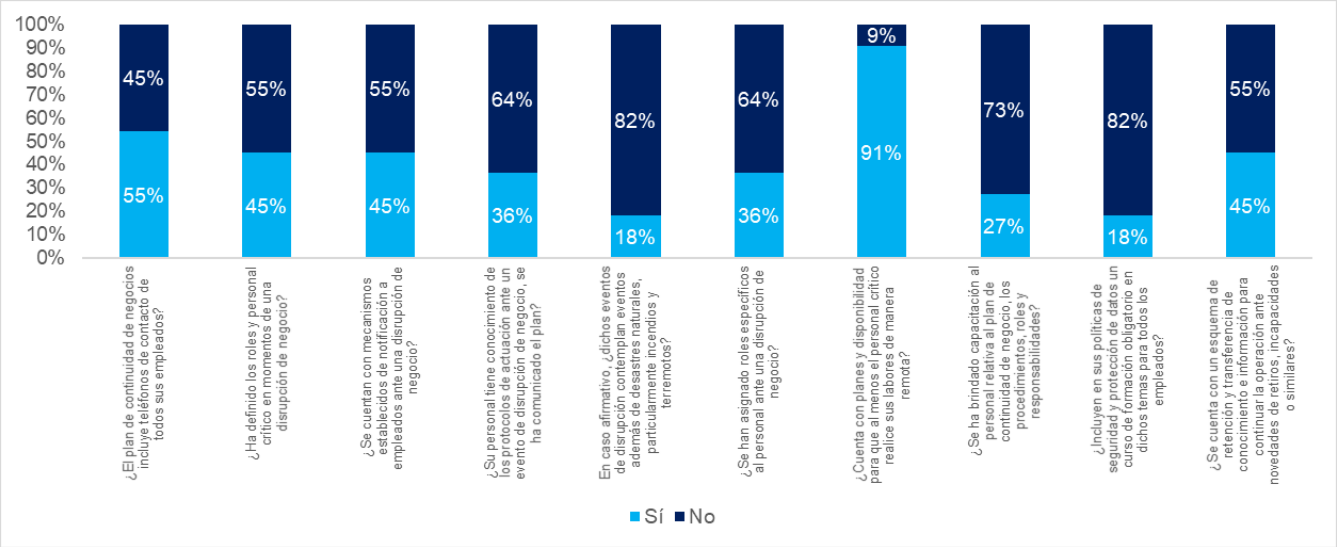
164. Finalmente, en relación con la redundancia de los sistemas de comunicación, el 55% de los encuestados manifestaron contar con enlaces telefónicos alternos, mientras que el 82% cuenta con enlace de comunicación de internet alterno o redundante. **Este elemento provee una fortaleza a las UIF en términos de capacidad de recuperación y de mantener sus funciones primordiales de recolección, análisis y difusión de información.**

3.5. Personal y PCN

165. En primera medida, de los encuestados, en el 55% de las UIF el PCN cuenta con información de contacto de todos los empleados. De esta forma, solo el 45% de las UIF cuentan con mecanismos de notificación de los empleados ante eventos de disrupción y en el 36%, el personal tiene conocimiento de los protocolos de actuación ante un evento de disrupción. En el 45% de las UIF se han definido los roles y el personal crítico responsable en un caso de interrupción de operaciones, pero solo el 36% de las UIF han asignado roles específicos al personal ante un evento de interrupción de operaciones. Una fortaleza de las estratégicas de continuidad de operaciones en las UIF radica en el hecho que **el 91% de quienes diligenciaron el instrumento cuenta con planes y disponibilidad para que al menos el personal crítico realice sus labores de manera remota**.

166. Tan solo el 27% de las UIF ha brindado capacitación al personal relativa al PCN, los procedimientos, roles y responsabilidades, aunque **en las entrevistas no estructuradas, diversas UIF desplegaron mecanismos de entrenamiento de personal, en temas misionales, pero también en temáticas relacionadas con medidas de ciberseguridad**. Sin embargo, solo en el 18% de las UIF incluyen en sus políticas de seguridad y protección de datos un curso de formación obligatorio en dichos temas para todos los empleados, aunque una UIF, a raíz de la pandemia, implementó un plan de capacitación de nuevos funcionarios totalmente virtual.

Figura 27 – PCN y personal de la UIF



167. En este sentido, una **acción de mejora de los PCN de las UIF es el contar con procedimientos de información a funcionarios de las UIF ante eventos de disrupción de operaciones de negocio y el establecimiento de roles y responsables, así como de planes de capacitación al respecto. Otro aspecto relevante es que la mayoría (82%) de los encuestados incluyen en su PCN exclusivamente eventos relativos a desastres naturales.** En este sentido, escenarios como el presentado como consecuencia de la pandemia, aunque se tuvo una respuesta eficiente por parte de las UIF de la región, no se encuentran planificados dentro de los PCN, lo cual genera un riesgo potencial.

168. Un aspecto relevante, dada la complejidad, tiempo y esfuerzo que implica el entrenamiento de personal en una UIF, es el hecho que en el 45% de los encuestados, se cuenta con un esquema de retención y transferencia de conocimiento e información para continuar la operación ante novedades de retiros, incapacidades o similares. El **implementar estratégicas de retención y transferencia de conocimiento puede llegar a ser de una importancia crítica en una UIF debido a que una proporción importante del conocimiento necesario para el desarrollo de las labores, en particular en análisis operativo y estratégico, es adquirido por el personal a través de la experiencia en la propia UIF.**

169. Por lo tanto, ante retiros masivos de personal por circunstancias de diversa índole, las capacidades de reacción y mantenimiento de niveles de producción pueden verse impactadas. Aunque algunas UIF cuentan con mecanismos de documentación de información y la persistencia de la misma en las bases de datos institucionales permite el

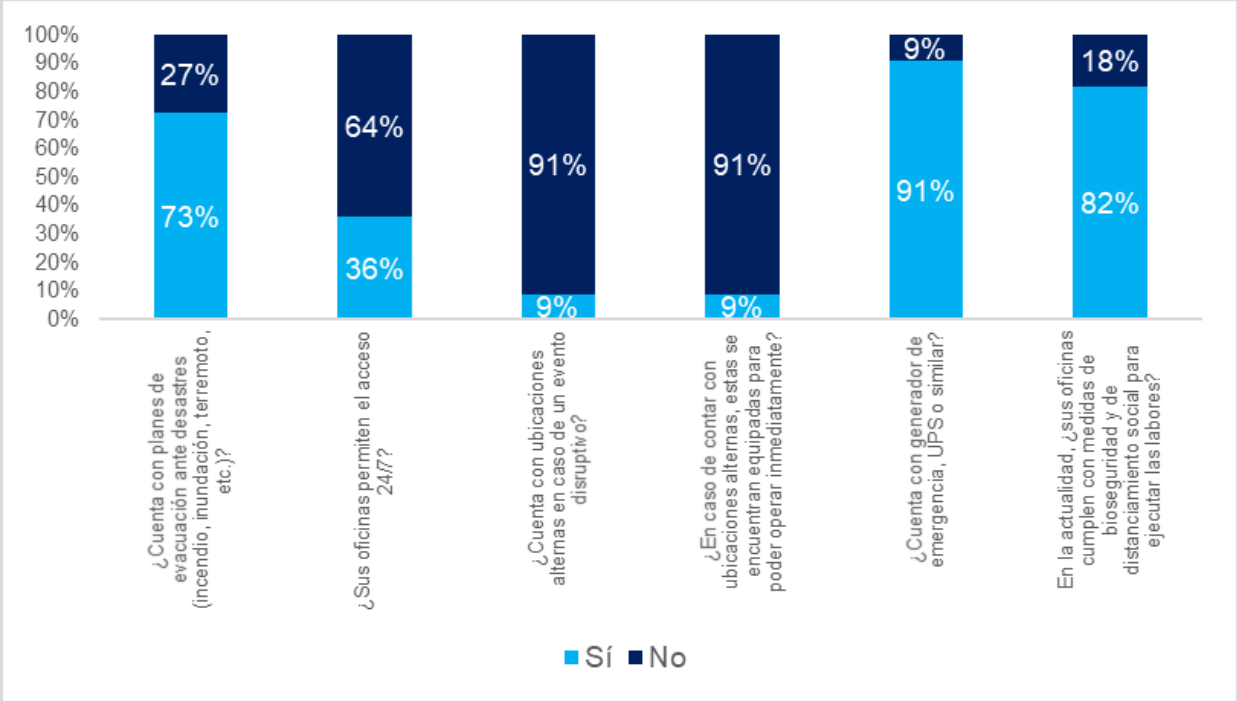
registro de las labores realizadas en la unidad, estas acciones son una parte de un plan de transferencia y retención de conocimiento.

3.6. Oficinas, PCN y ambiente físico

170. El 73% de las UIF que diligenciaron el instrumento cuentan con planes de evacuación ante desastres (incendio, inundación, terremoto, etc.). Debido a la criticidad de información que se almacena y maneja en la UIF, solo el 36% permite acceso 7x24 a las instalaciones. **Solo el 9% cuenta con ubicaciones alternas para operar, en casos de disrupción de operaciones; sin embargo, en situaciones extremas como las que se presentaron bajo pandemia, el uso de instalaciones alternas, aunque es una medida recomendada en los PCN, cuando se impone por parte del gobierno medidas de confinamiento estricto, no resultan efectivas dado que ninguna ubicación, principal o alterna puede ser utilizada**.

171. Sin embargo, el contar con instalaciones alternas facilita la implementación de medidas de distanciamiento social al habilitar las dos instalaciones simultáneamente. En la actualidad, el 82% de las UIF cumplen con las medidas de bioseguridad y distanciamiento requeridas. Finalmente, la gran mayoría de entidades encuestadas (91%), cuenta con generador de emergencia o UPS, lo cual, fortalece la capacidad de la UIF a responder a eventos adversos externos, en particular, fallos en el fluido eléctrico.

Figura 28 – PCN e instalaciones físicas

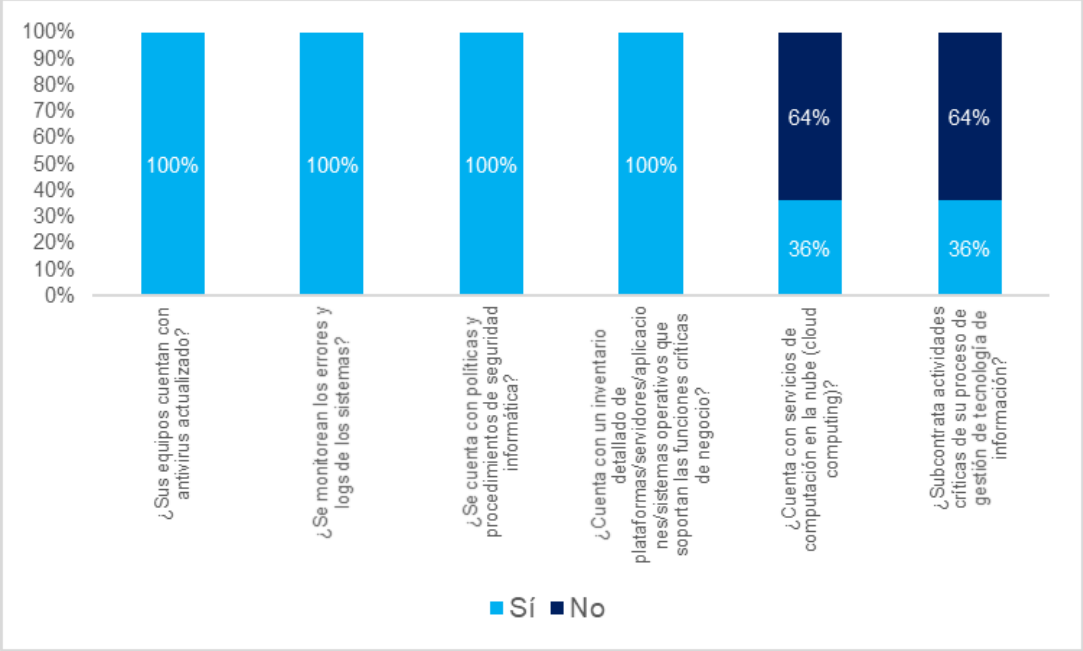


3.7. Tecnología de información de apoyo al PCN

172. La totalidad de quienes diligenciaron el instrumento de recolección de información estipularon que cuentan con antivirus actualizado, realizan monitoreo de logs de errores, cuentan con políticas y procedimientos de seguridad de la información, así como contar con un inventario detallado de la infraestructura de tecnología de información que soporta los procesos críticos de negocio. Estos elementos **muestran importantes fortalezas en los sistemas de tecnologías de información asociados a los PCN.**

173. Existen a su vez, aspectos en los cuales no todas las UIF que participaron en la encuesta, tienen posiciones homogéneas. Se observa que el **36% de las UIF cuentan con servicios de computación en la nube y la misma proporción subcontrata actividades críticas de tecnologías de información.**

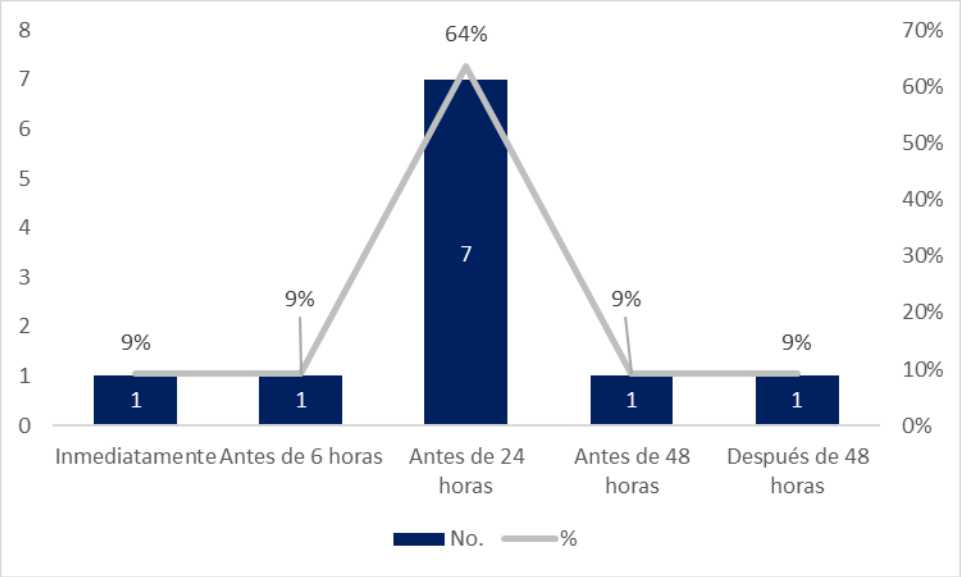
Figura 29 – PCN y tecnologías de información



174. Entre quienes subcontratan actividades críticas de tecnologías de información, estos elementos incluyen aspectos como el servicio de alojamiento de servidores en centros alternos de datos, actividades de desarrollo y mesa de ayuda, así como soporte técnico para redes, seguridad y sistemas operativos.

175. En lo que respecta a tiempos sin acceso a la red o plataforma tecnológica por parte de sus empleados que ocasionaría un impacto significativo, para el 9% de quienes diligenciaron el instrumento, dicho tiempo es inmediato, para otro 9%, el tiempo es menor a 6 horas, para el 64%, dicho impacto se manifiesta con una interrupción de hasta 24 horas. En resumen, **para el 82% de las UIF, una interrupción de hasta 24 horas en el acceso a sistemas tiene impactos significativos en la continuidad de operaciones.**

Figura 30 – ¿Después de cuánto tiempo sin acceso a su Red o Plataforma Tecnológica por parte de sus empleados se ocasionaría un impacto significativo en su negocio?

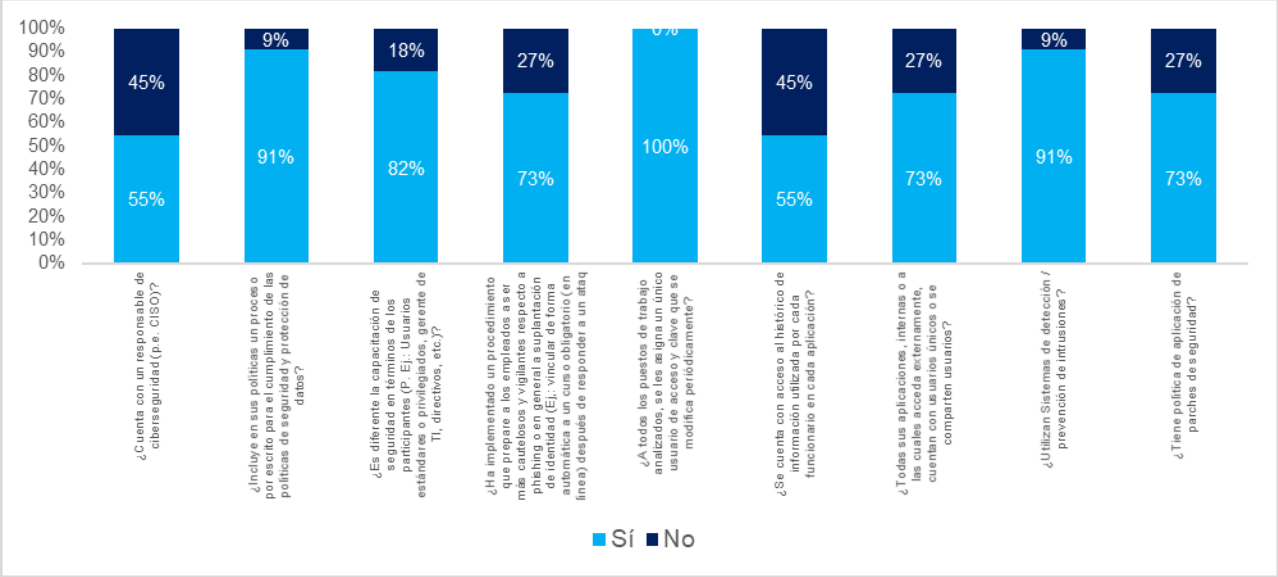


3.8. Seguridad de la red

176. El primer aspecto evaluado corresponde a la responsabilidad en términos de ciberseguridad¸ **tan solo el 55% de las UIF han designado un responsable para temas de ciberseguridad con un rol específico, como puede ser un CISO (Chief Information Security Officer).** Sin embargo, las UIF que diligenciaron la encuesta, han implementado **diversas estrategias de seguridad de red**. **Estas corresponden a la implementación de políticas, uso de herramientas especializadas de software de seguridad de red, diseño de planes de respuesta, capacitación de personal, entre otras.**

177. Dentro de etas acciones se encuentran, contar con políticas de seguridad de información y protección de datos que consten por escrito (91%), capacitaciones en seguridad de la información diferenciadas en función del público objetivo (82%), procedimientos de concientización a empleados en seguridad de información (73%), **almacenamiento del histórico de información accesada por los usuarios en cada aplicación (55%), otorgamiento de usuarios únicos a las aplicaciones que se acceden (73%)**, utilización de sistemas de detección e identificación de intrusiones (91%), políticas de aplicación de parches de seguridad.

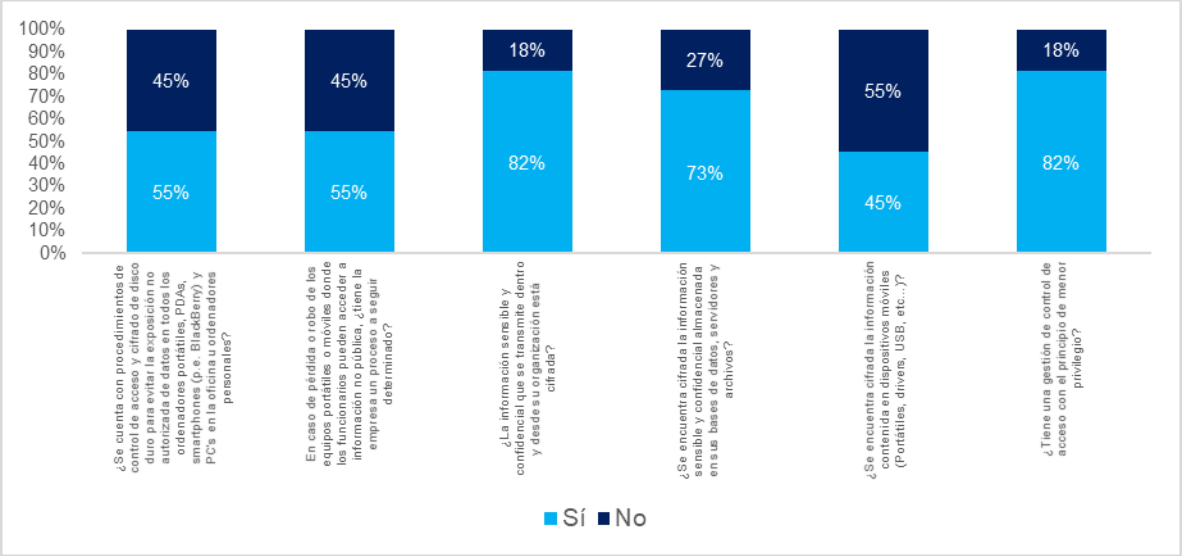
Figura 31 – Aspectos generales seguridad de la red



178. Otro grupo de acciones implementadas hacen referencia al **cifrado de información.** Dentro de estas acciones se encuentra el poseer procedimientos de control de acceso y cifrado de disco duro para evitar la exposición no autorizada de datos en todos los ordenadores portátiles, PDAs, smartphones (p.e. BlackBerry) y PC's en la oficina u ordenadores personales (55%), tener procedimientos específicos ante pérdida o robo de equipos portátiles o móviles (55%), cifrar la información sensible que se transmite desde y dentro de la entidad (82%), cifrar la información sensible y confidencial que reposa en las bases de datos de la UIF (73%), cifrar la información contenida en dispositivos móviles (45%).

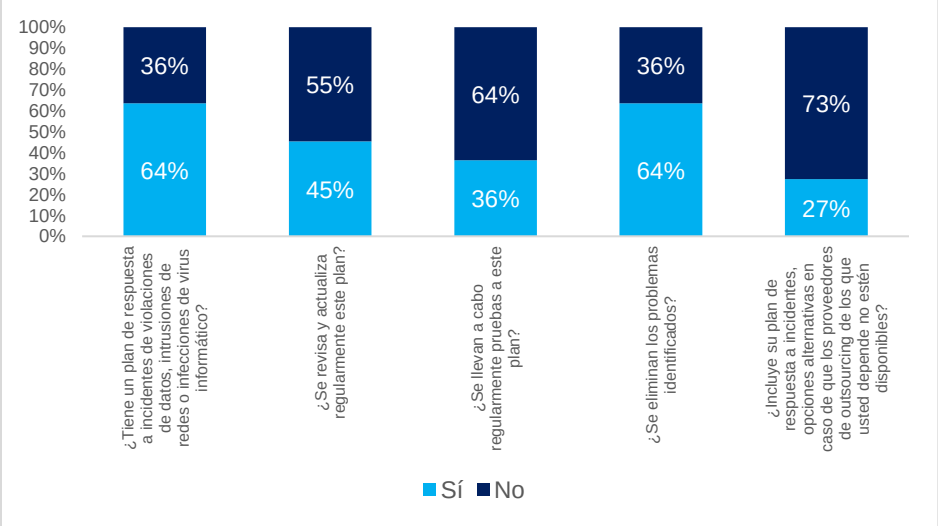
179. Estas políticas de cifrado varían entre los participantes del estudio. En algunos casos, todos los dispositivos móviles (pendrives o notebooks) deben estar cifrados; en otros casos, que **también fueron recurrentes en las entrevistas semistructuradas, se cuentan con políticas de seguridad de información adicionales tales como bloqueo de puertos USB, acceso a red a través de VPN, uso de máquinas virtuales para evitar el almacenamiento local de información**. En otros casos, políticas más estrictas de cifrado se encuentran en proceso de implementación.

Figura 32 – Aspectos relativos a cifrado de información



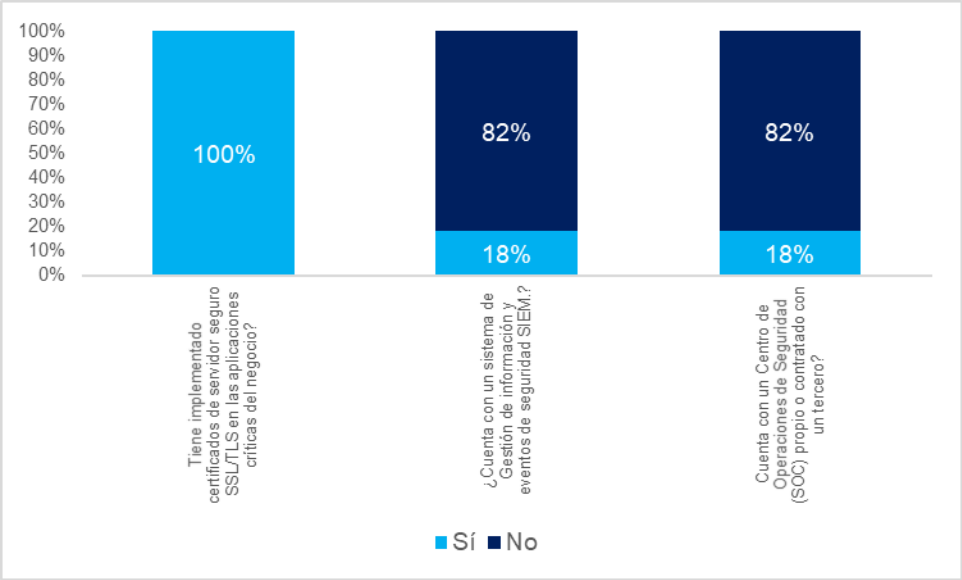
180. Un aspecto relevante corresponde el **contar con planes de respuesta a incidentes de violaciones de datos, intrusiones de redes o infecciones de virus informático** (64%), revisión permanente de dichos planes (45%), la realización de pruebas sobre el plan de intrusiones (36%) y la eliminación de problemas identificados (64%).

Figura 33 – Aspectos relativos planes de respuesta a incidentes de ciberseguridad



181. Los aspectos donde se presentan **mayores oportunidades de mejora se centran en contar con Sistemas de Gestión de Información y Eventos de Ciberseguridad – SIEM (18%), y el contar con un Centro de Operaciones de Seguridad (SOC)**

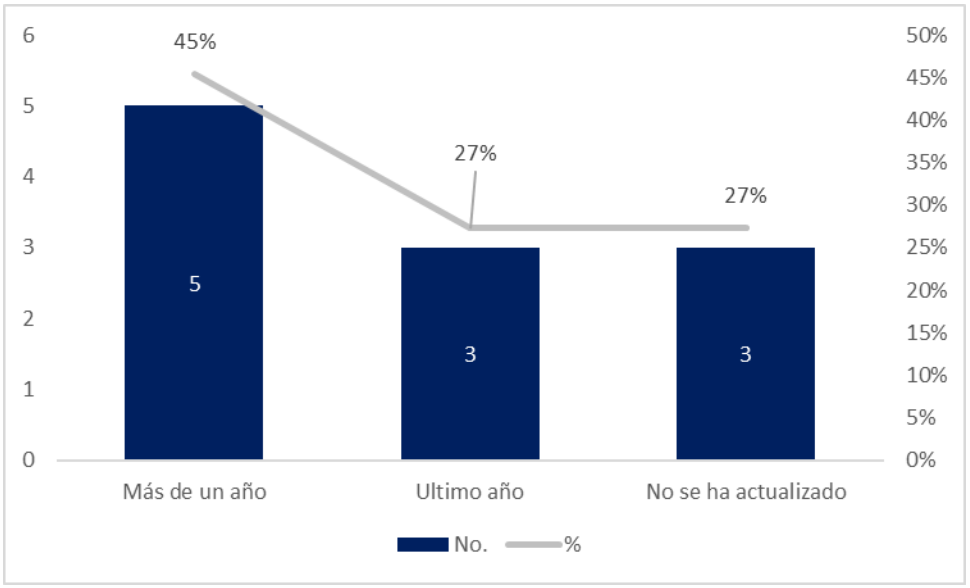
Figura 34 – Otros aspectos de seguridad de la red



182. Dentro de los **aspectos que todas las UIF han implementado están, el contar con usuarios únicos de acceso a los puestos de trabajo, que requieren cambios periódicos de claves, así como tener implementados certificados de servidor seguro SSL/TLS en las aplicaciones críticas del negocio.**

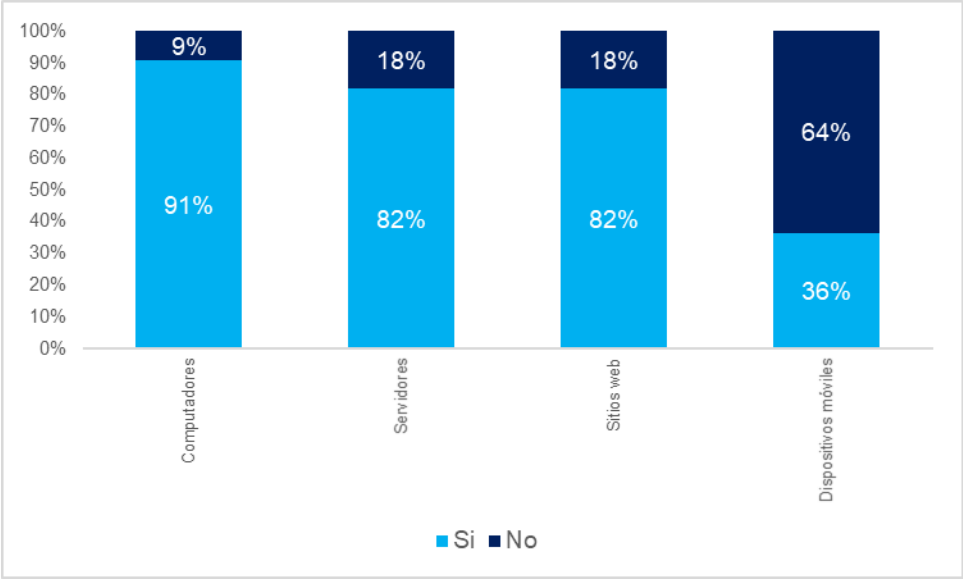
183. En relación con la actualización de la política de seguridad de la información, la mayor proporción de UIF (45%) hace más de un año no actualizan dicha política, el 27% realizaron una actualización en el último año y el 27% restante nunca han actualizado la política.

Figura 35 – Actualización de política de seguridad de la información



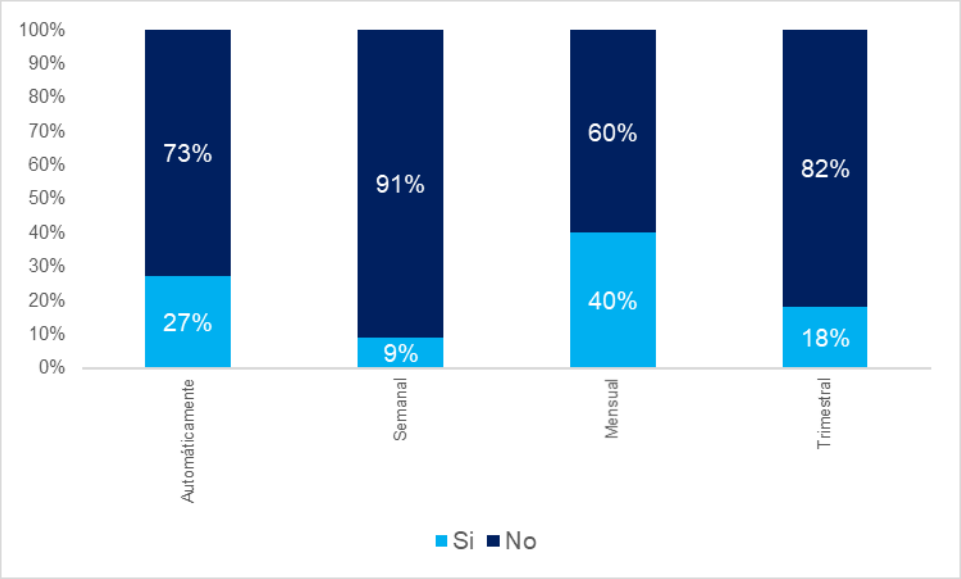
184. El 91% de los encuestados utiliza firewalls en computadores, el 82% en servidores, el 82% en sitios web y el 36% en dispositivos móviles. Este es otro aspecto relevante, puesto que el correcto funcionamiento de un firewall hace parte de una estrategia sólida de seguridad de información.

Figura 36 – Uso de firewall según dispositivo



185. Las políticas de actualización de parches de seguridad tienen diversas periodicidades. La actualización más común es mensual (40%), seguida de automáticamente (27%). Otras periodicidades tales como trimestral (18%) o semanal (9%) tiene menores proporciones. En todo caso, algunas UIF tienen actualizaciones que combina más de un intervalo de tiempo.

Figura 37 – Periodicidad de actualización de parches de seguridad



3.9. Otros elementos importantes del PCN

186. **Las UIF de la región han implementado diversas estrategias de administración y monitoreo de información.**

187. Las medidas de más amplio uso en este aspecto son el **tener implementada infraestructura tipo SAN o NAS para el almacenamiento de la información** (100% de las UIF), así como el que **los segmentos de alto riesgo de la red se encuentren segregados** (91% de las UIF).

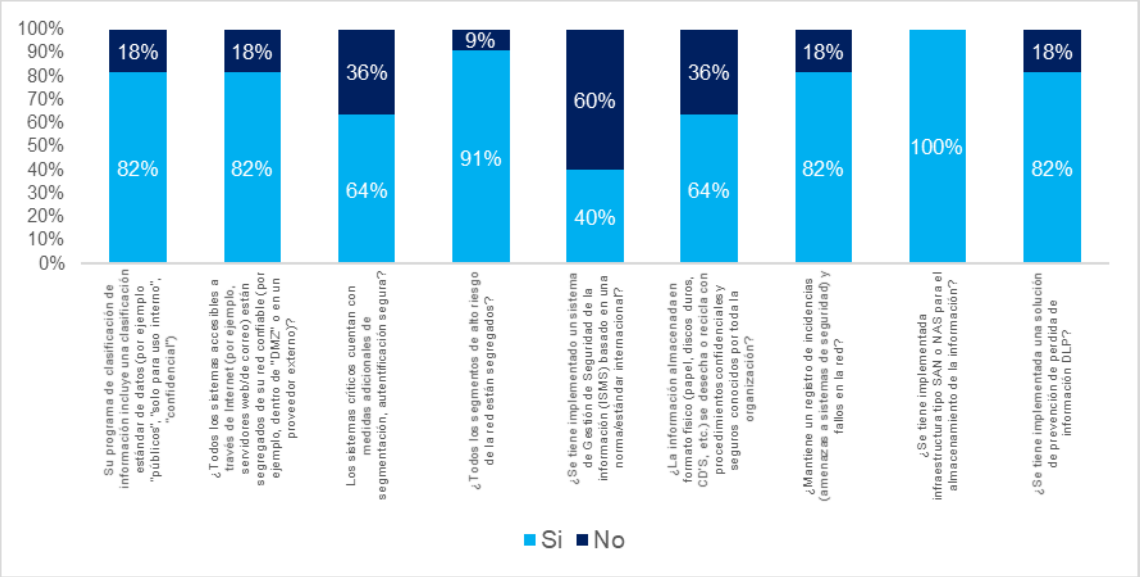
188. En este aspecto, el 82% de las UIF han contemplado en su programa de clasificación de información, categorías estándar de datos, por ejemplo “públicos”, “solo para uso interno”, “confidencial”. De igual forma, en esta misma proporción de encuestados, los sistemas accesibles a través de Internet (por ejemplo, servidores web/de correo) están segregados de su red confiable (por ejemplo, dentro de "DMZ" o en un proveedor externo); así como la implementación de alguna solución de prevención de

perdida de información DLP y el mantener un registro de incidencias (amenazas a sistemas de seguridad) y fallos en la red.

189. El 64% de las UIF tienen en sus sistemas críticos, con medidas adicionales de segmentación y autentificación segura. El mismo porcentaje de UIF desecha o recicla información almacenada en formato físico (papel, discos duros, CD'S, etc.) con procedimientos confidenciales y seguros conocidos por toda la organización.

190. La **mayor oportunidad de mejora para las UIF consiste en la ampliación de la adopción de Sistemas de Gestión de Seguridad de la información (ISMS) basados en una norma/estándar internacional**, que en la actualidad han sido implementados por el 40% de las UIF participantes.

Figura 38 – Administración y monitoreo de información



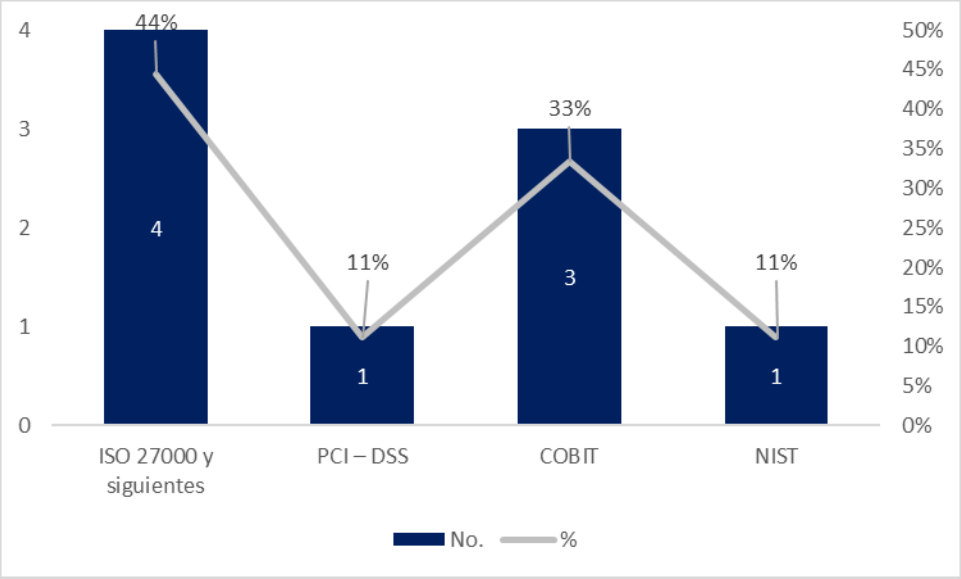
191. En relación con la segregación de sistemas, se aplican estrategias como:

a. Los sistemas y servidores y sistemas web de acceso público (entidades supervisadas o público en general) expuestos a la web, se encuentran en redes segmentadas (DMZ), en algunas ocasiones, protegidos por servicio CDN, protección de IPS y redundancia de enlaces de internet.
b. Los sistemas de información y servidores de uso restringido, se mantienen en la red segura.
c. Incluir seguridad de DNS externo.

192. De esta forma, en resumen, se implementa "**segregación de la red dependiendo de las funciones de los servidores, su exposición a internet, su exposición a los usuarios, así como una segregación de las redes de los usuarios**".

193. Finalmente, en relación con estándares o marcos de referencia asociados a seguridad de la información, el más comúnmente usado por las UIF de la región es la ISO 27000 (44%), seguido de Cobit (33%) con una participación marginal de PCI-DSS y NIST.

Figura 39 – ¿Se cumple con una o más de las siguientes leyes de seguridad/marcos de acción/estándares/requisitos?



3.10. Circunstancias adicionales

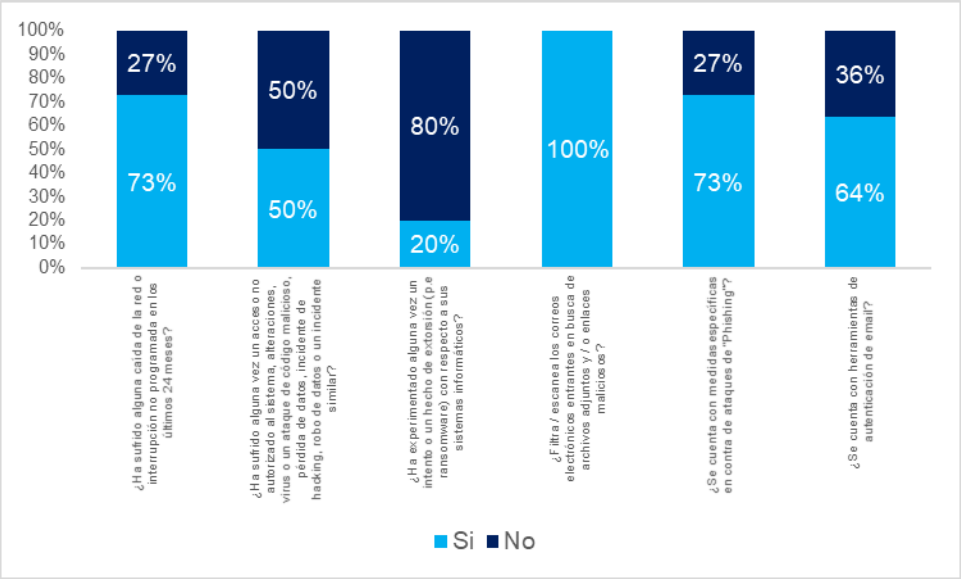
194. En primera medida, el 73% de quienes diligenciaron el instrumento sufrieron alguna caída de la red o interrupción no programada en los últimos 24 meses, lo cual evidencia que, a pesar de las medidas implementadas, no existen sistemas totalmente protegidos a interrupciones de continuidad.

195. El 50% de las UIF sufrieron alguna vez un acceso no autorizado al sistema, alteraciones, virus o un ataque de código malicioso, pérdida de datos, incidente de hacking, robo de datos o un incidente similar. **Lo cual demuestra el interés de cibercriminales de vulnerar este tipo de organizaciones**.

196. Sin embargo, **solo el 20% de las UIF han enfrentado escenarios en los cuales se haya experimentado un intento o un hecho de extorsión (p.ej. ransomware) con respecto a sus sistemas informáticos**.

197. Dentro de las medidas implementadas en la totalidad de UIF se encuentra el filtrar o escanear los correos electrónicos entrantes en busca de archivos adjuntos y/o enlaces maliciosos, mientras que el 73% de las UIF cuentan con medidas específicas en contra de ataques de "Phishing", y la proporción baja al 64% en lo que respecta a contar con herramientas de autenticación de email

Figura 40 – Medidas adicionales



3.11. Actividades de supervisión

198. El último aspecto que se contempló en el instrumento de recolección de información hizo referencia a las actividades de supervisión que algunas UIF de la región desarrollan, en función de la arquitectura normativa propia de cada país.

199. El 73% de las UIF encuestadas desarrollan actividades de supervisión.

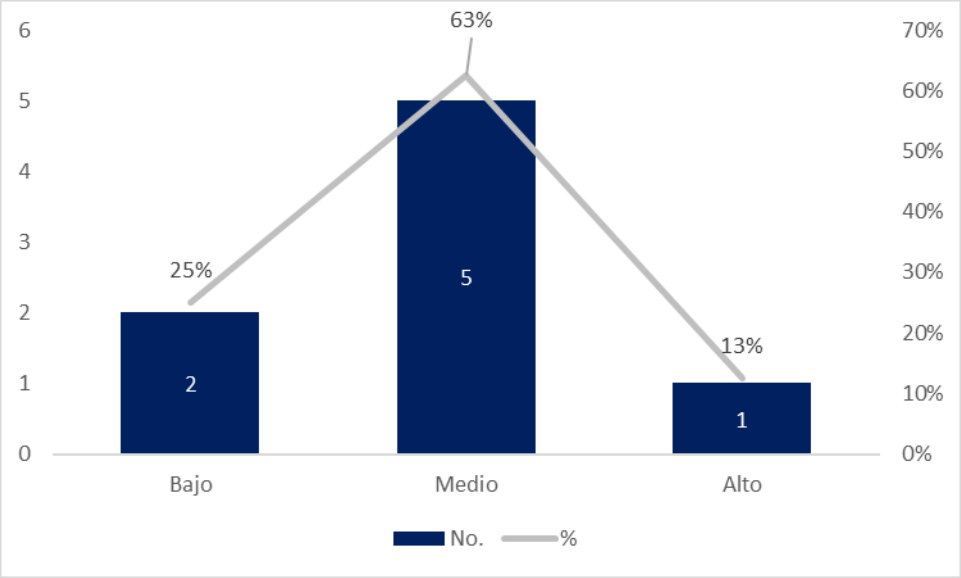
200. A pesar de tener alcances disímiles en términos de SO, en general, las actividades de supervisión se enfocan en uno o varios de los siguientes sectores:

a. APNFDs.

b. Sector Financiero, incluyendo bancos, en lo que respecta a supervisión de LA/FT/FPADM.
c. Sectores residuales de la economía.

201. Teniendo en cuenta lo anterior, la pandemia tuvo diversos niveles de afectación entre las UIF que desarrollan actividades de supervisión. Para el 25% de las UIF que diligenciaron el instrumento y que desarrollan este tipo de tareas, el nivel de afectación fue bajo, para el 63%, el nivel de afectación se considera medio y finalmente, para el 13% restante, la afectación fue alta.

Figura 41 – Nivel de afectación en actividades de supervisión de la UIF producto de la pandemia



202. En lo que respecta a l**as características de la afectación que sufrieron las actividades de supervisión**, estas se concentran en:

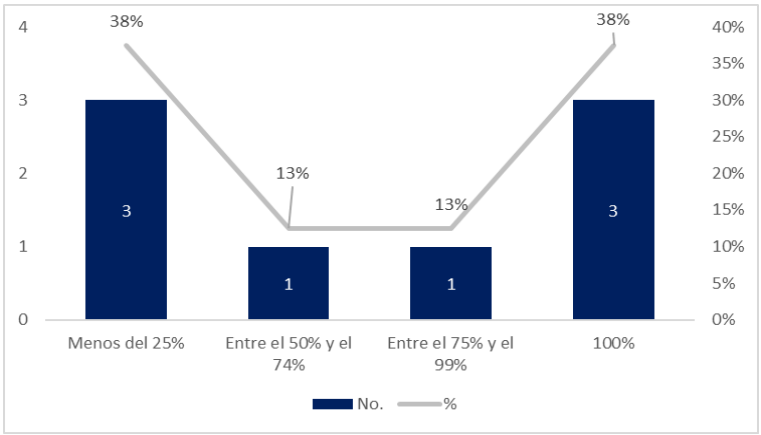
a. En función de los niveles de afectación de la pandemia y de las medidas de contención implementadas por los gobiernos, los SO presentaron limitaciones de variada intensidad en sus operaciones.
b. Lo anterior redundó en una limitación significativa de la posibilidad de supervisión in-situ. En este sentido, aunque algunas UIF que realizan supervisión de SO realizan actividades in-situ, la modalidad extra-situ ha tomado un importante momentum y se ha profundizado su uso y aplicabilidad.

203. Sin embargo, tanto en el instrumento de recolección de información como en las entrevistas no estructuradas, se observó que **las UIF desplegaron diversas acciones tendientes a minimizar el impacto de la pandemia y, por ende, asegurar un correcto proceso de supervisión, en donde fuera aplicable**. Dentro de las medidas implementadas están:

a. acciones de contingencia para realizar supervisión extrasitu
b. despliegue o profundización del uso de herramientas tecnológicas para brindar mayor apoyo a los SO.
c. Mecanismos de recolección de información para monitorear el restablecimiento de operaciones de las actividades de los SO
d. Capacitación de SO
e. Suspensión de procesos sancionatorios
f. Apoyo a los SO en el fortalecimiento de sus sistemas de administración de riesgo de LA/FT/FPADM, orientando la supervisión extra-situ en la identificación de brechas e incluso, el soporte en el cierre de dichas brechas.

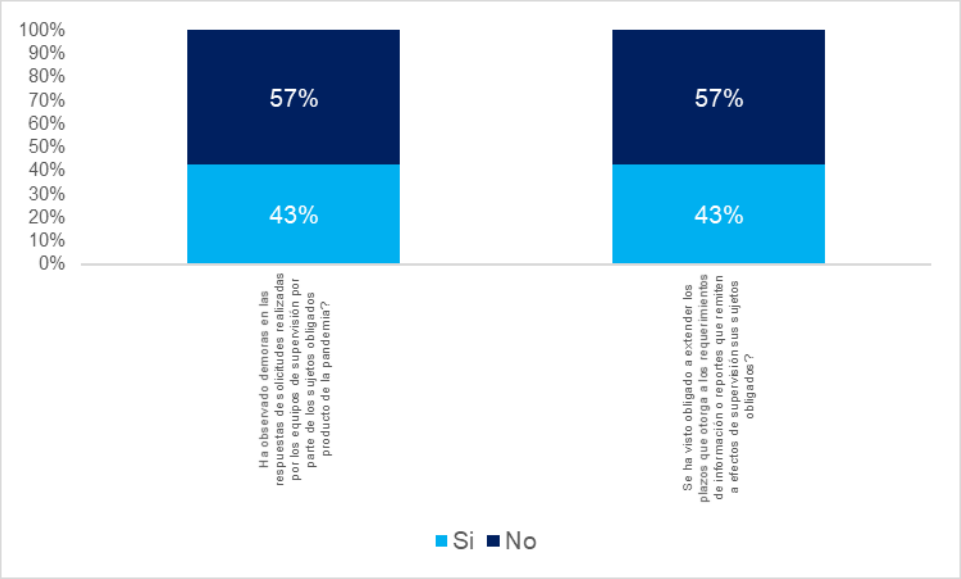
204. En este sentido, debido a la relevancia de la supervisión extra-situ, el que los equipos de supervisión cuenten con mecanismos de acceso remoto a la red corporativa se hace de vital importancia. El 38% de las UIF que desarrollan actividades de supervisión otorgan acceso remoto al 100% de los funcionarios encargados de labores de supervisión, el 13% de las UIF al 75-99% de los funcionarios de supervisión, en el 13% de las UIF dicho acceso se provee a entre el 50 y el 74% de los funcionarios con responsabilidades de supervisión y en el 38% de las UIF el acceso remoto es inferior al 25% de los encargados de supervisión de SO.

Figura 42 – Porcentaje del personal de supervisión que tiene acceso remoto a la red corporativa



205. Otro aspecto donde potencialmente se evidencian afectaciones a las labores de supervisión tiene relación con demoras por parte de los SO a las respuestas de solicitudes realizadas por los equipos de supervisión como producto de la pandemia. El 43% de las UIF que desarrollan acciones de supervisión experimentaron este tipo de demoras mientras que el 57% no experimentó dichas demoras. De esta forma, el 43% de las UIF con actividades de supervisión extendieron los plazos a los requerimientos de información o reportes que remiten a efectos de supervisión sus SO.

Figura 43 – Demoras en respuestas de requerimientos y extensión de plazos.



206. En relación con el **nivel de preparación de parte de los SO bajo supervisión de las UIF para una contingencia como la del COVID-19**, quienes diligenciaron el instrumento manifestaron, en términos generales, lo siguiente:

a. Los SO se vieron en la necesidad adaptarse a la pandemia, viéndose obligados a dejar de "operar temporal o permanentemente, otros han cambiado de actividad económica, y otros han cambiado sus procesos comerciales implementando canales de atención virtuales o semipresenciales, capacitando a sus trabajadores para realizar trabajo remoto, y adquiriendo equipos tecnológicos que les brinde dicho soporte", entre otras.
b. Debido a la heterogeneidad de las funciones de supervisión de las UIF, se observaron niveles de afectación diversos entre los SO. Sin embargo, y en particular para sector financiero, las "empresas más importantes han superado los momentos críticos en forma razonable".

c. Las empresas que sufrieron mayores niveles de impacto en la continuidad de sus operaciones, en general, pertenecían al grupo de APNFD.

207. Ante la pregunta de **posibles incumplimientos de parte de los SO bajo supervisión de la UIF a las normas ALACFTCFPADM**, se obtuvieron respuestas en una de las siguientes categorías:

a. No se observaron incumplimientos de parte de SO
b. No se observaron incumplimientos producto de la pandemia sino de la operativa de negocio.
c. Se observaron incumplimientos en la implementación de sistemas de gestión de riesgo ALACFTCFPADM

208. En lo que se refiere a cambios normativos producto de la pandemia, nuevamente, las respuestas obtenidas se enmarcan en alguna de las siguientes categorías:

a. No se han realizado ajustes normativos adicionales.
b. Se realizaron suspensiones temporales de plazos para el cumplimiento de obligaciones.
c. Ajuste temporal a los regímenes sancionatorios, consistente en sanciones de amonestación y no en multas pecuniarias, con excepción de sanciones de alta gravedad.

209. Por el momento, producto de la pandemia, no se plantea incorporar nuevos sectores como SO de supervisión bajo la órbita de las UIF encuestadas.

3.12. Otros aspectos relativos a las entrevistas no estructuradas

210. Como se expuso previamente, el instrumento de recolección de información fue complementado a través de siete (7) entrevistas no estructuradas con algunas UIF de la región. En dichas entrevistas se abordaron temas generales relativos a la respuesta de la UIF ante la pandemia de COVID-19, las estrategias de continuidad de negocio implementadas por parte de la UIF, tecnologías utilizadas, entre otros aspectos.

211. No todos los países entrevistados diligenciaron el instrumento de recolección de información. Sin embargo, las entrevistas permitieron enriquecer el análisis resultante del instrumento y se obtuvieron ópticas desde diferentes perspectivas.

212. **Dentro de los principales aspectos a resaltar de las entrevistas están**:

a. Varias UIF de la región venían implementando procesos de transformación digital, enfocados primordialmente a la digitalización de los mecanismos de

comunicación, ya sea con los SO y/o los receptores de información de inteligencia financiera. En este sentido, el haber implementado dichas tecnologías con antelación a la pandemia proporcionó una importante plataforma que permitió que, especialmente, las actividades asociadas a la recepción de información, no se vieran impactadas de forma traumática. De igual forma, aquellas UIF que habían digitalizado los mecanismos de difusión de información reforzaron la continuidad de operaciones en lo que respecta a comunicación con receptores autorizados.

b. Las UIF realizaron importantes ajustes a sus procesos internos con el fin de permitir que sus actividades se vieran impactadas lo menor posible. A este respecto, la mayor preocupación era el contar con mecanismos que aseguraran la protección y confidencialidad de la información, particularmente, en lo que respecta a acceso a bases de datos misionales y conexiones seguras remotas.
c. Dependiendo de las acciones diseñadas, se permitieron mayores o menores grados de conectividad remota de funcionarios de la UIF. En general, en aquellas UIF donde se presentaron mayores restricciones de acceso, estas tenían que ver con las actividades relacionadas con inteligencia financiera, como lo son la lectura y clasificación de ROS y el desarrollo de casos de inteligencia financiera.
d. Las tecnologías más ampliamente utilizadas por las UIF son: uso de conexiones seguras a través de VPN y accesos remotos a través de máquinas virtuales a los entornos de trabajo.
e. Algunas UIF desplegaron medidas adicionales de seguridad, tales como la realización de pruebas poligráficas a funcionarios con acceso remoto u otorgar acceso remoto a quienes hubieran aprobado pruebas poligráficas recientemente; mecanismos de autenticación fuertes de usuarios (token, firma digital, etc.), diseñó de procedimientos para intercambio de información en entornos no presenciales
f. Varias UIF implementaron estrategias de capacitación de funcionarios, en temáticas variadas, algunas de ellas asociadas a concientización y medidas de protección de ataques cibernéticos. De igual forma, se presentaron inquietudes relativas a la correcta disposición de seguridad en el trabajo de los entornos remotos de los funcionarios y seguimiento de variables asociadas al bienestar y manejo de estrés de los mismos e incluso, ajustes a los sistemas de evaluación de personal.
g. Se diseñaron diversas estrategias de comunicación permanente con las entidades reportantes, variando en alcance y profundidad. Desde boletines informativos hasta la retroalimentación constante a las entidades reportantes indicando tipologías y señales de alerta identificadas con el objetivo de apoyar los procesos

de identificación de operaciones sospechosas a tendencias delictivas durante la pandemia.

h. La oportunidad de expandir la oferta de capacitación a instituciones reportantes por medio del uso de webminars e elearning.

4. ANÁLISIS DE RIESGO

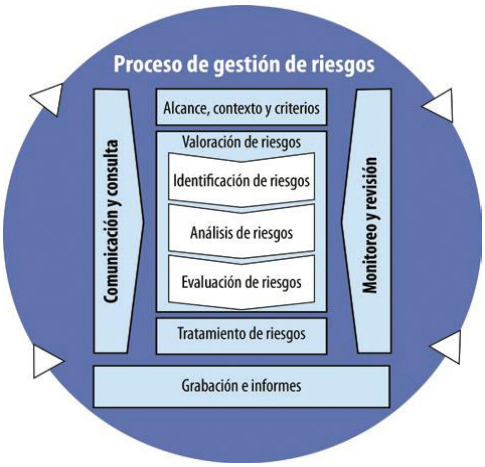
213. En concordancia con lo establecido en la norma ISO 22301:2019[77] y de acuerdo con el diagnóstico e información recolectada sobre la situación actual de la UIF se procedió a identificar, analizar y evaluar las amenazas que podrían afectar a estas organizaciones, especialmente aquellas que puedan provocar un evento que afecta la continuidad de las operaciones críticas.

214. La norma ISO 22301:2019 establece que la evaluación de riesgos, debe contemplar tres aspectos[78]:

a. Identificar el riesgo de interrupción de las actividades prioritarias de la organización;
b. analizar y evaluar los riesgos identificados.
c. Determinar cuáles riesgos necesitan tratamientos.

215. El análisis de riesgo es concordante con el proceso de gestión de riesgos definido en la norma ISO 31000:2018, el cual se presenta a continuación:

Figura 44 – Norma ISO 31000;2018. Proceso de gestión de riesgos.



[77] Seguridad y resilencia. Sistema de gestión de continuidad de negocio. Requisitos.
[78] ISO 22301:019. 8.2.3. Evaluación de riesgos

216. De igual forma, la norma ISO 22301:2018 estable la importancia del establecimiento del contexto[79], el alcance[80] y los criterios de valoración.

4.1. Establecimiento del contexto

217. El contexto interno y externo varían para cada UIF en función de diversos aspectos, sin embargo, se tienen algunos elementos en común.

218. En el contexto externo, se tendrá que evaluar la arquitectura legal bajo la cual opera la UIF. Un elemento que transversal a todas las UIF es el relativo a las exigencias planteadas desde las Recomendaciones del GAFI, en particular, lo que respecta a la Recomendación 29 y, en el caso del PCN, la nota interpretativa de dicha recomendación, sección D, la cual fue abordada con anterioridad en el presente informe.

219. En relación con el contexto interno, se debe tener en consideración el tipo de UIF, su esquema de gobernanza interna, su estructura organizacional, funciones y responsabilidades. Otro aspecto relevante en el establecimiento del contexto es el relativo a las capacidades de la UIF, tanto técnicas, tecnológicas y presupuestales, en este caso en términos del PCN, Un aspecto primordial para el establecimiento del contexto interno de las UIF es el relativo a sus sistemas de información, arquitecturas y flujos de información.

220. Estos aspectos, como se observó en el capítulo anterior, son heterogéneos entre las UIF de la región. Sin embargo, a partir de la información recolectada mediante encuestas y entrevistas, y a pesar de los niveles de afectación de la pandemia fueron heterogéneos y las respuestas de las UIF y los SO en muchas ocasiones dependieron del nivel de criticidad de las medidas de confinamiento implementadas, se identificaron las principales dificultades a las que se enfrentaron las UIF durante la pandemia:

a. Aunque en la mayoría de las entidades no hubo un paro total de actividades, la productividad si se vio afectada al no tener al 100% las personas y tecnologías disponibles en determinados momentos.
b. El reto de aprovisionar recursos tecnológicos para que el personal remoto pudiera trabajar desde casa la mayoría de las veces conectándose a las máquinas físicas de la UIF.
c. Se presentaron dificultades con los proveedores de servicios de internet y canales de comunicación siendo la conectividad inestable la mayor dificultad.

[79] Ibid 4
[80] Ibid 5

d. En la mayoría de UIF el trabajo se hizo de manera semipresencial los primeros meses.
e. La mayor preocupación radicó en mantener los mismos niveles de seguridad de la información permitiendo las conexiones remotas.
f. En varias UIF la recepción de reportes por parte de los SO fue una de las actividades que sufrió mayor impacto principalmente por retrasos. Sin embargo, el contar con sistemas de recepción electrónica de información minimizó los impactos en los procesos de recepción.
g. Las actividades de los analistas de operaciones se vieron afectadas al no poder tener acceso total a la información todo el tiempo, debido a las restricciones del trabajo remoto.
h. Una UIF presentó contagios de COVID-19 entre sus funcionarios, por lo que, además de las restricciones naturales de la pandemia, se vio en una situación de contención de contagios e implementación de medidas sanitarias.
i. En aquellas UIF que desarrollan procesos de supervisión, los dos retos de mayor relevancia en este aspecto se relacionaron con i. mantener capacidades de supervisión a través de actividades extrasitu remotas y; ii. Capacidad propia de las entidades supervisadas de continuar sus operaciones bajo condiciones de confinamiento.

4.2. Identificación de amenazas

221. Las amenazas entendidas como cualquier evento que puede afectar los activos[81] de información, hacen parte de los aspectos, que según la norma ISO 27001 deben contemplarse[82] en la identificación de riesgos.

222. Las fuentes de amenazas comunes identificadas para la mayoría de la UIF analizadas son:

[81] Recurso de valor tangible o intangible que debería ser protegido, lo que comprende personas, información, infraestructura, finanzas y reputación. ISACA. Fundamentals.
[82] ISO 27001. 4.2.1. numeral d.

Tabla 1 - Amenazas identificadas

Amenaza	Descripción
Desastres naturales	Eventos como terremoto, huracán, tsunami, incendio, inundación, entre otros; que pueden afectar la infraestructura física y tecnológica de la organización.
Ataques Informáticos	Incidente informático en el cual un ciber delincuente obtiene acceso y genera algún daño en los recursos tecnológicos de la organización.
Fallos tecnológicos	Fallo o daño en el hardware o software de la infraestructura tecnológica de la organización por obsolescencia, problemas eléctricos o falta de mantenimiento.
Errores internos no intencionales	Incidentes ocasionados por funcionarios no intencionales por falta de capacitación, errores humanos u omisiones.
Problemas sociales y de salud publica	Eventos sociales como huelgas, atentados terroristas, robos y problemas de salud pública como pandemias.

4.3. Clasificación del riesgo

223. El riesgo, según la norma ISO 31000:2018, se define con el "efecto de la incertidumbre sobre los objetivos".

224. En el caso de UIF, el riesgo asociado al PCN, representa el nivel de incertidumbre para el cumplimiento de los objetivos misionales de la institución, de acuerdo con las amenazas identificadas en los procesos existentes. Aunque el principal tipo de riesgo al que se puede exponer una organización al evaluar los PCN se asocia a riesgos operativos, indudablemente los demás tipos de riesgos pueden materializarse si el plan no se implementa correctamente. Por esta razón, se recomienda tener en cuenta la siguiente clasificación de riesgos cuando se valoren los riesgos:

Tabla 2 – Tipos de riesgos

Identificación	Nombre	Descripción
R1	Riesgo Estratégico.	Afectación de las decisiones que definen hacia dónde va la entidad.
R2	Riesgos de Imagen.	Afectación del buen nombre de la entidad, comprometiendo la confianza de las partes interesadas.
R3	Riesgos Operativos.	Interrupción o afectación del desempeño normal de las actividades y operaciones de la Entidad.
R4	Riesgos Financieros.	Pérdidas económicas causadas para la Entidad.
R5	Riesgos de Cumplimiento	Sanciones legales por la no aplicación del marco legal y regulatorio relacionado con seguridad de la información.

4.4. Criterios de valoración

225. Con el objetivo de poder realizar una valoración de riesgo[83] consistente, es fundamental, además de la definición de escalas de valoración, determinar los criterios de valoración. Es decir, la representación de cada escala.

226. La valoración de riesgos puede realizarse desde un enfoque cualitativo, semicualitativo o cuantitativo. El grado de "detalle que se requiere dependerá de la aplicación particular, la disponibilidad de datos confiables, de las necesidades para la toma de decisión de la organización"[84].

227. Existen diversos mecanismos de valoración de riesgo, sin embargo, la matriz probabilidad-consecuencia o probabilidad impacto, es una herramienta ampliamente utilizada en esta labor.

228. Según la norma ISO 31010, esta técnica es "rotundamente aplicable" en el proceso de valoración de riesgo (identificación; análisis incluyendo consecuencia, probabilidad y nivel de riesgo) y "aplicable para "evaluación de riesgo.

[83] Proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo. ISO 31000. 5.4.1.
[84] ISO 31010. 5.3.1.

229. La matriz consecuencia – probabilidad es "un medio para combinar calificaciones cualitativas y semicualitativas de consecuencias y las probabilidades para producir un nivel de riesgo o una calificación de riesgo"[85].

230. La matriz probabilidad – consecuencia tiene diversos usos[86]:

a. Para calificar riesgos, fuentes de riesgo o tratamientos para el riesgo con base en el nivel de riesgo.
b. Como herramienta de clasificación cuando se han identificado muchos riesgos.
c. Para seleccionar los riesgos que no necesitan consideración adicional en el momento de la evaluación
d. Para determinar si un riesgo específico es aceptable en forma amplia o no es aceptable en función de la zona donde se ubica en la matriz.
e. Como herramienta de comunicación de los niveles cualitativos de los riesgos en toda la organización.

231. Se debe tener en cuenta que la matriz probabilidad – consecuencia tiene fortalezas y limitaciones, las cuales se presentan a continuación

Tabla 3 – Matriz probabilidad – consecuencia. Fortalezas y limitaciones [87].

Limitaciones	Fortalezas
La matriz se debe diseñar de manera que sea adecuada para las circunstancias. Es difícil definir las escalas sin ambigüedad. El uso es muy subjetivo y tiende a haber variación significativa entre quienes califican. Los riesgos no se pueden acumular (es decir no se puede definir que un numero particular de riesgos bajos o un riesgo bajo identificado una cantidad de veces en particular sea equivalente a un riesgo medio).	Relativamente fácil de utilizar Proporciona una calificación rápida de los riesgos en diferentes niveles de importancia

[85] Ibid B.29.1.
[86] Ibid B.29.2.
[87] Ibid B.29.6.

Es difícil combinar y comparar el nivel de riesgo para diversas categorías de consecuencias.	

232. En este sentido, es necesario establecer las escalas de probabilidad y consecuencia, también conocida como impacto.

4.4.1. Escala de probabilidad

233. Con probabilidad se hace referencia a "la oportunidad que algo suceda, esté o no definido, medido o determinado objetiva o subjetivamente cualitativa o cuantitativamente, y descrito utilizando términos generales o matemáticos (como la probabilidad numérica o la frecuencia en un periodo de tiempo determinado)."[88]

234. Para cada amenaza identificada, se debe analizar el número de veces que ésta puede ocurrir en un lapso determinado. Se sugiere como guía la siguiente tabla para que el experto del proceso de valoración de riesgos identifique a cuál corresponde

Tabla 4 – Escala de probabilidad

Valor		Probabilidad
Cualitativo	**Cuantitativo**	
Casi seguro	5	Se espera que el evento ocurra en la mayoría de las circunstancias. Mas de una vez al año
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias. Al menos una vez en el último año
Posible	3	El evento podría ocurrir en algún momento. Al menos una vez en los últimos dos años
Poco probable	2	Una vez en los últimos tres años
Raro	1	No se ha presentado en los últimos tres años

235. Cuando no se cuente con estadísticas o registros sobre la ocurrencia o materialización de una amenaza determinada, el cálculo de la probabilidad se lleva a cabo basado en el conocimiento y experiencia del experto en el proceso y que a su vez se puede basar en registros o estadísticas de organizaciones del mismo sector.

[88] ISO Guía 73:2009. Definición 3.6.1.3.

4.4.2. Escala Consecuencia (Impacto)

236. La consecuencia, entendida como el resultado de un evento que afecta, positiva o negativamente, los objetivos[89] debe también ser evaluados.

237. Se propone tener en cuenta la siguiente escala de impacto para evaluar los riesgos a los que están expuestas las UIF frente a las amenazas que puedan perturbar las operaciones criticas identificadas. Cabe anotar que el ámbito económico tendría que evaluarse si es aplicable a la UIF en particular.

Tabla 5 – Escala de Impacto

Impacto	Cuantitativo	Ámbito impactado	Descripción del impacto
Catastrófico	5	Económico	• Pérdida o reducción en ingresos de más del 5%
		Operativo	• Ausencia de prestación de servicios misionales. • Incumplimiento en la prestación de servicios críticos. • Afectación de la credibilidad e imagen de la UIF a nivel internacional.
		Legal o regulatorio	• Sanciones y multas por incumplimiento de normatividad o legislación aplicable a nivel internacional.
		Tecnológico	• Indisponibilidad de infraestructura tecnológica para procesos críticos. • Falta de acceso a la información crítica del negocio.
Mayor	4	Económico	• Pérdida o reducción en ingresos entre el 2% y 4,9%
		Operativo	• Fallas, errores, inconsistencias e inexactitud en la prestación de los servicios misionales. • Afectación de la credibilidad e imagen de la UIF a nivel Nacional.
		Legal o regulatorio	• Sanciones y multas por incumplimiento de normatividad o legislación aplicable a nivel nacional.
		Tecnológico	• Indisponibilidad de parte de la infraestructura tecnológica para procesos críticos. • Indisponibilidad de sistemas de información complementarios o de apoyo

[89] Ibid. Definición 3.5.1.3.

Impacto	Cuantitativo	Ámbito impactado	Descripción del impacto
Moderado	3	Económico	• Pérdida o reducción en ingresos entre el 1% y 1,9%
		Operativo	• Problemas técnicos o logísticos en la prestación de los servicios misionales. • Afectación de la credibilidad e imagen de la UIF a nivel local.
		Legal o regulatorio	• Sanciones y multas por incumplimiento de normativa local.
		Tecnológico	• Pérdida temporal de acceso a servicios informáticos complementarios o de apoyo
Menor	2	Económico	• Pérdida o reducción en ingresos entre el 0,5% y 0,9%
		Operativo	• Fallas temporales en la prestación de servicios de carácter administrativo. • Afectación de la credibilidad e imagen de la UIF a nivel interno.
		Legal o regulatorio	• Amonestaciones o llamados de atención por incumplimiento de normativa local.
		Tecnológico	• Falla temporal de equipos informáticos no esenciales
Insignificante	1	Económico	• Pérdida o reducción en ingresos entre el 0,1% y 0,4%
		Operativo	• Demoras en la prestación de servicios de carácter administrativo.

4.5. Apetito de riesgo

238. A pesar que los estándares ISO no exigen en su proceso de valoración de riesgo la determinación del apetito de riesgo, se considera recomendable que desde la Alta Dirección de las UIF se defina este aspecto, debido a que hace parte integral de la gestión de riesgos corporativos, debido a que el apetito de riesgo define si los riesgos se encuentran dentro de los límites aceptados[90]. Sin embargo, la definición de apetito de riesgo hace parte del principio 7 del marco de referencia COSO[91].

239. La definición del apetito de riesgo tiene ventajas en cuatro (4) dimensiones[92]:

a. Estratégica: el apetito de riesgo ayuda a alinear los objetivos de la institución con el perfil de riesgo, diferenciando los riesgos que son admisibles de los que no lo

[90] Deloitte (2018), Apetito al riego. Ajustando los riesgos a nuestra medida.
[91] COSO (2020). Compliance risk management. Applying the COSO ERM Enterprise Risk Management. P. 12
[92] Instituto de Auditores Externos de España. Buenas prácticas de gestión de riesgo. Definición e implantación de Apetito de Riesgo. P. 20.

son. De esta forma, el apetito de riesgo integra la gestión de riesgos en la toma de decisiones operativas y la asignación de responsabilidades sobre los riesgos aceptados. Así, se mejora la planificación estratégica, se aumenta la efectividad del proceso de toma de decisiones y se desarrollan esquemas de seguimiento y medición del desempeño del riesgo

b. Operacional: el apetito soporta las actividades de inserción de la gestión de riesgos en los procesos operativos e integra los riesgos en la toma de decisiones operativas, mejorando el análisis de costo/beneficio de dichas decisiones y apoyando la asignación de recursos de forma más eficiente.
c. De Información: identificando los eventos relevantes para una organización en términos de riesgos potenciales y comunicándolos a las partes que demanden información, apoyando la conformación de una estructura de reporte clara. También, hace explícita la actitud de la alta dirección frente al riesgo, considera todos los grupos de interés y sus preferencias, crea una comunicación basa en pautas comunes para todos los grupos y, desarrolla un sistema de reporte integrado.
d. De cumplimiento: ayudando a determinar responsable y conscientemente aquello que la institución puede y no puede hacer, permitiendo mejorar la transparencia e implantando una cultura de gestión de riesgo.

240. En este orden de ideas, el **apetito de riesgo** puede definirse como "el riesgo que se está dispuesto a aceptar en la búsqueda de la misión/visión de la entidad"[93]. De otro lado, la **capacidad de riesgo** corresponde a "la cantidad de riesgo que una entidad es capaz de soportar en la búsqueda de sus objetivos"[94], mientras que la **tolerancia al riesgo** es "el nivel aceptable de variación que una entidad está dispuesta a aceptar en relación con el cumplimiento de sus objetivos"[95]. Gráficamente, estos tres conceptos se relacionan como se presenta a continuación:

[93] COSO. 2012. Compliance risk management. Applying the COSO ERM Enterprise Risk Management. Enterprise risk management. Understanding and Communicating Risk Appetite. P. 4
[94] Ibid
[95] Ibid

Figura 45 – Apetito, tolerancia y capacidad de riesgo[96].

4.6. Valoración del riesgo

241. Corresponde al producto cartesiano entre las variables probabilidad e impacto, tomando los valores identificados para cada amenaza en el proceso en estudio. Para esto se construye una tabla donde se cruzan estas variables, tal como se sugiere a continuación:

Tabla 6 – Mapa de calor

		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
PROBABILIDAD	Casi seguro	Alto	Alto	Extremo	Extremo	Extremo
	Probable	Moderado	Alto	Alto	Extremo	Extremo
	Posible	Bajo	Moderado	Alto	Extremo	Extremo
	Poco probable	Bajo	Bajo	Moderado	Alto	Extremo
	Raro	Bajo	Bajo	Moderado	Alto	Alto

242. Cabe anotar que se contará entonces con dos (2) valoraciones, de un lado de riesgo inherente, es decir, el riesgo que existe de manera intrínseca en cada actividad y que no puede ser eliminado y; de riesgo residual[97], que corresponde al riesgo remanente después del tratamiento del riesgo.

[96] https://nahunfrett.blogspot.com/2014/02/definiciones-de-apetito-tolerancia-y.html
[97] ISO Guía 73:2009. Definición 3.6.8.1.1.

243. Con base en la información recolectada de las UIF y las escalas de valoración recomendadas en las tablas anteriores, se obtiene como resultado el siguiente análisis de riesgo inherente basado en las amenazas comunes identificadas y los riesgos que pueden causar una interrupción de las actividades misionales. De igual forma, se incluyen los controles típicos para las amenazas descritas. No se realiza una evaluación de riesgo residual debido a que la efectividad de los controles, sus tipos, características y demás aspectos que afectan la valoración de los mismos difieren entre las UIF.

Tabla 7 – Principales amenazas que afectan la continuidad de operaciones de las UIF

Amenaza	Riesgo	Prob.	Imp.	Nivel	Controles
Desastres naturales	Indisponibilidad de servicios críticos por desastres naturales	1	5	A	Copias de seguridad Servidores replicas Servicios en Nube
Ataques Informáticos	Interrupción y/o daños de servicios críticos por ataques informáticos	4	4	E	Copias de seguridad Antimalware, Firewall Capacitación de personal
Daños tecnológicos	Interrupción de servicios críticos por Daños tecnológicos	3	4	E	Mantenimiento de HW Actualización y parcheo de SW
Errores internos no intencionales	Interrupción y/o daños de servicios críticos por incidentes internos no intencionales	3	3	A	Copias de seguridad
Problemas sociales y de salud publica	Indisponibilidad de servicios críticos por incidentes sociales y de salud publica	2	5	E	Copias de seguridad Trabajo remoto

244. Los controles listados corresponden a mecanismos implementados e identificados por algunas UIF en el levantamiento de información.

245. Los riesgos identificados y valorados anteriormente pueden variar dependiendo de las circunstancias particulares de cada organización, pero se espera que este análisis de riesgos sirva de guía para la verificación y actualización de los riesgos identificados por las UIF durante la pandemia.

246. De forma complementaria, podrá realizarse un análisis de riesgos de ciberseguridad, que tienen íntima relación con el PCN. Dentro del amplio rango de amenazas de ciberseguridad, en las entrevistas estructuradas consistentemente se planteó la preocupación de la seguridad de información en conexiones remotas, en este sentido, podrán tenerse en cuanta un amplio espectro de situaciones, dentro de las cuales se encuentran, por ejemplo, las amenazas humanas intencionales que preceden de un origen remoto como lo son:

a. Acceso lógico con intercepción pasiva.
b. Acceso lógico con corrupción de información en tránsito o de configuración.
c. Acceso lógico con modificación de información en tránsito.
d. Suplantación de origen o de identidad.
e. Repudio del origen o de la recepción de información en tránsito.

4.7. Análisis de impacto de negocio (BIA)

247. El análisis de impacto de negocio permite identificar los procesos críticos para las UIF y estimar tiempos de recuperación para que los procesos claves entren en operación rápidamente ante una interrupción asignándoles la mayor prioridad posible.

248. El BIA[98] analiza la manera en que los riesgos clave alteran las operaciones e identifica y cuantifica las capacidades que serían necesarias para su gestión. En este sentido, el BIA brinda una comprensión en relación con:

a. La identificación y la criticidad de los procesos clave de negocio, las funciones y los recursos asociados y las interdependencias importantes que existen para la entidad;
b. La manera en la cual los eventos perturbadores afectarán la capacidad y la habilidad para lograr los objetivos críticos y;
c. La capacidad y habilidad necesarias para la gestión del impacto de una alteración y la recuperación de la organización hasta los niveles de operación pactados.

249. El BIA se utiliza para determinar la criticidad y los marcos temporales de recuperación de los procesos y los recursos asociados (personas, equipos, tecnología) para garantizar el logro de los objetivos.

[98] ISO 31010. B.11

4.7.1. Definición de procesos críticos

250. Teniendo en cuenta las funciones primordiales o etapas en el proceso de análisis de información de una UIF, se sugiere identificar los procesos críticos basados en las siguientes cuatro (4) grandes actividades:

a. **Notificación (recepción de información)**: durante este proceso se debe asegurar la disponibilidad de las aplicaciones mediante las cuales se reciben los reportes por parte de los SO, manteniendo la misma confidencialidad e integridad de los datos reportados.
b. **Análisis de Información**: en este proceso, se debe garantizar que los analistas de información tengan acceso a las herramientas y datos necesarios para realizar su labor de forma remota, manteniendo la confidencialidad e integridad de la información de la organización.
c. **Comunicación del resultado del análisis de la información**: garantizar que la comunicación y comunicación de los casos e informes respectivos, se realice de forma segura a los receptores competentes, utilizando medio digitales, pero manteniendo la confidencialidad e integridad de la información
d. **Supervisión (en aquellas UIF donde se ejecuten este tipo de actividades)**: asegurar que los procesos de supervisión y comunicación con las entidades objeto de supervisión, se realicen de forma segura, permitiendo a los equipos de supervisión ejecutar sus labores de forma remota, manteniendo la confidencialidad e integridad de la información de la institución.

251. Estos procesos son elegidos debido a que, en caso de un evento que implique una interrupción de estos, la importancia e impacto para la UIF de su disponibilidad tendría un margen alto.

252. Es importante recalcar la importancia que tienen las áreas de tecnología dentro de la UIF como área que soporta los procesos misionales de la organización.

4.7.2. Identificar impactos, RTO y RPO

253. El BIA implica determinar las labores y los recursos esenciales para respaldar la continuidad de las operaciones de la UIF, su criticidad, su impacto para el negocio, sus RTO[99] y RPOs[100].

254. La definición de estos valores se sugiere de acuerdo con el promedio de los valores indicados en las entrevistas con las UIF:

[99] RTO: lapso en el cual debe restaurarse el proceso después de un desastre
[100] RPO: punto en el tiempo a partir del cual los datos deben ser restaurados

Tabla 8 – Servicios críticos. RTO y RPO sugeridos

Servicios Críticos	RTO Sugerido	RPO Sugerido
Notificación	< 2 horas	< 24 horas
Análisis de Información	< 4 horas	< 24 horas
Comunicación	< 6 horas	< 24 horas
Supervisión	< 24 horas	< 48 horas

4.7.3. Priorización de los procesos

255. Los RTO y los impactos sugeridos en el anterior punto se convierten en la base para definir y priorizar el orden en que se deberían restablecer las operaciones en las áreas críticas y así mismo las estrategias de continuidad que serán consideradas para cada proceso.

256. Se recomienda el siguiente orden de atención de los procesos de misión crítica, definidos de esa forma por su importancia para el desarrollo de las actividades encaminadas al desarrollo de la misión de la UIF

Tabla 9 – Servicios críticos. Priorización

Servicios Críticos	Prioridad	Observación
Notificación	Alta	Los procesos involucrados en esta etapa son de alta prioridad porque garantizan la recepción de información que sirve de materia prima para el desarrollo de las demás actividades misionales. Una interrupción en los servicios de notificación tiene efectos en la percepción de los SO sobre las capacidades de la UIF
Análisis de Información	Alta	Los procesos involucrados en esta etapa son de alta prioridad porque allí se desempeñan las actividades que generan valor para una UIF.

Servicios Críticos	Prioridad	Observación
		El flujo de información desde la UIF a distintos receptores autorizados depende de que los procesos de análisis de información se ejecuten sin interrupciones. La afectación en los procesos de análisis de información son insumo en el desarrollo de las actividades de los receptores y tienen efectos en la percepción de dichos receptores sobre las capacidades de la UIF.
Comunicación	Media	Los procesos involucrados en esta etapa son de prioridad media porque muestran el resultado de los demás procesos y la interacción con otras entidades. La alteración de los procesos de comunicación puede afectar la percepción de los receptores autorizados sobre las capacidades de la UIF.
Supervisión	Alta	Los procesos asociados a las acciones de supervisión se consideran de prioridad alta debido a que su afectación tiene implicaciones en la implementación de los sistemas ALA/CFT por parte de los supervisados. La alteración de estos procesos puede afectar los niveles de cumplimiento de supervisados y la percepción de la UIF.

5. CONCLUSIONES

257. A manera de resumen, como principales conclusiones del proceso de análisis de información presentado previamente, utilizando como insumo tanto las encuestas como las entrevistas no estructuradas, se tiene que:

a. A pesar que el periodo de análisis del año 2020 (enero-agosto) corresponde al 83% del periodo de tiempo del año 2019 (enero-diciembre) y a que en algunas jurisdicciones pueden darse picos de reporte hacia final de año, en el 27% de los encuestados, al compararse los ROS remitidos en el 2020 (parcial) versus el 2019, **se presentó un aumento de ROS en este periodo**.

b. Al comparar los mismos periodos de tiempo, no en todos los casos se presentaron reducciones en los volúmenes de requerimientos de información a través del canal seguro Egmont, tanto en recepción como en solicitud, siendo más marcada la reducción en los requerimientos recibidos.

c. En lo referente a casos de inteligencia financiera, al comparar el 2019 y el 2020 (parcial) no todas las UIF analizadas presentaron reducciones en el número de casos difundidos a autoridades competentes, y en donde se presentaron reducciones, en la mayoría de los países dichas reducciones no fueron drásticas.

d. Se observa que todas las UIF entrevistadas, en mayor o menor medida, implementaron estrategias de adaptación en los procesos de recepción, análisis y difusión de información, ya fuese a través de medidas de trabajo remoto (incluyendo políticas de ciberseguridad) y/o la implementación de protocolos de bioseguridad y modificaciones de horarios laborales o turnos, para el desempeño de sus labores desde las instalaciones de la institución. Se requirieron, en muchos casos, ajustes en los procesos de negocio, con el fin de adaptarlos a las nuevas condiciones. Diversos participantes expusieron el enfoque en una mayor articulación con los SO, a través del uso de canales digitales, brindando información de diversa índole, incluyendo señales de alerta y otra información de interés para los SO. De igual forma, en algunos casos, se tomaron medidas administrativas, tales como la extensión de plazos de reporte, régimen sancionatorio especial, para SO, implementación de supervisión extra-situ en aquellas UIF que cumplen labores de supervisión, entre otras medidas.

e. En lo que respecta a accesos remotos de los funcionarios de las UIF, en aquellas UIF donde dichas medidas fueron implementadas, la proporción de funcionarios de análisis operativo es mayor o igual a la proporción de funcionarios de análisis estratégico bajo conexión remota, solo en tres países reportó una tendencia inversa.

f. El 55% de las UIF han realizado un BIA, mientras que el 45% aún no han realizado esta acción.
g. El 64% de las UIF participantes del instrumento no cuentan con un PCN, el porcentaje de UIF que cuentan con un DRP aumenta al 55%, lo cual sienta una base importante para el PCN.
h. A pesar que no todas las UIF de la región cuentan con un PCN explícito, durante la pandemia implementaron en su gran mayoría, en función de la intensidad de las cuarentenas decretadas, medidas rápidas y efectivas que permitieran una operación continua de las actividades de inteligencia financiera y de supervisión en donde fuera aplicable, de tal forma que el impacto en las operaciones fuera mínimo.
i. Adicionalmente, una proporción importante de las UIF (83%) que en la actualidad no cuentan con un PCN, tienen programado su diseño en un plazo de máximo un año.
j. Los análisis de vulnerabilidades externas de los sistemas de las UIF es uno de los aspectos que muestra fortaleza entre las UIF que diligenciaron el instrumento.
k. El 100% de los entrevistados realizan copias de seguridad de los sistemas críticos, como lo es la base de datos de ROS. Estos procesos son totalmente automáticos, lo que reduce la posibilidad que se presenten eventos de riesgo operativo en su desarrollo. De igual forma, las UIF toman variadas acciones para preservar la información, tales como backups incrementales, respaldo externo e incluso, respaldo externo en bóveda bancaria. Así mismo, los backups tienen periodicidades disimiles, desde diarios hasta anuales, con políticas de respaldo tales como cintas en backups semanales.
l. En ese sentido, el 100% de las UIF que diligenciaron el instrumento, poseen sistemas de backup onsite. Sin embargo, el 55% de las estas cuentan con mecanismos alternos de backup. En este sentido, el 45% cuenta con backup offsite y el 27% cuenta con backup offline. También es importante resaltar que el 18% cuenta con más de dos mecanismos de backup. Todos estos aspectos relativos a los backups de información proveen importantes capacidades a las UIF para reaccionar de forma rápida y eficiente ante eventos adversos.
m. En relación con la redundancia de los sistemas de comunicación, el 55% de los encuestados manifestaron contar con enlaces telefónicos alternos, mientras que el 82% cuenta con enlace de comunicación de internet alterno o redundante. Este elemento provee una fortaleza a las UIF en términos de capacidad de recuperación y de mantener sus funciones primordiales de recolección, análisis, difusión de información y comunicación con diversas partes interesadas.

n. El 91% de quienes diligenciaron el instrumento cuenta con planes y disponibilidad para que al menos el personal crítico realice sus labores de manera remota. Tan solo el 27% de las UIF ha brindado capacitación al personal relativa al PCN, los procedimientos, roles y responsabilidades, aunque en las entrevistas no estructuradas, diversas UIF desplegaron mecanismos de entrenamiento de personal, en temas misionales, pero también en temáticas relacionadas con medidas de ciberseguridad.
o. Aunque solo el 9% cuenta con ubicaciones alternas para operar, en casos de disrupción de operaciones, en situaciones extremas como las que se presentaron bajo pandemia, el uso de instalaciones alternas, aunque es una medida recomendada en los PCN, cuando se impone por parte del gobierno medidas de confinamiento estricto, no resultan efectivas dado que ninguna ubicación, principal o alterna puede ser utilizada.
p. Se observa que el 36% de las UIF cuentan con servicios de computación en la nube y la misma proporción subcontrata actividades críticas de tecnologías de información
q. Para el 82% de las UIF, una interrupción de hasta 24 horas en el acceso a sistemas tiene impactos significativos en la continuidad de operaciones.
r. A pesar que el 55% de las UIF han designado un responsable para temas de ciberseguridad con un rol específico, como puede ser un CISO, las UIF que diligenciaron la encuesta, han implementado diversas estrategias de seguridad de red. Estas corresponden a la implementación de políticas, uso de herramientas especializadas de software de seguridad de red, diseño de planes de respuesta, capacitación de personal, entre otras.
s. Las UIF de la región implementan diversas estrategias de cifrado de información. También fueron recurrentes en las entrevistas semistructuradas, el contar con políticas de seguridad de información adicionales tales como bloqueo de puertos USB, acceso a red a través de VPN, uso de máquinas virtuales para evitar el almacenamiento local de información.
t. La totalidad de UIF que diligenciaron la encuesta han implementado mecanismos adicionales como el contar con usuarios únicos de acceso a los puestos de trabajo, que requieren cambios periódicos de claves, así como tener implementados certificados de servidor seguro SSL/TLS en las aplicaciones críticas del negocio.
u. Las UIF de la región han implementado diversas estrategias de administración y monitoreo de información Las medidas de más amplia implementación en este aspecto son el tener infraestructura tipo SAN o NAS para el almacenamiento de la

información (100% de las UIF), así como el que los segmentos de alto riesgo de la red se encuentren segregados (91% de las UIF).

v. El 50% de las UIF sufrieron alguna vez un acceso no autorizado al sistema, alteraciones, virus o un ataque de código malicioso, pérdida de datos, incidente de hacking, robo de datos o un incidente similar. Lo cual demuestra el interés de cibercriminales de vulnerar este tipo de organizaciones. Sin embargo, solo el 20% de las UIF han enfrentado escenarios en los cuales se haya experimentado un intento o un hecho de extorsión (p.ej. ransomware) con respecto a sus sistemas informáticos.

w. En lo que respecta a las características de la afectación que sufrieron las actividades de supervisión, estas se concentran en:
    i. En función de los niveles de afectación de la pandemia y de las medidas de contención implementadas por los gobiernos, los SO presentaron limitaciones de variada intensidad en sus operaciones.
    ii. Lo anterior redundó en una limitación significativa de la posibilidad de supervisión in-situ. En este sentido, aunque algunas UIF que realizan supervisión de SO realizan actividades in-situ, la modalidad extra-situ ha tomado un importante momentum y se ha profundizado su uso y aplicabilidad.

x. Las UIF con responsabilidades de supervisión, desplegaron diversas acciones tendientes a minimizar el impacto de la pandemia y, por ende, asegurar un correcto proceso de supervisión. Dentro de las medidas implementadas están:
    i. acciones de contingencia para realizar supervisión extrasitu
    ii. despliegue o profundización del uso de herramientas tecnológicas para brindar mayor apoyo a los SO.
    iii. Mecanismos de recolección de información para monitorear el restablecimiento de operaciones de las actividades de los SO
    iv. Capacitación de SO
    v. Suspensión de procesos sancionatorios
    vi. Apoyo a los SO en el fortalecimiento de sus sistemas de administración de riesgo de LA/FT/FPADM, orientando la supervisión extra-situ en la identificación de brechas e incluso, el soporte en el cierre de dichas brechas

258. Dentro de los principales aspectos a resaltar de las entrevistas no estructuradas están:

a. Varias UIF de la región venían implementando procesos de transformación digital, enfocados primordialmente a la digitalización de los mecanismos de

comunicación, ya sea con los SO y/o los receptores de información de inteligencia financiera. En este sentido, el haber implementado dichas tecnologías con antelación a la pandemia proporcionó una importante plataforma que permitió que, especialmente, las actividades asociadas a la recepción de información, no se vieran impactadas de forma traumática. De igual forma, aquellas UIF que habían digitalizado los mecanismos de difusión de información reforzaron la continuidad de operaciones en lo que respecta a comunicación con receptores autorizados.

b. Las UIF realizaron importantes ajustes a sus procesos internos con el fin de permitir que sus actividades se vieran impactadas lo menor posible. A este respecto, la mayor preocupación era el contar con mecanismos que aseguraran la protección y confidencialidad de la información, particularmente, en lo que respecta a acceso a bases de datos misionales y conexiones seguras remotas.
c. Dependiendo de las acciones diseñadas, se permitieron mayores o menores grados de conectividad remota de funcionarios de la UIF. En general, en aquellas UIF donde se presentaron mayores restricciones de acceso, estas tenían que ver con las actividades relacionadas con inteligencia financiera, como lo son la lectura y clasificación de ROS y el desarrollo de casos de inteligencia financiera.
d. Las tecnologías más ampliamente utilizadas por las UIF son: uso de conexiones seguras a través de VPN y accesos remotos a través de máquinas virtuales a los entornos de trabajo.
e. Algunas UIF desplegaron medidas adicionales de seguridad, tales como la realización de pruebas poligráficas a funcionarios con acceso remoto u otorgar acceso remoto a quienes hubieran aprobado pruebas poligráficas recientemente; mecanismos de autenticación fuertes de usuarios (token, firma digital, etc.), diseñó de procedimientos para intercambio de información en entornos no presenciales
f. Varias UIF implementaron estrategias de capacitación de funcionarios, en temáticas variadas, algunas de ellas asociadas a concientización y medidas de protección de ataques cibernéticos. De igual forma, se presentaron inquietudes relativas a la correcta disposición de seguridad en el trabajo de los entornos remotos de los funcionarios y seguimiento de variables asociadas al bienestar y manejo de estrés de los mismos e incluso, ajustes a los sistemas de evaluación de personal.
g. Se diseñaron diversas estrategias de comunicación permanente con los SO, variando en alcance y profundidad. Desde boletines informativos hasta la retroalimentación constante a las entidades reportantes indicando tipologías y señales de alerta identificadas con el objetivo de apoyar los procesos de

identificación de operaciones sospechosas a tendencias delictivas durante la pandemia.

h. La oportunidad de expandir la oferta de capacitación a SO por medio del uso de webminars e elearning.

259. Dentro de las principales oportunidades de mejora y fortalecimiento de las capacidades de continuidad de operaciones de las UIF se encuentran:

a. Designar un equipo con claras responsabilidades en términos del diseño e implementación del PCN.

b. Contar con copias offsite del PCN con el objetivo que, ante un evento de interrupción abrupta, se cuente con acceso a los mecanismos de recuperación debidamente documentados.

c. El contar con un centro alterno de datos potencia las capacidades de respuesta de la UIF ante situaciones adversas.

d. El formalizar un Plan de Manejo de Crisis, en el cual se implementen tácticas de comunicación específicas ante las partes con las que interactúa y que durante el transcurso de la crisis se tomen decisiones estratégicas para reducir su impacto, configura un elemento complementario valioso al PCN. En este sentido, en las entrevistas no estructuradas llevadas a cabo con diversas UIF de la región, se encontró que todas desplegaron estrategias de comunicación con sus partes de interés, con el objetivo de informar diversos aspectos asociados a las medidas que se iban implementando a raíz de la crisis provocada por el Covid-19.

e. El implementar estratégicas de retención y transferencia de conocimiento puede llegar a ser de una importancia crítica en una UIF debido a que una proporción importante del conocimiento necesario para el desarrollo de las labores, en particular en análisis operativo y estratégico, es adquirido por el personal a través de la experiencia en la propia UIF.

f. Contar con Sistemas de Gestión de Información y Eventos de Ciberseguridad – SIEM, y con un Centro de Operaciones de Seguridad (SOC), así como la ampliación de la adopción de Sistemas de Gestión de Seguridad de la información (ISMS) basados en una norma/estándar internacional, pueden apoyar de forma importante los esfuerzos de continuidad de operaciones de las UIF.

260. En el análisis de riesgos y BIA, se identificaron como principales amenazas las relativas a cinco (5) contextos: i. desastres naturales; ii. ataques informáticos; iii. fallos tecnológicos; iv. errores internos no intencionales; v. problemas sociales y de salud pública.

261. Asimismo, se proponen escalas de valoración en probabilidad e impacto para evaluar las amenazas a la continuidad de las operaciones de las UIF y se realiza una valoración en términos inherentes en dichas dimensiones, así como una propuesta de potenciales controles a implementar con el objetivo de determinar el nivel de riesgo residual. De esta forma, se identificaron como amenazas con nivel inherente extremo los ataques informáticos, los daños tecnológicos y los problemas sociales y de salud pública; como de nivel alto, los desastres naturales y los errores internos no intencionales. En la definición de procesos críticos de las UIF, se identificaron los asociados a las tareas de i. notificación; ii. análisis de información; iii. comunicación de resultados y; iv. actividades de supervisión (para aquellas UIF que desarrollan este aspecto). Se realiza una propuesta de RTO y RPO, donde en general, no se superan las 48 horas. Como última acción en esta sección, se determinaron las prioridades de los servicios críticos, asignándose prioridad alta a la notificación, análisis de información y supervisión; y una prioridad media a los procesos de notificación.

6. RECOMENDACIONES DE CONTINUIDAD DE NEGOCIO EN LAS UIF

262. Teniendo en cuenta los resultados de los procesos de recolección de información, tanto a nivel de encuestas como con las entrevistas realizadas, y en concordancia con los procesos críticos de las UIF identificados, asociadas al PCN, esta sección presenta las principales recomendaciones relativas al aseguramiento de continuidad de operaciones en una UIF. Estas recomendaciones incluyen las estrategias, medidas de seguridad y herramientas de implementación. Cabe anotar que se también como insumo estrategias que están siendo implementadas por otras UIF y que pueden entenderse como buenas prácticas de negocio.

263. Las siguientes recomendaciones están orientadas a que las UIF puedan reaccionar y continuar con sus actividades misionales en caso de presentarse algún incidente que provoque la interrupción de los servicios críticos de la organización, incluyendo circunstancias tales como la Pandemia por COVID-19.

264. Para ello, es importante que las siguientes recomendaciones puedan estar incluidas dentro del PCN de la organización y que se establezcan los escenarios y estrategias para que los funcionarios puedan acceder a sus herramientas de trabajo desde cualquier ubicación, de forma segura y con todas las especificaciones tecnológicas y administrativas que requieren para cumplir sus objetivos misionales.

265. De acuerdo con el diagnóstico e información recolectada sobre la situación actual de las UIF, el análisis de riesgo y el BIA se procedió a identificar aquellas acciones recomendadas para procurar la continuidad de las operaciones críticas de las UIF durante eventos de contingencia.

6.1. Escenarios de interrupción

266. Los escenarios de desastre, incidente, interrupción mayor o un evento contingente que se recomienda contemplar en el PCN son:

a. Cualquier incidente externo o interno que pudiera potencialmente causar una interrupción de las operaciones del negocio, tales como la pérdida de los servicios de suministro eléctrico o de telecomunicaciones.
b. Cualquier incidente externo o interno que impida el acceso a sistemas de información y, bases de datos.
c. Cualquier incidente que afecte al funcionamiento del hardware o del software y que suponga una interrupción superior a las 24 horas.
d. Cualquier incidente interno que pudiera potencialmente causar o afectar la interrupción de las operaciones de los sistemas de información, como son la falla en los servidores o puntos de conexión.
e. Cualquier incidente que suponga la paralización de actividades de la organización por motivos ajenos a la tecnología, tales como problemas laborales propios o del sector o problemas laborales que afecten al área geográfica donde se encuentra ubicada la organización.
f. Incidentes que causen un daño físico en las instalaciones o equipos, como fuego, humo o daños por agua.
g. Eventos que afecten de forma indirecta la posibilidad de acceso a las instalaciones, como evacuación de emergencia por amenaza terrorista, o amenazas externas tales como incendios en instalaciones cercanas, fuga de gases tóxicos, etc.
h. Desastres regionales no previstos o inesperados, que puedan causar daños en las instalaciones y equipos e impedir el acceso normal al personal encargado o quien haga sus funciones de las operaciones informáticas, aunque las instalaciones estén intactas, tales como inundaciones, huracanes etc.
i. Eventos que afecten la salud pública y que puedan impedir el acceso normal de funcionarios a las instalaciones de la organización, tales como pandemias.

6.2. Tipos de contingencia

267. Las estrategias y acciones para seguir dependerán del tipo de contingencia que se presente:

a. **Menor**: Afecta alguno de los sistemas críticos definidos y podrá ser subsanada o corregida rápidamente por medio de los mecanismos de diagnóstico y reparación

de fallas, activando los procedimientos de atención de incidentes utilizados día a día por la organización.

b. **Mayor**: Afecta varios o la totalidad de servicios críticos definidos e interrumpe la operación normal de la organización, se declarará desastre y se activaran los planes de acción para la recuperación inmediata de los servicios críticos, de acuerdo con las estrategias definidas.

6.3. Estrategias de Continuidad de Negocio

268. En caso de materialización de alguno de los escenarios de interrupción descritos anteriormente y dependiendo del tipo de desastre presentado, las estrategias recomendadas para las UIF, en función de los servicios críticos afectados, son los siguientes:

269. Proceso de notificación: Durante este proceso se debe asegurar la disponibilidad de las aplicaciones mediante las cuales se reciben los reportes, tanto objetivos como de operaciones sospechosas, por parte de los obligados, manteniendo la misma confidencialidad e integridad de los datos reportados.

Tabla 10 – Estrategias de continuidad de negocio. Proceso de notificación

PROCESO DE NOTIFICACIÓN		
Estrategias	**Medidas de seguridad**	**Herramientas de implementación**
Aplicaciones de acceso público o en la nube, que permitan al SO realizar la entrega de información y que garanticen la autenticidad del SO y trazabilidad de la información entregada.	Las aplicaciones públicas o en la nube para recepción de información, deben permitir al reportante auto gestionar todo el proceso de entrega de información y a nivel de seguridad contar mínimo con un canal seguro de comunicación que permita que la información viaje cifrada y con un mecanismo de autenticación multifactor para validar la identidad del SO.	Para garantizar la comunicación segura de las aplicaciones públicas o en la nube, se debe implementar un certificado de servidor seguro SSL/TLS. Para la autenticación multifactor, se pueden emplear distintos métodos como: token de seguridad o una contraseña única basada en tiempo TOTP.

Acceso remoto seguro a las aplicaciones requeridas por los funcionarios encargados de recibir y tramitar la información entregada en otros medios por parte de los SO.	Es necesario que los funcionarios que requieran acceder a los sistemas de información para el cargue de reportes, utilicen una conexión segura VPN e igualmente cuenten con un mecanismo de doble autenticación para validar su identidad.	Para la creación de VPNs de acceso remoto, se requiere de la infraestructura tecnológica para su gestión, comúnmente los productos de seguridad como cortafuegos incluyen esta característica.
Procedimiento seguro de recepción de información recibida en medio físico y entrega para el trámite del responsable.	El acceso a los repositorios de documentos de trabajo deberá realizarse a través de VPN únicamente, deberán estar alojados en un sistema de almacenamiento centralizado administrado por perfiles y usuarios y si es posible, se debe restringir la salida de información de la red interna de la organización.	Para el almacenamiento de información, se recomienda contar con infraestructura tipo SAN o NAS y controlar su acceso y uso mediante políticas de dominio. Para evitar temas de fuga de información, si es posible implementar una solución de prevención de perdida de información DLP.
Entrega de computadores en préstamo para los funcionarios que lo requieran.	Establecer un protocolo de préstamo de computadores a empleados, con controles de seguridad para la entrega, el uso y devolución.	Para el préstamo de computadores se recomienda realizar copia de seguridad del equipo antes de su salida, instalar un software de cifrado de disco y antimalware, si es posible implementar una solución de prevención de perdida de información DLP o en su defecto inhabilitar puertos USB u otro medio que sirva para la copia de información.

Copias de seguridad para salvaguardar la información enviada por los SO.	Implementar un procedimiento de copias de seguridad que garantice una periodicidad y tiempo de retención conforme al RPO definido y que repose fuera de las instalaciones principales de la UIF.	Contar con copias offsite con el objetivo que, ante un evento de interrupción abrupta, se cuente con acceso a los mecanismos de recuperación de los sistemas de información para la recepción de reportes.
Centro Alterno de Datos para el respaldo de las aplicaciones y datos de los sistemas de información para la recepción de reportes.	Aprovisionar la infraestructura requerida para respaldar las principales aplicaciones y datos de la UIF, que cuente con redundancia de datos, acceso seguro, capacidades distribuidas y balanceo de canales para garantizar la disponibilidad de la operación.	Contar con un sitio alterno en ubicación segura o en nube para fortalecer las capacidades de respuesta de la UIF ante situaciones adversas que afecten los sistemas de información para la recepción de reportes.

270. Proceso de análisis de información: Durante este proceso, se debe garantizar que los analistas de información tengan acceso a las herramientas y datos necesarios para realizar su labor de forma remota, manteniendo la confidencialidad e integridad de la información de la organización. Este proceso de análisis de información aplica tanto al análisis operativo como estratégico. De igual forma, estas estrategias pueden ser utilizadas en los procesos de supervisión que lleven a cabo las UIF.

Tabla 11 – Estrategias de continuidad de negocio. Proceso de análisis de información

PROCESO DE ANÁLISIS DE INFORMACIÓN		
Estrategias	**Medidas de seguridad**	**Herramientas de implementación**
Acceso remoto seguro a las aplicaciones y documentos requeridos por los funcionarios analistas de información para realizar adecuadamente su labor.	Es necesario que los funcionarios que requieran acceder a los sistemas de información misionales utilicen una conexión segura VPN e igualmente cuenten con un mecanismo de doble autenticación para validar su identidad.	Para la creación de VPNs de acceso remoto, se requiere de la infraestructura tecnológica para su gestión, comúnmente los productos de seguridad como cortafuegos incluyen esta característica.

	Realizar pruebas de confiabilidad de funcionarios antes de la autorización de acceso remoto.	
Autenticación multifactor para validar la identidad del analista, especialmente cuando acceda a sistemas con información sensible o confidencial.	El acceso a los repositorios de documentos de trabajo deberá realizarse a través de VPN únicamente, deberán estar alojados en un sistema de almacenamiento centralizado administrado por perfiles y usuarios y si es posible, se debe restringir la salida de información de la red interna de la organización.	Para la autenticación multifactor, se pueden emplear distintos métodos como: token de seguridad o una contraseña única basada en tiempo TOTP.
Mecanismos de seguridad para monitorear y controlar el acceso, uso y difusión de la información sensible gestionada por los analistas de información	Contar con sistemas de monitoreo, que permitan la visibilidad, auditoria y trazabilidad de las actividades de los analistas de información.	Para el almacenamiento de información, se recomienda contar con infraestructura tipo SAN o NAS y controlar su acceso y uso mediante políticas de dominio. Para evitar temas de fuga de información, si es posible implementar una solución de prevención de perdida de información DLP. Para el monitoreo de las actividades de los usuarios, se recomienda la implementación de un sistema de Gestión de información y eventos de seguridad SIEM y si es posible contar con un Centro de Operaciones de Seguridad (SOC).

Entrega de computadores en préstamo para los funcionarios que lo requieran.	Establecer un protocolo de préstamo de computadores a empleados, con controles de seguridad para la entrega, el uso y devolución.	Para el préstamo de computadores se recomienda realizar copia de seguridad del equipo antes de su salida, instalarles un software de cifrado de disco y antimalware, si es posible implementar una solución de prevención de perdida de información DLP o en su defecto inhabilitar puertos USBs u otro medio que sirva para la copia de información.
Copias de seguridad para salvaguardar la información sensible gestionada por los analistas de información.	Implementar un procedimiento de copias de seguridad que garantice una periodicidad y tiempo de retención conforme al RPO definido y que repose fuera de las instalaciones principales de la UIF.	Contar con copias offsite con el objetivo que, ante un evento de interrupción abrupta, se cuente con acceso a los mecanismos de recuperación de los sistemas de información para la gestión de los analistas de información.
Centro Alterno de Datos para el respaldo de las aplicaciones y datos de los sistemas de información para la labor de los analistas de información.	Aprovisionar la infraestructura requerida para respaldar las principales aplicaciones y datos de la UIF, que cuente con redundancia de datos, acceso seguro, capacidades distribuidas y balanceo de canales para garantizar la disponibilidad de la operación.	Contar con un sitio alterno en ubicación segura o en nube para fortalecer las capacidades de respuesta de la UIF ante situaciones adversas que afecten los sistemas de información sensible gestionada por los analistas de información.

271. Proceso de comunicación: Durante este proceso se debe garantizar que la comunicación y difusión de los casos e informes respectivos, se realice de forma segura a los receptores competentes, utilizando medio digitales, pero manteniendo la confidencialidad e integridad de la información.

Tabla 12 – Estrategias de continuidad de negocio. Proceso de comunicación de información

PROCESO DE COMUNICACIÓN		
Estrategias	**Medidas de seguridad**	**Herramientas de implementación**
Establecer un protocolo seguro para la entrega de informes de casos a las autoridades competentes.	Implementar un protocolo seguro de común acuerdo con las autoridades competentes, en donde se controle quien envía, quien recibe y la trazabilidad de la entrega a través de medios digitales.	Comunicaciones cifradas, e-mail firmado digitalmente, herramientas de software de cifrado de archivos y documentos.
Utilizar medios digitales para la entrega de informes de casos y otra información, garantizando la identidad del emisor y receptor, la confidencialidad e integridad de los archivos comunicados.	Utilizar mecanismos de firma digital para remitir los informes de casos de forma segura y confidencial.	Se deben adquirir firmas digitales para aquellos funcionarios autorizados a remitir los informes de casos a las autoridades competentes, estas firmas son suministradas por entidades certificadoras oficiales en cada país y se utilizan para firmar digitalmente un archivo y comprobar su validez.
Copias de seguridad para salvaguardar la información sensible sobre los casos entregados a las autoridades competentes.	Implementar un procedimiento de copias de seguridad que garantice una periodicidad y tiempo de retención conforme al RPO definido y que repose fuera de las instalaciones principales de la UIF.	Contar con copias offsite con el objetivo que, ante un evento de interrupción abrupta, se cuente con acceso a los mecanismos de recuperación de la información sensible sobre los casos entregados a las autoridades competentes.

BIBLIOGRAFIA

Deloitte. (2018). Apetito de Riesgo. Ajustando los riesgos a nuestra medida. Disponible en https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/2018/3.Apetito-al-Riesgo.pdf

COSO (2012). Compliance risk management. Applying the COSO ERM Enterprise Risk Management. Enterprise risk management. Understanding and Communicating Risk Appetite. Disponible en https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf

COSO (2020). Compliance risk management. Applying the COSO ERM Enterprise Risk Management, Disponible en https://www.coso.org/Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

Egmont (2014). Annual Report 2012 – 2013.

Egmont (2014). Proceso de Apoyo y Cumplimiento.

Egmont Group (2018). Entendiendo la Independencia Operativa y autonomía de las UIF. https://egmontgroup.org/en/filedepot_download/1661/101

Egmont (2018). Entendiendo la Independencia Operativa y Autonomía de las UIF. Resumen Ejecutivo. https://egmontgroup.org/en/filedepot_download/1661/107

FATF (2018). Professional Money Laundering.

FMI (2004). Unidades de Inteligencia Financiera. Panorama General

Foro Económico Mundial (2019). Informe de Riesgos Mundial, 2019.

GAFILAT (2019). Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva. Disponible en https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/3857-recomendaciones-metodologia-actdec19-1/file

GAFILAT (2020). Comunicado del GAFILAT sobre COVID-19 – Coronavirus. 8 de abril de 2020. https://gafilat.org/index.php/es/espanol/19-noticias/102-comunicado-del-gafilat-sobre-Covid-19-coronavirus

Gilmore, W. (1999). Dirty Money: The Evolution Of Money-Laundering Counter-Measures, segunda edición. (Estrasburgo: Council of Europe Press).

Grupo Egmont (1995). The First International Meeting of Organizations Devoted to Anti-Money Laundering (Bruselas).

INCIBE. (2020). Obtenido de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Instituto de autodores interno de España. Definición e implementación del apetito de riesgo.

ISACA. Cybersecurity Fundamentals.

ISO 22301. (2019). *Sistema de Gestión de Continuidad de Negocio*

ISO 27001 (2018). Tecnología de información. Técnicas de seguridad, sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

ISO 31000. (2018). Gestión de Riesgo - Directrices

ISO 31010. (2018). Técnicas de valoración de riesgo.

ISO Guía 73. (2009). Gestión de riesgos. Terminología.

Ministerio de las Tecnologías de Información - Colombia. MINTIC. (2010). *Guía para la preparación de las TIC para la continuidad del negocio*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

Riesgos Cero. (2020). Obtenido de https://www.riesgoscero.com/academia/especiales/guia-para-gestionar-un-plan-de-continuidad-de-negocio-segun-la-iso-22301

Transparencia Internacional (2019). Financial intelligence units (FIUs): Effective institutional design,

UIAF (2014). Introducción al marco jurídico y estándares internacionales antilavado de activos y contra la financiación del terrorismo.

UIAF (2014). Lo que debe saber del lavado de activos y la financiación al terrorismo.