GAFILAT

DIAGNÓSTICO REGIONAL DE CIBERSEGURIDAD

APLICADO A LAS UNIDADES DE INTELIGENCIA FINANCIERA (UIF) DE LOS PAÍSES DEL GAFILAT

DICIEMBRE 2025

Presidencia *pro-tempore* Guatemala 2025

www.gafilat.org

El GAFILAT agradece el apoyo brindado por la Superintendencia de Bancos de Guatemala en el diseño, la diagramación y corrección de estilo del presente documento. El contenido de esta publicación es completa responsabilidad del Grupo de Acción Financiera de Latinoamérica (GAFILAT).

I. ÍNDICE

II. ACRÓNIMOS Y SIGLAS

ALA ..... Antilavado de activos
CFT ..... Contra el financiamiento del terrorismo
CSF ..... *Cyber Security Framework* (Marco de Ciberseguridad)
ISO ..... *International Organization for Standardization* (Organización Internacional de Normalización)
GAFILAT ..... Grupo de Acción Financiera de Latinoamérica
NIST ..... *National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología)
UIF ..... Unidad de Inteligencia Financiera
TPRM ..... *Third Party Risk Management* (Gestión de Riesgo de Terceros)
KPI ..... *Key Performance Indicators* (Indicador Clave de Desempeño)

III. INTRODUCCIÓN

Los ataques cibernéticos constituyen una amenaza en constante crecimiento que ha adquirido dimensiones preocupantes a nivel global y regional. Su impacto puede ser devastador para los particulares, las organizaciones y, especialmente, para los sistemas financieros de los países, al ocasionar pérdidas económicas significativas y comprometer la integridad, disponibilidad y confidencialidad de la información. En el caso de las Unidades de Inteligencia Financiera (UIF), el riesgo es aún mayor, pues un ataque exitoso podría afectar directamente la seguridad nacional y socavar los esfuerzos colectivos de prevención y combate del lavado de activos y del financiamiento del terrorismo.

La Tercera Actualización del Informe de Amenazas Regionales en materia de Lavado de Activos 2019–2021 (Grupo de Acción Financiera de Latinoamérica, 2022), identificó un incremento relevante de las actividades de cibercrimen, como el *phishing* y el *vishing*, dentro de las tipologías de estafa y fraude, ocupando el séptimo lugar entre las amenazas regionales. En el período 2022–2023 (Grupo de Acción Financiera de Latinoamérica, 2024), esta amenaza ascendió a la cuarta posición, lo que evidencia una tendencia sostenida al alza que demanda atención prioritaria por parte de los países miembros.

De acuerdo con el *Allianz Risk Barometer 2025 (Allianz Commercial, 2025),* una encuesta anual realizada entre más de 3.700 expertos en gestión de riesgos de 106 países, los incidentes cibernéticos se posicionan, por tercer año consecutivo, como el riesgo número uno a nivel mundial, con un 38 % de las respuestas, siete puntos porcentuales más que en la edición anterior. El estudio resalta que esta amenaza domina en todos los continentes y se mantiene como la principal preocupación en más de 20 países, evidenciando que la exposición a ataques cibernéticos se ha convertido en un factor transversal que impacta la estabilidad operativa y reputacional de las organizaciones. Además, el barómetro subraya que los riesgos cibernéticos están estrechamente vinculados con otros grandes riesgos corporativos, como la interrupción del negocio, la gestión de datos sensibles y la dependencia tecnológica, lo que exige un enfoque estratégico e integral de resiliencia.

En este contexto, las Recomendaciones del Grupo de Acción Financiera Internacional (GAFI), (especialmente aquellas relacionadas con las funciones de las UIF, la protección de la información financiera y el intercambio seguro de datos), subrayan la importancia de que las instituciones cuenten con sistemas tecnológicos sólidos y confiables que aseguren la confidencialidad, integridad y disponibilidad de la información que gestionan. La protección de los reportes de operaciones sospechosas, el acceso seguro a bases de datos sensibles y la garantía de canales de intercambio de información rápidos y seguros con contrapartes nacionales e internacionales constituyen obligaciones esenciales para el cumplimiento de los estándares internacionales. Por ello, el fortalecimiento de la resiliencia cibernética de las UIF no solo responde a una necesidad operativa, sino que es también un aspecto relevante para la efectiva implementación de las Recomendaciones del GAFI.

Ante este panorama, la Presidencia *Pro Tempore* del GAFILAT identificó la necesidad de fortalecer la resiliencia cibernética de las UIF, reconociendo que la protección de la información que estas manejan es esencial para salvaguardar la confidencialidad de la inteligencia financiera. La exposición de datos sensibles o su acceso por actores maliciosos podría tener consecuencias graves, tanto a nivel operativo como estratégico, afectando la confianza y la cooperación internacional.

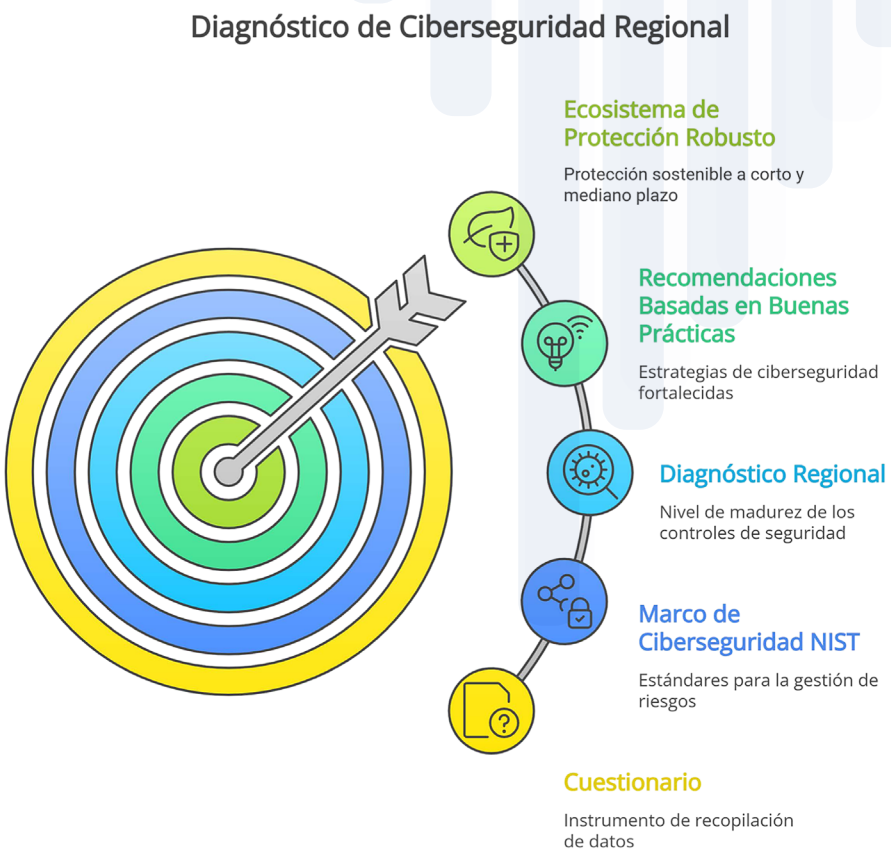
En ese sentido, la Presidencia impulsó por primera vez en el foro del GAFILAT una iniciativa específica sobre ciberseguridad para las UIF, orientada a promover la preparación, prevención y recuperación ante posibles incidentes. Este esfuerzo representa un paso inicial hacia un objetivo más amplio: extender progresivamente las capacidades de ciberseguridad a las autoridades competentes y a los sujetos obligados, fortaleciendo de manera integral la infraestructura de protección y respuesta del sistema Antilavado de Activos y Contra el Financiamiento del Terrorismo (ALA/CFT) en la región.

IV. OBJETIVO

La Presidencia *Pro Tempore* del GAFILAT, estableció en su Plan de Acción 2025 un eje dedicado a la ciberseguridad, con el objetivo de proporcionar herramientas a las UIF para prevenir y evitar ser víctimas de ataques cibernéticos en sus infraestructuras, y proteger sus sistemas e información. Asimismo, se planteó como objetivo general realizar un estudio que permita visualizar las buenas prácticas y avances en materia de prevención de ataques de esta índole en un plano regional.

El primer objetivo específico de este informe es contar con un diagnóstico regional de implementación de medidas de ciberseguridad en las UIF del GAFILAT, que permita establecer el nivel de madurez de los controles de seguridad con base a la información obtenida del instrumento utilizado (cuestionario), aplicando uno de los marcos de ciberseguridad de mayor aceptación, desarrollado desde el año 2013 en su primera versión y recientemente actualizado en su versión 2.0 por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de los Estados Unidos de América, quien lleva más de un siglo emitiendo estándares técnicos y científicos para que sean aplicados en entidades gubernamentales y privadas con interés en la gestión de riesgos derivados de amenazas cibernéticas, sobre lo cual se desarrolla el presente informe.

Así también, a partir de los resultados del diagnóstico, deriva el segundo objetivo específico dirigido a formular recomendaciones basadas en buenas prácticas estándar, que sirvan como una herramienta de apoyo para fortalecer las estrategias o políticas de ciberseguridad de las UIF de la región, contribuyendo al desarrollo de un ecosistema de protección más robusto y sostenible a corto y mediano plazo, en función de las capacidades y recursos disponibles en cada jurisdicción.



V. METODOLOGÍA

A. RECOPILACIÓN DE LA INFORMACIÓN

Para la elaboración del presente diagnóstico, se formuló un cuestionario de 41 preguntas agrupadas en tres secciones, con opciones de respuesta de selección múltiple y texto abierto, diseñado en la herramienta de *Microsoft Forms*, el cual fue remitido a los 18 países miembros del GAFILAT, para ser completado por funcionarios apropiados de las UIF participantes.

Se obtuvo insumos de 12 de los 18 países miembros, siendo estos: Bolivia, Chile, Colombia, Ecuador, El Salvador, Guatemala, Nicaragua, Panamá, Paraguay, Perú, República Dominicana y Uruguay.

La primera sección del diagnóstico se dirigió a conocer el perfil institucional de la UIF; la segunda, consistió en una autoevaluación para que cada UIF la realizara bajo la escala de madurez NIST según los parámetros indicados; y, la última sección tenía el propósito de conocer si la UIF deseaba formar parte de la red de expertos en tecnología de la información o ciberseguridad regional para compartir experiencias o casos sobre amenazas de ciberseguridad identificadas, y de ser afirmativo el caso, recabar los datos de contacto.

B. MARCO DE CIBERSEGURIDAD DEL NIST

Como parte de la metodología aplicada para realizar el diagnóstico y emitir las recomendaciones, se utilizó el Marco de Ciberseguridad del NIST *(National Institute of Standards and Technology, 2025)* en su versión 2.0, internacionalmente reconocido por su aplicabilidad a todo tipo de instituciones y por su alineación con mejores prácticas certificables (por ejemplo, ISO 27001:2022). El NIST pone a disposición gratuitamente guías, herramientas y documentación que permiten a cualquier entidad interesada fortalecer su postura de ciberseguridad, gestionar el apetito de riesgo derivado del uso de tecnologías y hacer frente al panorama creciente de amenazas cibernéticas.

El Marco de Ciberseguridad *("Cybersecurity Framework", CSF)* del NIST versión 2.0 está integrado por 106 requisitos de ciberseguridad (es decir, subcategorías o requerimientos) que toda institución debe procurar cumplir, tomando en cuenta su propio contexto: recursos, procesos, procedimientos, sistemas y redes, dado que cada UIF interactúa con otras entidades y se expone al riesgo de ataques cibernéticos dinámicos. Estos 106 requerimientos están agrupados en 23 categorías (también llamados dominios de acción), asociadas a seis funciones o áreas de focalización de esfuerzos, siendo estas: gobernar, identificar, proteger, detectar, responder y recuperar.

1. ¿Qué es el NIST y por qué es un buen referente?

El NIST es una agencia estadounidense dedicada a desarrollar estándares, directrices y buenas prácticas, incluida la seguridad de la información. El CSF del NIST fue concebido para ayudar a las organizaciones a comprender, gestionar y reducir los riesgos de ciberseguridad de forma sistemática.

La versión 2.0 del CSF amplía su cobertura, adopta un lenguaje más universal, incluye el nuevo componente de gobernanza y está diseñada para todo tipo de organizaciones (independientemente de su tamaño o sector) que busquen fortalecer su resiliencia frente a ciberamenazas.

Para una UIF que actúa en el ecosistema regional ALA/CFT, como es el caso del Grupo de Acción Financiera de Latinoamérica (GAFILAT), y aún en un plano internacional en cooperación con contrapartes de otras regiones, este marco ofrece una estructura robusta, reconocida internacionalmente, que posibilita la comparación de su postura de ciberseguridad, la identificación de brechas, la priorización de acciones y la construcción de un plan de mejoras alineado con estándares globales.

2. Las funciones del marco y su relevancia

Las seis funciones del CSF 2.0 establecen un ciclo completo de gestión del riesgo de ciberseguridad:

FUNCIÓN	DESCRIPCIÓN
Gobernar	**Función estratégica introducida en la versión 2.0, que exige que la organización defina claramente roles, responsables, estrategias, políticas, apetito de riesgo cibernético, y que se integre la ciberseguridad dentro de la gobernanza corporativa y de riesgo global.** La estrategia, expectativas y política de gestión de riesgos de ciberseguridad de las UIF se establecen, se comunican y se supervisan. La función gobernar proporciona resultados que informan sobre las medidas que las unidades pueden tomar para lograr y priorizar los resultados de las otras cinco funciones en el contexto de su misión y las expectativas de las partes interesadas. Las actividades de gobernanza son fundamentales para incorporar la ciberseguridad en la estrategia general de gestión de riesgos de las unidades. Gobernar aborda la comprensión del contexto organizacional; el establecimiento de la estrategia de ciberseguridad y la gestión de riesgos de la cadena de suministro de ciberseguridad; los roles, las responsabilidades y las autoridades; la política; y la supervisión de la estrategia de ciberseguridad.
Identificar	**Comprender el negocio, los activos, los riesgos, y establecer el contexto para gestionar el riesgo de ciberseguridad.** Se comprenden los riesgos actuales de ciberseguridad de las unidades, los activos de las UIF (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios, personal), los proveedores y los riesgos de ciberseguridad relacionados permite a las unidades priorizar sus esfuerzos de acuerdo con su estrategia de gestión de riesgos y las necesidades de la misión identificadas en gobernar. Esta función también incluye la identificación de oportunidades de mejora para las políticas, planes, procesos, procedimientos y prácticas de la organización que respaldan la gestión de riesgos de ciberseguridad, con el fin de fundamentar las iniciativas de las seis funciones.
Proteger	**Implementar salvaguardias apropiadas para asegurar la entrega de servicios críticos, incluyendo políticas, formación, controles de acceso, tecnología de protección, entre otros.** Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de las UIF. Una vez identificados y priorizados los activos y riesgos, la función proteger facilita la protección de dichos activos para prevenir o reducir la probabilidad y el impacto de eventos adversos de ciberseguridad, así como para aumentar la probabilidad y el impacto de aprovechar las oportunidades. Los resultados que abarca esta función incluyen la gestión de identidades, la autenticación y el control de acceso; la concienciación y la formación; la seguridad de los datos; la seguridad de la plataforma (es decir, la protección del *hardware*, el *software* y los servicios de las plataformas físicas y virtuales); y la resiliencia de la infraestructura tecnológica.
Detectar	**Establecer capacidades para identificar eventos de ciberseguridad de forma oportuna, mediante monitoreo, análisis y procedimientos de alerta.** Se detectan y analizan posibles ataques y vulnerabilidades de ciberseguridad. La función detectar permite el descubrimiento y el análisis oportuno de anomalías, indicadores de vulnerabilidad y otros eventos potencialmente adversos que puedan indicar la ocurrencia de ataques e incidentes de ciberseguridad. Esta función facilita el éxito de las actividades de respuesta y recuperación ante incidentes.

FUNCIÓN	DESCRIPCIÓN
Responder	**Desarrollar e implementar las acciones necesarias cuando se detecta un incidente, para contener su impacto, mitigar consecuencias y comunicar de forma adecuada.** Se toman medidas ante un incidente de ciberseguridad detectado. La función facilita la capacidad de contener los efectos de los incidentes de ciberseguridad. Los resultados de esta función abarcan la gestión, el análisis, la mitigación, la generación de informes y la comunicación de incidentes.
Recuperar	**Restaurar capacidades o servicios afectados por un incidente para volver a la normalidad, y mejorar la resistencia.** Se restauran los activos y las operaciones afectados por un incidente de ciberseguridad. La función recuperar facilita la restauración oportuna de las operaciones normales para reducir los efectos de los incidentes de ciberseguridad y facilitar una comunicación adecuada durante las tareas de recuperación

Tabla 1. Descripción de las funciones de NIST versión 2.0

Para una UIF, cada una de estas funciones adquiere relevancia particular, por ejemplo, la función de gobernar asegura que la confidencialidad de la inteligencia financiera esté respaldada por políticas institucionales; la función de detectar permite identificar rápidamente accesos no autorizados o anomalías; la función de Recuperar asegura que, ante un incidente, los sistemas críticos vuelvan a operar y la cooperación regional no se vea interrumpida.

3. Niveles de madurez y escala de riesgos

El CSF 2.0 define los niveles de implementación para evaluar qué tan madura es la gestión del riesgo de ciberseguridad en la organización. Para una mejor comprensión de la escala de nivel de madurez, descritos a continuación:

Nivel de madurez	Descripción
1 - Inexistente	No hay conciencia ni procesos formales de ciberseguridad. Los riesgos no se identifican ni gestionan. Ejemplo: un área de la unidad almacena datos sensibles sin cifrado y sin políticas de acceso.
2 - Inicial	Los controles son reactivos y dependen de acciones individuales (Ejemplo: un empleado resuelve un incidente de *phishing* sin protocolos). No hay documentación ni métricas.
3 - Repetible	Existen prácticas informales basadas en experiencias pasadas (Ejemplo: se aplican parches de seguridad, pero sin un calendario fijo). Falta estandarización y supervisión de la dirección.
4 - Definido	Los procesos están documentados y alineados a marcos como ISO 27001 o NIST (Ejemplo: la unidad tiene un protocolo de respuesta a incidentes y realiza auditorías anuales de cumplimiento).

Nivel de madurez	Descripción
5 - Administrado	Se usan métricas para monitorear riesgos (Ejemplo: tiempo de detección de amenazas, tasa de fraudes bloqueados). La alta dirección recibe reportes periódicos.
6 - Optimizado	La ciberseguridad se integra con la estrategia del negocio. Uso de IA/ML para predicción de amenazas y mejora continua (Ejemplo: análisis automatizado de transacciones fraudulentas en tiempo real).
7 - No Aplicable	El objetivo de control no se aplica al área que se está evaluando.

Tabla 2. Descripción de los Nivel de Madurez de NIST versión 2.0 utilizado en el cuestionario compartido.

En cuanto a la escala de riesgos, el marco ayuda a una institución a alinear la evaluación de sus activos, amenazas, vulnerabilidades, impacto y probabilidad, permitiendo definir su apetito de riesgo, establecer tolerancias, priorizar acciones. A continuación, se describe la escala de niveles de riesgo:

Riesgo	DESCRIPCIÓN
Muy Alto	Prácticamente se está expuesto a múltiples amenazas debido a que, o no existen controles, o no son los adecuados o carecen de fortaleza, por consiguiente, el riesgo es crítico ya que el no tomar acciones e implementar controles adecuados pudiera representar para la institución la paralización total o parcial de las operaciones, pérdidas económicas importantes o daños a la reputación.
Alto	La ocurrencia efectiva de ciertas amenazas pudiera representar pérdidas económicas significativas o una paralización de operaciones en servicios claves. Lo anterior debido a que los controles existentes no están totalmente ajustados.
Medio	Se está expuesto a ciertas amenazas ya que aún falta la implementación de algunos controles y entonación apropiada de los mismos, pudiendo representar trabajos adicionales debido a daños ocasionados a ciertos procesos puntuales.
Bajo	Se está poco expuesto a amenazas debido a que existen controles adecuados y bien implementados. Si ocurriera una amenaza, el daño para la institución se pudiera aceptar ya que existe la posibilidad de recuperación mediante una baja inversión de recursos.
Muy Bajo	Prácticamente no se está expuesto a amenazas ya que los controles están bien implementados y con un alto nivel de madurez. Si ocurre una amenaza el grado del daño es despreciable.

Tabla 3. Descripción de los niveles de riesgo en el CSF NIST.

4. Aplicación del CSF en el diagnóstico

La adopción del NIST CSF 2.0 en el diagnóstico de las UIF de la región permite lo siguiente:

- Contar con un lenguaje común y reconocido internacionalmente para evaluar la postura de ciberseguridad.
- Comparar la situación de las UIF frente a un marco escalable y aplicable al sector público/regulatorio.
- Evaluar la madurez institucional (nivel de gobernanza, recursos, procesos, tecnología) y establecer un punto de partida para mejoras progresivas.
- Priorizar las áreas de mayor riesgo (por ejemplo, detección de intrusiones, protección de datos, recuperación ante incidentes) sobre la base del diagnóstico.
- Promover la alineación con estándares certificados como ISO 27001, facilitando la confianza entre las autoridades del sistema ALA/CFT.

En conclusión, el uso del Marco de Ciberseguridad del NIST versión 2.0 como base para el diagnóstico y las recomendaciones, proporciona un enfoque estructurado, estratégico, medible y adaptable, que respalda la necesidad de fortalecer las capacidades de las UIF en la región, garantizar la confidencialidad de la inteligencia financiera y mejorar su resiliencia ante el aumento de las amenazas cibernéticas.

C. DIAGNÓSTICO

Como resultado del análisis sobre el autodiagnóstico realizado por las UIF de los países miembros de GAFILAT que participaron, fue posible identificar preocupaciones similares sobre los ciberincidentes a los que las agencias pudieran verse afectadas, a pesar de que el contexto de las UIF participantes en el diagnóstico sean diferentes en su mayoría.

Se debe tomar en cuenta que, en atención a la naturaleza altamente sensible de la información vinculada con infraestructura tecnológica, capacidades operativas y eventuales deficiencias de seguridad, este diagnóstico no incorpora datos ni descripciones específicas por país, con el fin de resguardar información crítica cuya divulgación podría generar riesgos operativos para las UIF. En consecuencia, el presente documento expone únicamente hallazgos, tendencias y conclusiones de carácter general y regional, suficientes para comprender el nivel de desarrollo y las necesidades comunes en materia de ciberseguridad.

El cuestionario permitió identificar aspectos relevantes para conocer las capacidades de respuesta y gestión de incidentes de ciberseguridad, los cuales se describen a continuación:

- **Naturaleza de las UIF:** once de las doce UIF participantes son de naturaleza administrativa (92%) y una de tipo judicial (8%).

- **Estructura organizacional de la UIF:** con relación a la consulta sobre a que institución se encuentra adscrita la UIF, fue identificado que el valor mayor de similitud es de tres UIF, que están adscritas al Ministerio de Hacienda de su país, seguido de dos que están adscritas a la Superintendencia de Bancos, al igual que dos UIF adscritas a la Presidencia del país.

  Esto permite confirmar que el contexto y riesgos pueden variar, aunque en su mayoría, aplicando la clasificación del Reporte de *Verizon Data Breach Report* 2025, pudieran tomarse en consideración los riesgos de ciberseguridad identificados y materializados del sector público más representativos, siendo los siguientes: el acceso no autorizado por intrusiones a sistemas, y aprovechamiento de errores de configuración en aplicaciones web, que representan el 78% de las 946 brechas de ciberseguridad confirmadas de 1.422 incidentes de ciberseguridad registrados en dicho estudio y del sector financiero, adicional a las amenazas del sector público, se identifican las amenazas de ingeniería social como los más representativos.

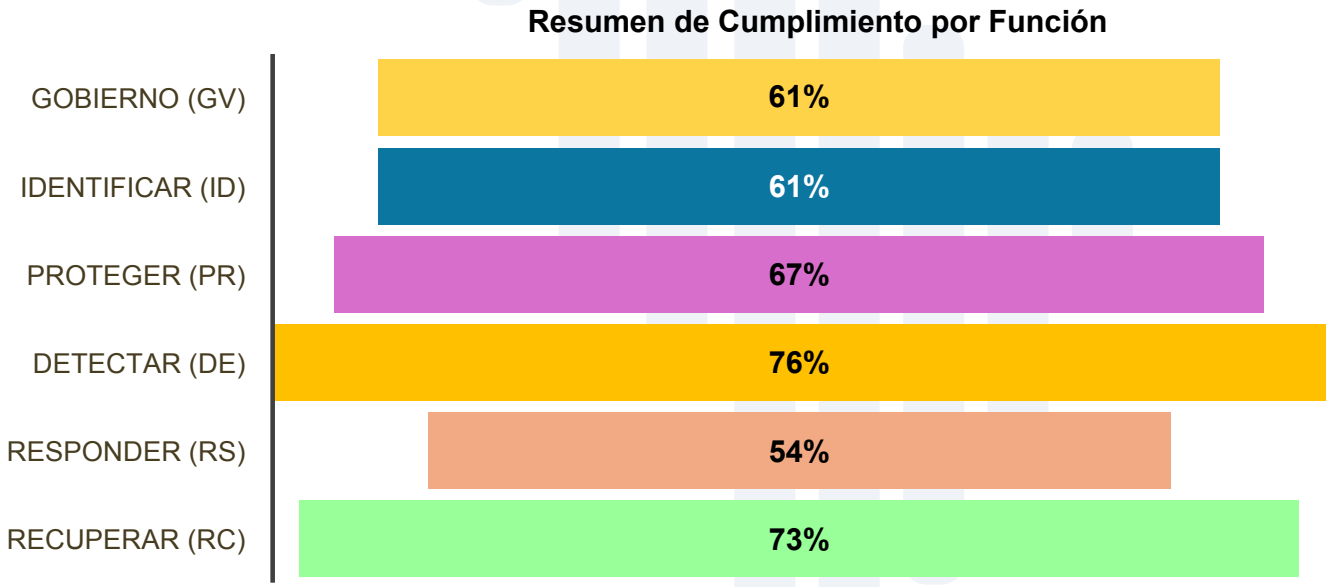
- **Tamaño de las UIF**: en promedio, la cantidad de colaboradores de las UIF que forman parte del GAFILAT es de 85. La UIF más grande está conformada por 159 colaboradores y la más pequeña cuenta con 12 colaboradores.

- **Dependencia de tecnología dedicada**: las doce UIF participantes cuentan con una dependencia de tecnología dedicada, conformada en promedio por 9 colaboradores. La dependencia de tecnología más grande se encuentra conformada por 27 colaboradores y la más pequeña por 2 colaboradores.

- **Personal dedicado para la gestión de amenazas de ciberseguridad**: las doce UIF afirman tener personal dedicado para la gestión de amenazas de ciberseguridad. En promedio existen 2 personas designadas para la gestión de ciber incidentes, determinando que el equipo más grande se encuentra conformado por 5 personas.

- **Infraestructura propia de tecnología para el análisis y resguardo de información**: once de las doce UIF cuentan con infraestructura tecnológica propia y solo una UIF comparte que utiliza infraestructura propia de forma parcial y el uso de servicios de nube.

- **Resumen de cumplimiento de NIST CSF versión 2.0 de las UIF de los países miembros de GAFILAT**: Después del análisis consolidado de información y las respuestas recibidas de autoevaluación, fue posible establecer el nivel de cumplimiento, administrado con el desglose de resultados descritos a continuación y que permiten confirmar que las UIF que participaron en el diagnóstico, manifiestan tener definidos controles que apoyan a cada una de las funciones de NIST y que existen métricas de cumplimiento aplicados a los controles que apoyan a la identificación, protección, detección, respuesta, recuperación y gobernanza aplicables a los sistemas, redes y servicios digitales necesarios para la continuidad del cumplimiento de las funciones de las UIF.



Gráfica 1. Resultados del nivel de cumplimiento de requerimientos de NIST CSF 2.0
Fuente: Informe técnico de diagnóstico emitido por empresa contratada para análisis de resultados.

El resultado compartido permite, de forma general, ubicar recomendaciones que pudieran adoptarse a corto o mediano plazo a fin de mejorar el nivel de cumplimiento a optimizado, siendo este el más alto, así como fortalecer los controles en las áreas más débiles: identificación, respuesta y gobernanza de la gestión de ciberincidentes. A continuación, se presenta un cuadro con los resultados del nivel de madurez asignado por las UIF a las preguntas de la Sección 2 – Autoevaluación conforme a la escala de madurez NIST del cuestionario. Se muestra la nota global por unidad, junto con la calificación total y el promedio obtenido en cada pregunta evaluada, de la cual permitió establecer los porcentajes del nivel de cumplimiento de NIST.

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10	U11	U12	Total
17. ¿La organización ha identificado sus activos críticos?	6	4	6	4	6	4	2	4	6	5	4	4	55
18. ¿Se han evaluado los riesgos de ciberseguridad?	6	3	6	5	6	4	3	6	6	4	4	3	56
19. ¿Existe un plan de respuesta ante incidentes?	6	4	6	4	6	6	4	4	6	4	4	3	57
20. ¿Se realiza monitoreo continuo de seguridad?	6	6	6	5	6	6	5	4	6	5	4	4	63
21. ¿Se capacita al personal en ciberseguridad?	6	3	6	3	6	4	2	1	6	4	4	4	49
22. ¿Se aplican controles de acceso adecuados?	6	4	6	4	6	6	5	5	5	5	4	5	61
23. ¿Se gestionan las vulnerabilidades regularmente?	6	6	6	5	4	6	5	4	6	5	4	3	60
24. ¿Se realiza respaldo periódico de la información?	6	6	6	4	6	6	6	5	6	5	4	3	63
25. ¿Se evalúan proveedores externos en términos de seguridad?	6	3	3	1	4	6	5	2	5	4	3	3	45
26. ¿Se cuenta con políticas de seguridad documentadas?	6	4	6	4	6	5	6	6	6	5	4	4	62
27. ¿Se revisan y actualizan los controles de seguridad?	6	5	6	5	6	5	2	5	6	5	4	4	59
28. ¿Se realiza análisis forense tras incidentes?	6	4	4	2	4	6	3	1	3	3	3	3	42
29. ¿Se protege la información sensible adecuadamente?	6	4	4	4	6	6	4	5	6	4	4	4	57
30. ¿Se mide el desempeño del programa de ciberseguridad?	6	4	6	3	6	4	1	2	5	4	4	3	48
31. ¿Se alinea la estrategia de ciberseguridad con los objetivos del negocio?	6	3	6	6	6	6	4	5	6	4	4	3	59
	90	63	83	59	84	80	57	59	84	66	58	53	

Tabla 4. Consolidado de la autoevaluación de la Sección 2 del cuestionario.

Nivel de madurez	DESCRIPCIÓN
1 - Inexistente	No existe algún proceso establecido que apoye a dar una respuesta a la pregunta realizada.
2 - Inicial	Existen acciones reactivas y solo dependen de la acción de una persona de forma empírica, sin procedimientos establecidos.
3 - Repetible	Existen procedimientos no documentados ni aprobados por la alta dirección, basados en experiencias pasadas.
4 - Definido	Existen procedimientos documentados y aprobados por la alta dirección, que son comunicados y se ponen en práctica.
5 - Administrado	Existen métricas para evaluar el cumplimiento del proceso o acciones consultadas, para su seguimiento y adecuado tratamiento.
6 - Optimizado	La estrategia de ciberseguridad si incluye el tema consultado y está integrado dentro de la estrategia de la Organización.

Tabla 5. Descripción de los niveles de madurez del CSF NIST.

Por último, se presentan los principales desafíos enfrentados por las UIF en la implementación de controles de ciberseguridad y las acciones tomadas para atenderlos.

Desafíos	Medidas adoptadas
***Phishing* y exposición de información sensible.**	Se implementaron campañas informativas y de concientización.
Resistencia al cambio ante la aplicación de controles y políticas más estrictas.	Se realizaron capacitaciones y campañas de sensibilización en ciberseguridad.
Disponibilidad presupuestaria.	Se gestionó apoyo de organismos internacionales.
Gestión de parches y actualizaciones en servidores y aplicaciones *legacy*.	Se fortalecieron políticas para regular el versionamiento de sistemas operativos en servidores.
Falta de cultura en ciberseguridad y desconocimiento de amenazas.	Se reforzó la gobernanza, separando la gestión de ciberseguridad del área de TI; se asignaron más recursos para la implementación de controles y se conformó el Comité de Seguridad de la Información.
Escasez de personal técnico especializado en ciberseguridad.	Se recurrió a la contratación de servicios de *outsourcing*.
Metodología institucional de gestión de riesgos no alineada con la evaluación de riesgos de ciberseguridad en activos críticos.	Se estableció una metodología específica de gestión de riesgos de ciberseguridad por activo de información, complementaria a la institucional.
Intercambio de información con unidades complementarias e interinstitucionales.	Se habilitó el intercambio de información mediante canales seguros, como VPN.
Desarrollo óptimo de pruebas de hackeo ético.	Se utilizaron herramientas de pentesting (ej. Kali Linux).
Matriz de accesos a aplicativos ante cambios, desligues y rotación de personal (ausencia de sistema integral de control de accesos).	*(No se indicó medida específica).*
Ausencia de procedimientos para la gestión de información crítica y de herramientas de identificación y gestión de riesgos.	Se promovió la gobernanza de datos mediante consultorías y se planificó la adquisición de una herramienta ejecutiva para la medición y gestión de riesgos.

Desafíos	Medidas adoptadas
Aparición de nuevas amenazas.	Se redujeron superficies de ataque, se actualizaron defensas tecnológicas (antimalware, DLP, antispam), se aplicaron parches en sistemas operativos, se fortaleció la inteligencia de amenazas y se estableció monitoreo continuo.
Costo de implementación de soluciones tecnológicas, cumplimiento normativo, transformación digital, procesos manuales y complejidad de sistemas.	Se priorizaron riesgos y se adoptó una implementación gradual de soluciones de ciberseguridad.

VI. CONCLUSIONES

- Realizando un análisis global de las respuestas registradas en la sección 2, se identifica que seis UIF (50%) se autoevaluaron en el nivel más alto de cumplimiento respecto de los aspectos consultados. Si bien una validación más precisa requeriría un proceso técnico más extenso —con revisiones documentales y contrastación de evidencias para los 106 requerimientos del NIST CSF 2.0—, los resultados obtenidos permiten contar con un panorama consolidado del nivel de madurez alcanzado. Sobre esta base, el diagnóstico ofrece elementos suficientes para identificar brechas comunes, orientar las áreas de mejora prioritarias y sustentar las recomendaciones que se presentan a continuación.
- Del total de 15 preguntas evaluadas, el 33% reflejó un nivel de madurez promedio de 'Administrado', el 54% de 'Definido' y el 33% de 'Repetible', por lo que el presente diagnóstico permitió establecer recomendaciones que las UIF de los países miembros puedan conocer y evaluar con mayor detalle y adoptar en sus estrategias de ciberseguridad, acorde al apetito de riesgo y recursos existentes.
- Las pregunta 25, relacionada con la evaluación de proveedores externos en términos de seguridad, y la 28, vinculada al análisis forense tras incidentes, obtuvieron una calificación menor a 4 lo que significa que existen procesos básicos y repetidos en camino a ser formalizados, estandarizados y optimizados que deben de darse prioridad y que apoyan a una adecuada respuesta de incidentes de ciberseguridad.
- El diagnóstico realizado establece un nivel generalmente adecuado de gestión de esfuerzos de ciberseguridad, que incluye métricas que permitan adoptar la mejora continua de los procesos necesarios para medir la efectividad de la estrategia de ciberseguridad de la UIF.
- Más de la mitad de las UIF cuentan con un Comité de Seguridad de la Información y dos unidades afirman contar con un Oficial de Seguridad de la Información CISO *(Chief Information Security Officer),* lo que permite brindar retroalimentación a la alta dirección sobre la situación de ciberseguridad.
- Las doce UIF manifiestan interés en establecer una red de contactos de expertos en ciberseguridad que permitan compartir experiencias y casos de amenazas de ciberseguridad identificadas, lo cual contribuiría a realizar diagnósticos periódicos que faciliten adaptar las estrategias de ciberseguridad acorde a los riesgos dinámicos y complejos de la actualidad.
- La concientización y canales de comunicación establecidos para la gestión de incidentes de ciberseguridad, predomina como acciones que se realizan en las UIF, para reducir la probabilidad de una brecha de seguridad.

VII. RECOMENDACIONES

A partir de los resultados del diagnóstico, se presentan a continuación las recomendaciones correspondientes a cada dominio de acción y categoría de NIST CSF evaluados. Estas recomendaciones abordan las principales brechas identificadas y proponen iniciativas y buenas prácticas orientadas a consolidar y fortalecer el nivel de madurez de las UIF, así como la eficacia de sus procesos institucionales en el corto y mediano plazo.

A. Función: detectar

Categoría	**El monitoreo continuo (DE. CM):** los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros eventos potencialmente adversos.	Plazo	**Corto**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio administrado en todas las subcategorías evaluadas del marco NIST CSF v2.0. Sin embargo, en la subcategoría DE.CM-06: "Las actividades y servicios de los proveedores externos son monitoreados para detectar eventos potencialmente adversos", se identificó un nivel de madurez repetible, lo que evidencia una brecha respecto al resto de las subcategorías evaluadas.

Recomendación

Para avanzar hacia el nivel de madurez administrado en la subcategoría DE.CM-06: "Las actividades y servicios de los proveedores externos son monitoreados para detectar eventos potencialmente adversos", se recomienda a las UIF fortalecer o implementar las iniciativas siguientes:

1. **Estandarizar el proceso de supervisión de proveedores externos:** documentar un procedimiento formal que defina los roles, responsabilidades y frecuencia de monitoreo, asegurando su alineación con la política general de gestión de riesgos de cada UIF.
2. **Clasificar y priorizar proveedores críticos:** identificar a los proveedores que manejan información sensible o prestan servicios esenciales. Establecer criterios de criticidad para clasificarlos, determinar su nivel de riesgo y priorizar el monitoreo en función del impacto potencial para la unidad.
3. **Integrar requisitos de seguridad en contratos y acuerdos:** solicitar la incorporación de cláusulas específicas de seguridad y monitoreo en los contratos con proveedores. Definir métricas de cumplimiento y establecer mecanismos de reporte periódico de seguridad.
4. **Evaluar periódicamente la seguridad en proveedores críticos:** realizar revisiones regulares de seguridad y asegurar que las unidades de negocio comprendan la importancia del monitoreo, así como los procedimientos para escalar incidentes relacionados con terceros.
5. **Automatizar y monitorear continuamente:** adoptar soluciones de *Third Party Risk Management (TPRM)* o plataformas de seguridad que permitan la supervisión continua de la postura de ciberseguridad de los proveedores, además, se podría robustecer más adelante con alertas automatizadas para detectar comportamientos anómalos o incumplimientos.
6. **Definir indicadores de desempeño (KPIs) y reportes:** establecer métricas claras para medir la efectividad del monitoreo, como:
   - Porcentaje de proveedores críticos con monitoreo activo.
   - Número de incidentes detectados en terceros.
   - Nivel de cumplimiento de los SLA de seguridad.

Categoría	**El análisis de eventos adversos (DE. AE):** se analizan anomalías, indicadores de compromiso y otros eventos potencialmente adversos para caracterizar los eventos y detectar incidentes de ciberseguridad.	Plazo	**Mediano**

Situacion actual

Las UIF presentan un nivel de madurez promedio Administrado en la totalidad de las subcategorías evaluadas del NIST CSF v2.0.

Recomendación

Se recomienda conservar el nivel de madurez administrado y continuar fortaleciendo los controles para asegurar un proceso sólido, consistente y con capacidad de adaptación frente a nuevas amenazas. Para ello, se plantean las acciones siguientes:

1. Actualizar de forma continua los procedimientos de análisis de eventos, garantizando su alineación con las políticas de gestión de incidentes.
2. Fortalecer las capacidades de correlación y contextualización, incorporando inteligencia de amenazas *(Threat Intelligence)* que permita mejorar la detección temprana y reducir falsos positivos.
3. Mantener criterios claros de severidad e impacto, promoviendo que los analistas diferencien con rapidez entre eventos menores y potenciales incidentes críticos.
4. Automatizar el análisis inicial de eventos, utilizando herramientas que agilicen la clasificación y priorización de alertas.
5. Implementar un esquema de monitoreo y mejora continua, sustentado en métricas e indicadores de desempeño que midan la efectividad del proceso.
6. Realizar revisiones periódicas y documentar las lecciones aprendidas, integrando mejoras derivadas de incidentes pasados para fortalecer la resiliencia de las unidades.

B. Función: recuperar

Categoría	**RECOVER (RC):** se restauran los activos y operaciones afectados por un incidente de ciberseguridad.	Plazo	**Corto**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio administrado en la mayoría de las subcategorías evaluadas conforme al marco NIST CSF v2.0. No obstante, en la subcategoría RC.RP-02: “Las acciones de recuperación se seleccionan, delimitan, priorizan y ejecutan” se identificó un nivel de madurez Repetible, mientras que en la subcategoría RC.RP-01: “La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez iniciada desde el proceso de respuesta a incidentes” se alcanzó un nivel definido. Estos resultados evidencian una brecha respecto al resto de las subcategorías evaluadas.

Recomendación

Para avanzar hacia el nivel de madurez administrado en las subcategorías que presentan brechas respecto al promedio, se recomienda a las UIF implementar las iniciativas siguientes:

1. Integrar el plan de recuperación con la política general de continuidad de negocio y gestión de incidentes, asegurando que se establezcan:
   - Procedimientos definidos y estandarizados para la selección, delimitación, priorización y ejecución de las acciones de recuperación.

- Roles y responsabilidades claramente asignados para cada etapa del proceso de recuperación.

2. Definir umbrales de impacto (operacional, regulatorio, reputacional) que permitan decidir qué acciones se ejecutan primero e incorporar matrices de criticidad para facilitar decisiones rápidas y consistentes.
3. Integrar el proceso de recuperación con el plan de respuesta a incidentes.
4. Implementar mecanismos de monitoreo y control mediante el establecimiento de indicadores de desempeño (KPIs) como: tiempo promedio de ejecución de acciones de recuperación, porcentaje de acciones completadas según prioridad, cumplimiento de SLA de recuperación.
5. Realizar capacitación y simulacros periódicos.
   - Involucrar activamente al personal de la unidad en la ejecución de acciones de recuperación bajo distintos escenarios.
   - Realizar simulacros periódicos que validen la efectividad del proceso y permitan ajustar y robustecer los procedimientos.
   - Incorporar lecciones aprendidas de incidentes y simulacros en el plan de recuperación.

Categoría	**Comunicación de recuperación de incidentes (RC.CO):** las actividades de restauración se coordinan con partes internas y externas.	**Plazo**	**Mediano**

Situacion actual

Las UIF presentan un nivel de madurez promedio administrado en la totalidad de las subcategorías evaluadas del NIST CSF v2.0.

Recomendación

Se recomienda conservar el nivel de madurez Administrado, asegurando un proceso sólido, consistente y con capacidad de adaptación frente a nuevas amenazas. Para ello, se plantean las siguientes buenas prácticas:

1. Usar canales seguros y redundantes.
   - Definir y automatizar el uso de canales cifrados (correo seguro, mensajería corporativa, portales de crisis).
   - Establecer mecanismos redundantes (SMS, llamadas automatizadas) para asegurar la comunicación incluso si la infraestructura principal está afectada.
2. Integrar con sistemas de monitoreo y respuesta.
   - Conectar el SIEM/SOAR con directorios corporativos *(Active Directory, IAM)* para identificar automáticamente responsables y grupos de interés.
   - Integrar con sistemas de *ticketing* (*ServiceNow*, *Jira*, etc.) para que las tareas de recuperación se asignen y comuniquen sin intervención manual.

C. Función: proteger

Categoría	**Administración de identidades, autenticación y control de acceso (PR. AA):** el acceso a los activos físicos y lógicos está limitado a los usuarios, servicios y *hardware* autorizados, y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado.	**Plazo**	**Mediano**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio administrado en todas las subcategorías evaluadas del NIST CSF versión 2.0, lo que evidencia que sus procesos de gestión de identidades y accesos se encuentran formalizados, integrados y en proceso de ser medidos, bajo un enfoque orientado al riesgo.

Recomendación

Con el objetivo de consolidar el nivel de madurez administrado en todas las Unidades de Información Financiera, se recomienda implementar y reforzar las buenas prácticas detalladas a continuación:

1. **Contar con políticas de acceso:** mantener políticas de gestión de identidades y accesos debidamente formalizadas, revisándolas al menos una vez al año para garantizar su alineación con riesgos emergentes y regulaciones internacionales.
2. **Gestionar el ciclo de vida de identidades:** mantener procesos formales para el alta, modificación y baja de usuarios, servicios y dispositivos, integrando la gestión de identidades con los sistemas de RRHH y administración de activos, para asegurar la trazabilidad.
3. **Robustecer la autenticación:** mantener la obligatoriedad de autenticación multifactor (MFA) en accesos críticos y evaluar la adopción progresiva de métodos más seguros (*passwordless*, biometría) para mitigar riesgos asociados a contraseñas.
4. **Aplicar el principio de mínimo privilegio:** garantizar que los accesos se otorguen únicamente en función de roles y responsabilidades, realizando revisiones periódicas de permisos para evitar acumulación de privilegios innecesarios.
5. **Gestionar cuentas privilegiadas:** fortalecer el control sobre cuentas administrativas mediante soluciones de *Privileged Access Management* (PAM).
6. **Monitorear sesiones privilegiadas:** supervisar y registrar las sesiones privilegiadas para asegurar trazabilidad y cumplimiento normativo.
7. **Tener registros centralizados:** mantener registros unificados de accesos físicos y lógicos para mejorar la visibilidad y el control.
8. **Realizar auditorías periódicas:** realizar auditorías regulares que validen la correcta aplicación de controles y permitan detectar desviaciones.
9. **Integrar la dimensión físico-lógica:** procurar que los sistemas de control de acceso físico estén integrados con la gestión de identidades digitales.
10. **Proteger las áreas críticas:** validar que los accesos a zonas sensibles se encuentren restringidos y monitoreados de manera continua.
11. **Capacitar y concientizar:** mantener programas de formación en buenas prácticas de gestión de accesos y uso seguro de credenciales.
12. **Definir indicadores de desempeño:** definir indicadores clave (KPIs) que midan la eficacia de los controles de acceso.

Categoría	**Sensibilización y capacitación (PR. AT):** el personal de la organización recibe formación y concienciación en materia de ciberseguridad para que pueda realizar sus tareas relacionadas con la ciberseguridad.	Plazo	**Corto**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio definido en todas las subcategorías evaluadas del NIST CSF versión 2.0. Sin embargo, cuatro de las doce UIF analizadas se encuentran en un nivel de madurez inferior, lo que evidencia la oportunidad de fortalecer los procesos de sensibilización y capacitación dentro de la organización.

Recomendación

Para avanzar hacia el nivel de madurez definido en aquellas UIF que presentan brechas respecto al promedio, se recomienda implementar o reforzar esfuerzos en las siguientes iniciativas:

1. Establecer un programa de concientización y formación en ciberseguridad, acompañado de un calendario anual con objetivos definidos, contenidos estructurados y que esté aprobado por la alta dirección.
2. Implementar capacitaciones periódicas y obligatorias en ciberseguridad para todo el personal, incluidos contratistas y terceros con acceso a sistemas críticos, empleando diversos formatos (presencial, virtual, simulaciones y campañas de comunicación interna) y contenidos diferenciados según el perfil de los

participantes (usuarios generales, administradores de sistemas y directivos). Asimismo, se recomienda incorporar la sensibilización como parte integral de los procesos de inducción y de gestión del talento humano.

3. Realizar, al menos una vez al año, ejercicios prácticos de ciberseguridad como simulaciones de *phishing* y escenarios de respuesta a incidentes, con el fin de evaluar el nivel de concientización alcanzado por el personal de la unidad.
4. Definir indicadores clave (KPIs) como porcentaje de personal capacitado, resultados de evaluaciones y reducción de incidentes relacionados con errores humanos.

Categoría	**Seguridad de datos (PR.DS):** los datos se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	Plazo	**Corto**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio definido en la mayoría de las subcategorías evaluadas del NIST CSF versión 2.0, lo que evidencia una oportunidad para fortalecer los controles existentes y avanzar hacia el siguiente nivel de madurez.

Recomendación

Para alcanzar el nivel de madurez Administrado en todas las subcategorías, se recomienda que las UIF implementen o fortalezcan las siguientes iniciativas:

1. **Contar con políticas de seguridad de datos:** mantener políticas de seguridad de datos debidamente formalizadas, aprobadas por la alta dirección y sujetas a revisión anual.
2. **Clasificar y etiquetar la información:** implementar un esquema formal de clasificación de datos (confidencial, restringido, público) que guíe el manejo de la información, así como la implementación de mecanismos de etiquetado automático.
3. **Controlar los accesos basados en riesgo:** aplicar controles de acceso a los datos en función de su nivel de criticidad y sensibilidad, realizando revisiones periódicas de los permisos para evitar la acumulación de privilegios que no correspondan con las funciones actuales de los colaboradores.
4. **Proteger datos en tránsito y en reposo:** se recomienda el uso de cifrado robusto en la transmisión y almacenamiento de información crítica y la implementación paulatina de soluciones de gestión de claves con procesos formalizados de rotación y protección.
5. **Monitorear y registrar actividades sobre datos:** mantener registros centralizados de accesos y modificaciones a datos sensibles, integrándolos en los sistemas de monitoreo (SIEM) para identificar patrones anómalos y detectar intentos de acceso no autorizado.
6. **Gestionar copias de seguridad y recuperación:** mantener procesos de respaldo periódico de datos críticos y pruebas regulares de restauración. Además, se recomienda que las copias de seguridad se cifren y almacenen en ubicaciones seguras.
7. **Proteger contra pérdida y fuga de datos (DLP):** valorar la posibilidad de implementar soluciones de *Data Loss Prevention* (DLP) para monitorear y controlar la transferencia de información sensible.
8. **Alinear la seguridad de datos con la gestión de riesgos:** alinear la seguridad de datos con la estrategia global de gestión de riesgos de la unidad e incorporar métricas e indicadores clave (KPIs) que midan la efectividad de los controles de protección de datos.

Categoría	**Seguridad de la plataforma (PR.PS):** el *hardware*, el *software* (por ejemplo, *firmware*, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger su confidencialidad, integridad y disponibilidad.	Plazo	**Medio**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio definido en la mayoría de las subcategorías evaluadas del NIST CSF versión 2.0. Solo una de las subcategorías alcanzó un nivel de madurez inferior al promedio.

Recomendación

Para que las UIF logren consolidar el nivel de madurez Definido en todas las subcategorías, se brindan las siguientes recomendaciones y técnicas que ayudaran a este propósito.

1. **Contar con políticas y procedimientos:** mantener políticas y procedimientos para la gestión segura de hardware, *software* y servicios de plataforma, formalizadas y aprobadas por la alta dirección y sujetas a revisión anual.
2. **Inventariar y gestionar los activos tecnológicos:** mantener un inventario actualizado de *hardware, software* y servicios utilizados en la unidad, así como un proceso de alta, modificación y baja de activos tecnológicos.
3. **Gestionar parches y actualizaciones:** la aplicación de parches y actualizaciones de *firmware*, sistemas operativos y aplicaciones debe estar regulada mediante un procedimiento formal. Asimismo, se recomienda definir un calendario de mantenimiento preventivo y correctivo, así como llevar un registro detallado de las actividades realizadas durante el año.
4. **Tener configuraciones seguras y estandarizadas:** implementar configuraciones base seguras *(hardening)* para sistemas operativos, aplicaciones y dispositivos de red.
5. **Controlar los cambios en plataformas:** mantener un proceso de gestión de cambios que considere la evaluación de riesgos, aprobación y registro de modificaciones en plataformas físicas y virtuales.
6. **Monitorear y registrar las actividades en plataformas:** implementar mecanismos de monitoreo continuo sobre el uso y desempeño de *hardware* y *software*. Posteriormente, integrar los registros en sistemas de monitoreo centralizados (SIEM) para detectar anomalías o accesos no autorizados.
7. **Gestionar a los proveedores y servicios externos:** realizar evaluaciones de seguridad a los proveedores que suministran *hardware*, *software* o servicios de plataforma, y fortalecer los contratos solicitando la inclusión de cláusulas de seguridad y acuerdos de nivel de servicio (SLA).
8. **Promover la formación periódica del personal técnico:** promover que el personal responsable de la administración de sistemas y servicios reciba formación periódica en prácticas seguras, así como en la concientización sobre riesgos asociados a configuraciones inadecuadas o al uso de *software* obsoleto.

Categoría	**Resiliencia de la infraestructura tecnológica (PR. IR):** las arquitecturas de seguridad se gestionan con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de los activos, así como la resiliencia de la organización.	Plazo	**Mediano**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio administrado en todas las subcategorías evaluadas del NIST CSF versión 2.0.

Recomendación

Se recomienda mantener y fortalecer el nivel de madurez administrado, asegurando la aplicación consistente de controles de acceso adecuados, tal como lo han establecido las UIF en sus dependencias, con el propósito de garantizar que las redes, entornos y activos tecnológicos permanezcan protegidos frente a accesos lógicos no autorizados, así como ante amenazas de carácter ambiental.

D. Función: responder

Categoría	**Gestión de incidentes (RS. MA):** se gestionan las respuestas a los incidentes de ciberseguridad detectados.	Plazo	**Mediano**

Situacion actual

Las UIF alcanzaron un nivel de madurez promedio definido en todas las subcategorías evaluadas del NIST CSF versión 2.0, lo que confirma la existencia de un marco formal y documentado que orienta la gestión de incidentes. Si bien este nivel de madurez resulta aceptable, se recomienda fortalecer las prácticas y controles implementados con el propósito de avanzar hacia el nivel de madurez superior.

Recomendación

Para avanzar al nivel de madurez Administrado en todas las UIF, se recomienda implementar las siguientes buenas prácticas:

1. **Establecer métricas e indicadores de desempeño:** definir indicadores clave (KPIs) para medir la eficacia de la gestión de incidentes: tiempo medio de detección (MTTD), tiempo medio de respuesta (MTTR), tiempo de recuperación, número de incidentes recurrentes. Además, se recomienda establecer un sistema de reporte periódico a la alta dirección donde se presenten los resultados del desempeño de la gestión de incidentes.
2. **Realizar simulaciones y ejercicios de respuesta a incidentes:** al menos una vez al año, realizar simulaciones de incidentes como ejercicios de mesa *(Tabletop)*, simulaciones técnicas, simulaciones de crisis, que permitan validar la efectividad de los procedimientos y el conocimiento de los responsables del proceso.
3. **Automatizar y contar con herramientas de soporte:** automatizar tareas repetitivas (aislamiento de equipos, bloqueo de cuentas, generación de alertas) para reducir tiempos de reacción. Conforme se vaya avanzando en el nivel de adopción, hacer la integración de plataformas de *Security Information and Event Management* (SIEM) y *Security Orchestration, Automation and Response* (SOAR) para mejorar la detección y respuesta.
4. **Gestionar el conocimiento y brindar retroalimentación:** establecer un repositorio centralizado de incidentes y lecciones aprendidas en la actualización de políticas, procedimientos y planes de respuesta.
5. **Fortalecer la comunicación:** definir protocolos de comunicación interna y externa durante incidentes que consideren la notificación a entes reguladores, clientes y socios estratégicos cuando corresponda. Además, se recomienda establecer un comité de crisis que se encargue de coordinar la respuesta en incidentes.
6. **Capacitar continuamente al personal:** mantener la capacitación periódica del personal técnico y directivo en gestión de incidentes, así como formación específica en detección temprana, contención y recuperación.

VIII. REFERENCIAS

Allianz Commercial. (15 de Enero de 2025). *Allianz Risk Barometer 2025*: *Cyber top business risk as climate change hits record high.* Obtenido de *Allianz Commercial*: https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2025.html

Grupo de Acción Financiera de Latinoamérica. (2022). Tercera Actualización del Informe de Amenazas Regional en materia de Lavado de Activos 2019 – 2021. Obtenido de GAFILAT: https://biblioteca.gafilat.org/?p=441

Grupo de Acción Financiera de Latinoamérica. (2024). Cuarta Actualización del Informe de Amenazas Regionales en materia de Lavado de Activos y Financiamiento del Terrorismo 2022-2023. Obtenido de GAFILAT: https://biblioteca.gafilat.org/?p=6966

National Institute of Standards and Technology. (2025). Cibersecurity and Privacy. Obtenido de NIST: https://www.nist.gov/cybersecurity-and-privacy

National Institute of Standards and Technology. (2025). Cibersecurity Framework (CSF) 2.0. Obtenido de NIST: https://www.nist.gov/cyberframework

Verizon Business. (2025). 2025 Data Breach Investigations Report. Obtenido de *Verizon*: https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

PROTEGEMOS LA INTEGRIDAD
DE LOS SISTEMAS FINANCIEROS
DE LATINOAMÉRICA