JIU/REP/2021/3

Naciones Unidas

La ciberseguridad en las organizaciones del sistema de las Naciones Unidas

Informe de la Dependencia Común de Inspección

Preparado por *Jorge Flores Callejas, Aicha Afifi y Nikolay Lozinskiy*

JIU/REP/2021/3
Español
Original: inglés

La ciberseguridad en las organizaciones del sistema de las Naciones Unidas

Informe de la Dependencia Común de Inspección

Preparado por *Jorge Flores Callejas, Aicha Afifi y Nikolay Lozinskiy*

Naciones Unidas • Ginebra, 2021

Equipo encargado del proyecto:

Jorge Flores Callejas, Aicha Afifi, Nikolay Lozinskiy, Inspectores

Vincent Hermie, Oficial de Evaluación e Inspección

Szilvia Petkov, Oficial de Evaluación e Inspección Asociada

Hervé Baudat, Asistente de Investigación

Dejan Dincic, Consultor

Charlotte Claveau, Alina Datsii, Bianca Canevari, Pasantes

Resumen

La ciberseguridad en las organizaciones del sistema de las Naciones Unidas

En el mundo digitalizado de hoy, la ciberseguridad se ha convertido en una cuestión de importancia para las organizaciones internacionales, y las Naciones Unidas no son una excepción. La transformación digital, la creciente dependencia de las tecnologías de la información y las comunicaciones (TIC) y las soluciones ciberhabilitadas, y el hecho de que las ciberamenazas se multipliquen constantemente, tanto en sofisticación como en potencial disruptivo, han llevado a un aumento sin precedentes de los riesgos de ciberseguridad a los que se enfrenta el sistema de las Naciones Unidas. Aunque la ciberseguridad surgió por primera vez en el ámbito de las TIC, ahora que los sistemas de gestión de la información están profundamente arraigados en la mayoría de las actividades empresariales y que el panorama de las amenazas ha evolucionado considerablemente, exigiendo algo más que meras defensas basadas en la tecnología, ya no parece viable considerar la ciberseguridad únicamente a través de la lente reductora de las TIC. En el presente informe, los Inspectores abogan por la integración de las consideraciones de ciberseguridad en marcos organizativos más amplios, como la gestión del riesgo institucional, la planificación de la continuidad de las actividades y la integridad y seguridad, así como por la incorporación de la cuestión en toda la organización.

En años recientes, el sistema de las Naciones Unidas ha sido cada vez más consciente de que es preciso prestar atención a la ciberseguridad. Las posibles consecuencias de una posición débil en materia de ciberseguridad trascienden, en efecto, la mera perturbación de la infraestructura y los sistemas de TIC o el volumen de datos que pueden a la postre quedar expuestos. Lo que está en juego más bien es la capacidad de las organizaciones del sistema de las Naciones Unidas para cumplir sus mandatos, y también su credibilidad ante sus miembros y beneficiarios. Además, muchas categorías de personas cuyos datos custodian las organizaciones del sistema de las Naciones Unidas pueden quedar expuestas a importantes consecuencias adversas en caso de ser filtrados. Aunque los ciberataques pueden afectar de manera diferente a organizaciones con mandatos y estructuras diversas, la amenaza es real y compartida. Ninguna organización está a salvo de experimentar en alguna ocasión un incidente de ciberseguridad, independientemente de lo preparada que esté o lo vigilante que sea. Además, si se desdeñan los riesgos de que ello ocurra, el impacto en la reputación y las repercusiones operacionales, jurídicas y financieras pueden ser considerables.

Objetivos del presente examen y estructura del informe

Los principales objetivos del presente examen son: a) identificar y analizar los retos y riesgos comunes en materia de ciberseguridad a los que se enfrentan individualmente las organizaciones del sistema de las Naciones Unidas, así como las respectivas respuestas a dichos retos, teniendo en cuenta los requisitos contextuales específicos de las organizaciones (perspectiva vertical); y b) examinar las actuales dinámicas interinstitucionales que facilitan un enfoque de la ciberseguridad a nivel de todo el sistema para mejorar la coordinación, la colaboración y el intercambio de información entre las organizaciones del sistema de las Naciones Unidas y, en su caso, las posibilidades de compartir soluciones (perspectiva horizontal).

Basándose en la autoevaluación proporcionada por las organizaciones participantes, los Inspectores presentan en primer lugar, en el capítulo II, una instantánea del panorama de ciberseguridad al que se enfrenta el sistema de las Naciones Unidas, describiendo los tipos de amenazas y los medios de ataque más frecuentes, con indicaciones sobre su impacto notificado, y llamando la atención sobre determinadas cuestiones técnicas que deben examinarse más a fondo. En el capítulo III, los Inspectores examinan las disposiciones institucionales y las prácticas conexas en las organizaciones del sistema de las Naciones Unidas en relación con un conjunto de elementos clave

identificados en el curso del examen que contribuyen a la ciberresiliencia de las organizaciones y ponen de relieve las buenas prácticas, de haberlas. En el capítulo IV, la atención se centra en los mecanismos interinstitucionales destinados a fomentar la coordinación y la colaboración entre las organizaciones del sistema de las Naciones Unidas y las capacidades operativas que permiten el desarrollo y la aplicación de soluciones compartidas en materia de ciberseguridad, cuando dichas soluciones son razonables. Los expertos están de acuerdo en que la respuesta debe basarse en las características y requisitos propios de cada organización (en función de su mandato, la información que posee o gestiona, la exposición, los recursos, etc.). Al mismo tiempo, las organizaciones del sistema de las Naciones Unidas no operan de forma aislada y están interconectadas en muchos aspectos, en particular a través de la programación conjunta y de un cierto grado de interdependencia en sus mandatos y actividades. Por lo tanto, es esencial reconocer las áreas de exposición común, así como explorar los ámbitos susceptibles de ser objeto de un enfoque concertado.

La ciberseguridad en el sistema de las Naciones Unidas

No hay una sola organización del sistema de las Naciones Unidas que no haya sufrido algún tipo de ciberataque, grande o pequeño. Las acciones maliciosas dirigidas a los usuarios de los sistemas de información (a través de *phishing*, robo de identidad, esquemas basados en una "persona entrometida", etc.) o a la infraestructura (*malware*, ataques de denegación de servicio distribuida, etc.) son, con mucho, la fuente más frecuente de las amenazas denunciadas. Mientras que las amenazas a la ciberseguridad se asocian comúnmente con operaciones técnicas sofisticadas, la comunidad de expertos observa un cambio palpable, en virtud del cual se ha pasado de los jáquers que atacan servidores, redes y dispositivos situados al final de la cadena a otros que piratean a las personas, utilizando técnicas de ingeniería social destinadas a manipular a los individuos para que divulguen información sensible con propósitos fraudulentos y otros fines ilícitos. La pandemia de enfermedad por coronavirus (COVID-19) exacerbó aún más los riesgos relacionados con la ingeniería social: más de dos tercios de las organizaciones participantes informaron de un fuerte aumento de las amenazas y vulnerabilidades de ciberseguridad durante los confinamientos globales, que desconectaron a muchos usuarios de los recursos de ciberseguridad gestionados de forma centralizada.

Al mismo tiempo, la repercusión comunicada de los incidentes experimentados por las organizaciones participantes fue limitada, lo que podría llevar a la conclusión prematura de que no hay motivos graves de preocupación. No es esta la conclusión a la que han llegado los Inspectores. En primer lugar, los datos recopilados implican necesariamente algunos ángulos ciegos, entre ellos los resultantes de una comprensible reticencia a exponer el nivel de vulnerabilidad conocido y de la naturaleza opaca de las actividades cibernéticas en general, lo que parece indicar que la magnitud exacta de la amenaza y las consecuencias conexas pueden ser simplemente desconocidas. La mayoría de las veces, especialmente en el caso de los ataques más sofisticados, los adversarios no tienen ningún incentivo para revelar su presencia ni las vulnerabilidades que han explotado, lo que sugiere que es probable que el número de violaciones del sistema y de fugas de datos sea significativamente mayor de lo que se informa. La brecha entre "aquello que se sabe que se desconoce" y lo que se conoce sobre la magnitud de la amenaza de ciberseguridad es amplia, pero la que separa "lo que se sabe que se desconoce" con "lo que no se sabe que se desconoce" puede ser aún más inquietante. Por lo tanto, juzgar la gravedad de la amenaza en función de los casos en que sabemos que dicha amenaza se ha materializado en el pasado sería una equivocación. El potencial de daño sigue siendo elevado y exige una atención y priorización constantes.

Diferencias en cuanto a la madurez de las organizaciones y aspectos concretos de la preparación tecnológica

El presente examen no pretendía ofrecer una evaluación exhaustiva de la solidez de las disposiciones operativas o de la infraestructura técnica de cada organización participante, sino más bien comprender las capacidades generales existentes y singularizar algunas cuestiones comunes que pudieran merecer especial atención. Por razones obvias

vinculadas al objeto del presente examen, los Inspectores optaron por no revelar disposiciones organizativas específicas que pudieran poner en peligro la seguridad de las entidades en cuestión. Teniendo en cuenta las limitaciones inherentes al hecho de que la información se haya recopilado principalmente a través de la autoevaluación, así como las considerables diferencias en el nivel de detalle proporcionado por los encuestados, la Dependencia Común de Inspección observó diferencias significativas en el enfoque que las organizaciones participantes han adoptado en sus respectivas respuestas a las amenazas a la ciberseguridad y, en consecuencia, en la madurez de su posición de ciberseguridad. Estas diferencias pueden explicarse debido a: el entorno en el que opera cada organización; los requisitos que impone el tipo de datos que se custodian; el nivel de comprensión del problema y la prioridad concedida a la ciberseguridad por sus dirigentes; la propia perspectiva histórica de las organizaciones; la disponibilidad de recursos; y la gran variedad de soluciones de sistemas de TIC, herramientas y software utilizadas a lo largo y ancho del sistema.

Las organizaciones participantes opinaron que habían comprendido bien los aspectos técnicos fundamentales de la ciberseguridad y que habían invertido en ella de acuerdo con sus respectivas capacidades. En cuanto a la capacidad tecnológica y operativa, los Inspectores se limitaron a destacar una serie de cuestiones que podrían merecer una atención más específica, como la gestión de los dispositivos de usuario final y las herramientas que facilitan el trabajo a distancia, en particular en el contexto de la pandemia de COVID-19; los riesgos asociados a remanentes de sistemas heredados, adquiridos en el pasado o establecidos a nivel interno con el tiempo, que podrían no ser compatibles con los actuales barridos y parcheados de seguridad; la continua expansión del uso de la computación en la nube; las disposiciones organizativas para la gestión de la vulnerabilidad; y las prácticas de tecnología de la información en la sombra que implicaban el uso y la aplicación de herramientas tecnológicas fuera del marco corporativo de las TIC. Cabe señalar que, a pesar de los numerosos desafíos encontrados, la llegada de la pandemia también ha propiciado algunos avances positivos. Las entidades de las Naciones Unidas se vieron obligadas a examinar más detenidamente sus marcos de gestión de la seguridad, y los proyectos corporativos de TIC planificados empezaron a materializarse bajo el apremio de la necesidad inmediata. Puede decirse que el cambio masivo al trabajo a distancia, realizado casi sin previo aviso, llevó a muchas organizaciones a acelerar sus esfuerzos para mejorar la seguridad del acceso remoto y puede haber proporcionado un impulso muy necesario para materializar medidas en este sentido.

Elementos que contribuyen a mejorar la ciberresiliencia

Los Inspectores examinaron una serie de elementos que podrían mejorar la posición de ciberseguridad de las organizaciones del sistema de las Naciones Unidas y su capacidad para identificar, prevenir y detectar las ciberamenazas, así como para responder a los incidentes y recuperarse de ellos. Se requiere un enfoque multifacético que implique a la organización a todos los niveles: los órganos legislativos y de gobierno; los mecanismos de supervisión; la dirección ejecutiva; los gestores intermedios tanto de las dependencias administrativas como de las sustantivas o institucionales; y el personal en general. Además, la naturaleza transversal del asunto requiere una perspectiva más amplia que vaya más allá de las TIC e integre firmemente la ciberseguridad en la gestión de los riesgos institucionales, así como la búsqueda de una mayor convergencia entre la seguridad física y la ciberseguridad. Por último, sin ser por ello menos importante, la capacidad interna de recursos humanos especializados, complementada con servicios contratados a proveedores externos para hacer frente a necesidades específicas y puntuales y una asignación de recursos financieros acorde con las necesidades de cada organización constituyen la columna vertebral de una posición de ciberseguridad sólida. En resumen, el grado en que estos elementos se reflejan en el enfoque de ciberseguridad de una organización influye directamente en su ciberresiliencia. Por lo tanto, los Inspectores recomiendan que los jefes ejecutivos inicien un examen de la organización en su conjunto para estudiar el grado en que cada uno de estos elementos, como se detalla más adelante, está integrado en las políticas y prácticas de la organización, e informen de los resultados a sus órganos legislativos y rectores con miras a recibir orientación sobre cómo reforzar

aún más la ciberresiliencia, teniendo en cuenta los puntos fuertes y débiles identificados en ese proceso (recomendaciones 1 y 2).

Órganos legislativos y de gobierno para proporcionar orientación estratégica y recursos

En el sistema de las Naciones Unidas, la ciberseguridad se sigue percibiendo como una cuestión predominantemente técnica, lo que quizás explique el hecho de que los órganos legislativos y rectores, en la mayoría de las organizaciones, hayan sido hasta la fecha raramente invitados a tomar parte en la cuestión, y que tampoco ellos hayan solicitado hacerlo. Habida cuenta de las dimensiones más amplias de la ciberseguridad señaladas en el presente informe, los Inspectores opinan que los órganos legislativos y rectores deberían implicarse más a fondo en la cuestión y proporcionar orientación estratégica de alto nivel, incluso mediante la formulación de una declaración explícita apostando por una mayor asunción de riesgo y la correspondiente asignación de recursos, que contribuyan a lograr el nivel de protección deseado. En términos más generales, la dirección ejecutiva debería reflexionar sobre la forma de informar regularmente sobre asuntos de ciberseguridad a los órganos legislativos y rectores y utilizarla para facilitar la interacción con dichos órganos, dentro de los límites de lo que puede considerarse necesario y suficiente sin poner en peligro las defensas de la organización. Teniendo en cuenta la naturaleza abrupta y de potencial alto impacto de los incidentes de ciberseguridad, los Inspectores también aconsejan a las organizaciones que prevean la necesidad de elevar los incidentes a los órganos legislativos y rectores, tanto internamente como entre los miembros de dichos órganos, así como los procedimientos a seguir en los casos en que ello sea necesario.

La atención de los organismos de supervisión contribuye a mejorar las medidas de ciberseguridad

Se comprobó que los mecanismos de supervisión interna y externa de las organizaciones del sistema de las Naciones Unidas habían prestado atención a las cuestiones de ciberseguridad, incluso cuando no había referencias específicas a este tema en sus mandatos. Los Inspectores se encontraron con varios ejemplos de mejoras institucionales introducidas en el marco de la ciberseguridad de las organizaciones participantes que tenían su origen en recomendaciones de supervisión (por ejemplo, la creación de un puesto de oficial jefe de seguridad de la información, recomendaciones sobre formación, establecimiento de una hoja de ruta a seguir, etc.). De hecho, los comités de auditoría y supervisión abordan las cuestiones de ciberseguridad como parte de su mandato, que abarca la gestión de los riesgos corporativos de la empresa, y no en el contexto de la gobernanza de las TIC. Es encomiable que estos comités hayan adoptado el tema, no solo para apoyar a la dirección, sino también como forma de informar a los órganos legislativos y rectores sobre los riesgos de ciberseguridad relevantes, permitiéndoles contribuir a la mitigación de los riesgos de la organización. Para garantizar que todos los órganos de supervisión aporten el máximo valor desde el punto de vista de la ciberseguridad, es importante que los conocimientos y la experiencia de los expertos en ciberseguridad de una organización determinen y alimenten la labor de la función de supervisión.

Marcos reguladores, cumplimiento y rendición de cuentas

Las organizaciones participantes se remiten a una amplia gama de normas sectoriales sobre ciberseguridad, a veces a más de una, y la mayoría de ellas ya han obtenido la certificación con arreglo a la norma ISO 27001, tienen previsto hacerlo, o han optado por ajustar voluntariamente su marco a esa norma sin solicitar certificación oficial. Los Inspectores no abogan por una norma sectorial o un enfoque armonizado para todo el sistema a este respecto, ya que diferentes normas pueden servir perfectamente para diferentes propósitos y ofrecer opciones adecuadas para distintos niveles de madurez. No obstante, hay razones de peso para inspirarse —de manera formal o informal— en las normas pertinentes del sector a la hora de establecer y gestionar el propio marco

normativo. Por lo tanto, las organizaciones participantes deben identificar la norma adecuada y, dentro de esa norma, los controles más pertinentes, basándose en el nivel de protección necesario que se ajuste a su propia situación, en función de los requisitos y los riesgos identificados a través de una adecuada evaluación de riesgos de ciberseguridad específicamente pensada para la organización.

Varias de las principales normas del sector exigen la existencia de políticas específicas de ciberseguridad y procedimientos documentados como pilar fundamental de los controles que sustentan el enfoque de la ciberseguridad de una entidad. Con algunas pocas excepciones, puede decirse que las organizaciones participantes han reconocido la importancia de contar con un marco de referencia articulado que guíe su enfoque de la ciberseguridad. Las estrategias de alto nivel en materia de TIC suelen incluir consideraciones de ciberseguridad, aunque con distintos grados de elaboración. Más de dos tercios de las organizaciones participantes han desarrollado instrumentos específicos sobre ciberseguridad, tres de ellas están revisando su marco y cuatro están en proceso de desarrollar políticas específicas. Al mismo tiempo, en cuatro organizaciones participantes la función de ciberseguridad, incluido el marco normativo asociado, se consideró que era, en el mejor de los casos, incipiente. La cuestión del cumplimiento —y, en particular, de la aplicación obligatoria en caso de incumplimiento— de las directivas vigentes inspiraba menos confianza en relación con la existencia de una cultura de ciberseguridad corporativa a nivel de todo el sistema. En opinión de los Inspectores, esto justifica un examen más detallado y enfoques más matizados para mejorar la exigencia de responsabilidad por las brechas de seguridad y proteger a las organizaciones de forma más general.

La cultura de ciberseguridad fluye desde el nivel directivo hacia niveles inferiores

El primer paso para inculcar una cultura de ciberseguridad es que la propia dirección sea consciente de los riesgos asociados y desarrolle una comprensión de las implicaciones de una ciberhigiene deficiente. Ello supone la adopción de una posición más activa por parte de los altos directivos a la hora de garantizar que los mecanismos de gobernanza interna se establezcan de manera que les proporcionen la información y la base de datos probatorios que necesitan. El papel de la dirección ejecutiva a este respecto trasciende la mera toma de decisiones sobre la asignación de recursos. Un elemento clave es fomentar una cultura interna en la que el reconocimiento y el seguimiento proactivo de los incidentes ocurridos no se vea como el reconocimiento de un fracaso, sino más bien como un punto de partida para abordar conjuntamente un problema compartido y proteger mejor la organización y sus activos. Otras formas en las que la dirección ejecutiva puede inspirar la adopción de medidas e influir en la mentalidad de la cadena de mando en términos concretos son modelando los comportamientos recomendados, garantizando la responsabilidad de la dirección en toda la organización, participando en programas de concienciación y desplegando un estilo de liderazgo comprometido en cuestiones de ciberseguridad en general. Es necesario un cambio cultural en el sistema de las Naciones Unidas, y la aportación de los directores ejecutivos a la hora de marcar la pauta desde arriba es esencial para lograrlo.

Integrar la ciberseguridad como empeño a nivel de toda la organización

En consonancia con la idea cada vez más extendida de que la responsabilidad de la ciberseguridad no puede recaer únicamente en los departamentos de TIC, la mayoría de las organizaciones participantes han reconocido, de un modo u otro, que tanto los departamentos administrativos como los sustantivos tienen un papel que desempeñar. Sin embargo, la información recopilada durante el presente examen sugiere que las dependencias organizativas en general pueden no ser todavía suficientemente receptivas a la integración de los requisitos de ciberseguridad y resiliencia en el diseño y la ejecución de sus proyectos y actividades. En algunos sectores, las políticas y procedimientos de ciberseguridad se veían al parecer como un impedimento para la agilidad y la eficiencia operativas, más que como escudos protectores de la reputación y los activos de las organizaciones. Es especialmente importante que los directores ejecutivos contrarresten activamente estas percepciones. Hacer más explícitas las dimensiones de ciberseguridad

de las funciones programáticas y administrativas puede reducir los malentendidos sobre las funciones y responsabilidades complementarias de los distintos departamentos y también abordar la falta de implicación detectada entre algunas partes interesadas durante el presente examen. La integración de las consideraciones de ciberseguridad en las políticas y prácticas que rigen la labor de todos los departamentos sería en sí misma un reconocimiento de que cada área de trabajo en una organización tiene su propia contribución que aportar al objetivo de disponer de un enfoque de toda la organización al respecto.

El personal como primera línea defensiva

El reto de educar a cada miembro del personal sobre su papel en la protección de la información y los activos digitales de la organización, así como sobre la importancia de someterse a las políticas, procedimientos y mejores prácticas en materia de ciberseguridad, sigue ahí. El factor humano ha cobrado más importancia no solo en el panorama general de las amenazas a la ciberseguridad, como queda reflejado en la preocupación mundial por los usuarios finales individuales que son, cada vez más, blanco de ataques, sino también como elemento importante en la estructura de defensa de las organizaciones participantes, siempre que dichos usuarios reciban la formación adecuada. La constatación de que la responsabilidad de la ciberprotección empieza por unos usuarios bien informados y vigilantes ha desencadenado importantes actividades de formación e iniciativas de sensibilización, a pesar de las limitaciones de recursos, la fatiga formativa de los usuarios y las dificultades para seguir la constante evolución de la cuestión. No obstante, la multitud de programas e iniciativas individuales no parecen llevarse a cabo de forma coherente, sistemática o basada en los riesgos. Por lo tanto, los Inspectores aconsejan a las organizaciones que se propongan desarrollar un programa global de formación y sensibilización concebido como una herramienta proactiva para cambiar la cultura interna mediante el establecimiento de objetivos claros bien definidos para cada categoría de interesados en función de los riesgos que puedan representar para la organización, en lugar de proponer módulos individuales a todos sin guiarse por una visión estratégica. Es fundamental prestar atención a los usuarios ocasionales de los sistemas corporativos de TIC, incluidos los delegados de conferencias, los pasantes, los visitantes y otras categorías de personal que no forman parte de la plantilla, ya que estos usuarios suelen conectarse a la infraestructura corporativa con sus propios dispositivos. Además, al ser usuarios poco frecuentes de los sistemas en cuestión, es menos probable que estén familiarizados con su uso correcto y seguro, ajustado a las políticas y prácticas organizativas de rigor.

Optimización del gasto e inversión en ciberseguridad

La estimación de los recursos dedicados actualmente a la ciberseguridad representa un reto, debido a las características de los marcos financieros y presupuestarios de las organizaciones del sistema de las Naciones Unidas y a sus prácticas de gestión y contabilidad de dichos recursos. Ni que decir tiene que un marco de ciberseguridad bien protegido tiene su precio. A pesar del aumento de los recursos asignados a ciberseguridad, los profesionales del sistema de las Naciones Unidas siguen percibiendo la escasez de recursos como un obstáculo para lograr que sus organizaciones puedan cubrir todos los aspectos de la ciberresiliencia. Un punto importante a tener en cuenta es que las sumas gastadas en ciberseguridad no reflejan automáticamente el nivel de protección. Más que debatir sobre el "cuánto", la clave es determinar "dónde" deben asignarse los recursos para conseguir el impacto más decisivo. Independientemente de la cantidad de fondos disponibles, la información recopilada no apunta a la existencia de un enfoque coherente de la priorización del gasto en ciberseguridad por parte de las organizaciones del sistema de las Naciones Unidas, lo que aumenta el riesgo de un uso ineficiente de unos recursos ya de por sí escasos. Para optimizar los gastos en ciberseguridad, así como las inversiones conexas, una evaluación exhaustiva de los ciberriesgos que culmine en un estudio de viabilidad en el que se detallen los costos, los beneficios, los riesgos y los ahorros previstos, y se haga referencia a las posibles consecuencias financieras de no realizar la inversión, es un requisito previo para conseguir el apoyo de los órganos legislativos y rectores y obtener un nivel adecuado de asignación de recursos.

Capacidad interna de expertos en ciberseguridad

Más de la mitad de las organizaciones participantes han creado una capacidad interna de recursos humanos especializados y asignados a fines concretos, que oscilan entre un único experto en seguridad de la información, asignado a veces solo a tiempo parcial, hasta una dependencia organizativa más amplia, dirigida por un jefe de seguridad de la información. Por el contrario, en diez organizaciones participantes las tareas de ciberseguridad las llevan a cabo principalmente los responsables de TIC, compaginándolas con sus otras funciones. En el ámbito de la ciberseguridad se recurre con frecuencia a expertos externos debido a su compleja naturaleza técnica, que evoluciona constantemente y requiere un grado considerable de especialización que resulta difícil y costoso mantener disponible y actualizado de forma permanente. Recurrir a proveedores externos para potenciar y complementar la capacidad interna es inevitable e incluso deseable, para poder seguir respondiendo a la rápida evolución de los acontecimientos novedosos en el ciberespacio. La medida en que se recurre a ellos queda a discreción de cada organización, en función de sus propias necesidades y contexto. Sin embargo, a juicio de los Inspectores, es importante que las organizaciones conserven un grado adecuado de control, supervisión y capacidad técnica a nivel interno para gestionar eficazmente las capacidades aportadas por los proveedores externos e interactuar con ellas. Poder contar con un puesto de jefe de seguridad de la información dedicado a este fin puede proporcionar el enfoque y la garantía necesarios para hacer realidad este propósito. Las funciones principales que recaen bajo la responsabilidad del director de seguridad de la información van más allá de la elaboración de controles a nivel operativo y, por defecto, incluyen una dimensión de gestión para garantizar que se incorporan de la forma más completa posible las consideraciones de ciberseguridad como una cuestión de gestión de los riesgos y la resiliencia de la organización.

Tomando nota de las disparidades en la configuración interna observadas en las organizaciones participantes, que pueden ser más indicativas de las limitaciones a las que se enfrentan que de una elección deliberada o estratégica, los Inspectores creen que disponer de conocimientos especializados sobre ciberseguridad a nivel interno contribuye a reforzar la posición de la organización, pero también del sistema en su conjunto, y es una inversión que merece la pena tener en cuenta. Además, sería prudente que cada organización evaluara si podría salir ganando en caso de procurar crear un centro de operaciones de seguridad, incluso en su forma más rudimentaria, que debería basarse en un análisis coste-beneficio específico para la organización que incluya parámetros como la complejidad de la configuración de la infraestructura de las TIC de la organización, el número y el tipo de activos y procesos críticos gestionados, el volumen global de los flujos de datos y, por tanto, la frecuencia de las amenazas, y otros factores. Uno de los aspectos importantes de un centro de operaciones de seguridad formal, independientemente de su tamaño y capacidad, es el enfoque que proporciona a la hora de supervisar las operaciones a diario y de desempeñar un papel crucial de coordinación y sincronización, así como para mejorar la concienciación de la organización, lo que puede constituir un cambio significativo en lo que hace a una asignación eficiente de los recursos y capacidades a nivel interno.

Ciberseguridad: ¿una prioridad para todo el sistema?

A lo largo de los años, tanto los Estados Miembros como la dirección ejecutiva han declarado prioritario el fortalecimiento de la posición de ciberseguridad del sistema de las Naciones Unidas mediante una mayor coordinación y colaboración entre las organizaciones a nivel estratégico y una mejor capacidad operativa en todo el sistema. No obstante, a pesar de la existencia de los diversos recursos, mecanismos e iniciativas importantes de que se dispone dentro del sistema, incluida la evidente voluntad política, los avances a la hora de hacer realidad estas aspiraciones declaradas no están tan claros. A fecha de hoy, no existe ninguna entidad encargada oficialmente de impulsar la agenda de un enfoque armonizado en materia de ciberseguridad, y los esfuerzos de ciberseguridad de todo el sistema se concentran institucionalmente en torno a los mecanismos de coordinación interinstitucional en el marco de la Junta de los Jefes Ejecutivos del Sistema

de las Naciones Unidas para la Coordinación, contando con el apoyo operativo, en cierta medida, del Centro Internacional de Cálculos Electrónicos de las Naciones Unidas como proveedor de servicios compartidos de ciberseguridad para varias organizaciones del sistema de las Naciones Unidas. En el presente examen, los Inspectores constataron que no había suficientes vínculos entre la dirección estratégica a nivel de todo el sistema y la capacidad operacional, lo que había afectado a la dinámica entre esas estructuras y probablemente estaba costando caro al sistema en forma de ganancias de eficiencia no realizadas debido a las oportunidades de colaboración más directa frustradas.

Nivel básico de protección y requisitos mínimos de defensa convenidos que se necesitan

La idea de que una deficiente protección contra las ciberamenazas en una organización hace que todo el sistema sea más vulnerable goza de general aceptación. Por ello, puede decirse que el sistema de las Naciones Unidas es tan fuerte como su eslabón más débil. Sin embargo, las iniciativas anteriores destinadas a introducir puntos de referencia comunes o evaluaciones de madurez comparativas entre las organizaciones no recibieron suficiente apoyo, y los detractores de esas iniciativas adujeron que la diversidad de las configuraciones estructurales y el contexto en el que operaban las organizaciones eran otros tantos obstáculos que limitaban el valor de tales enfoques colectivos o acumulativos. Además, las organizaciones participantes mostraron escaso interés, en los niveles superiores, por compartir su información interna sobre ciberseguridad, por razones de confidencialidad y por la preocupación que suscitaba dejar al descubierto las propias vulnerabilidades incluso entre las organizaciones. Estas preocupaciones podrían mitigarse mediante acuerdos de intercambio de información, que podrían ofrecer las salvaguardias adecuadas. Sin embargo, los intentos de instituir una capacidad operativa en todo el sistema para prevenir y detectar las ciberamenazas y responder a ellas aún no han dado resultados tangibles. Algunas de las lagunas a este respecto han sido cubiertas por el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas, cuya gama de servicios de ciberseguridad ha atraído a una considerable cartera de clientes, si bien de forma voluntaria, por lo que solo satisface parcialmente las necesidades del sistema. A pesar del escaso éxito que han tenido hasta la fecha los esfuerzos de todo el sistema por adoptar un enfoque común o concertado, ya sea a nivel conceptual u operacional, los Inspectores consideran que la fijación de un nivel básico de protección y de unos requisitos mínimos de defensa para las organizaciones de las Naciones Unidas, y por tanto para el sistema en su conjunto, continúa siendo un objetivo válido que sigue mereciendo la pena tratar de hacer realidad.

Mecanismos interinstitucionales de ciberseguridad

El mecanismo interinstitucional que se ocupa de la ciberseguridad está en pie desde hace tiempo y funciona en general, aunque algunos de los ambiciosos objetivos que se había fijado aún no se han traducido en resultados tangibles más allá del sólido nivel de intercambio de información y de profesionales a nivel de todo el sistema que ha propiciado. Los registros de la Red Digital y Tecnológica y del Comité de Alto Nivel sobre Gestión demuestran que, durante un período de al menos 30 años, la ciberseguridad ha figurado bastante alto en la agenda de todo el sistema. Desde 2011, el Grupo de Interés Especial sobre la Seguridad de la Información, que funciona en el marco de la Red Digital y Tecnológica, ha sido el principal mecanismo para promover la cooperación y la colaboración interinstitucionales con el fin de optimizar la seguridad de la información en el seno de las organizaciones que lo componen. Según su mandato, su objetivo principal es compartir conocimientos, aunque, tras la revisión de dicho mandato en 2018, también se hace hincapié en su papel a la hora de emprender proyectos conjuntos, una aspiración que se amplió con el llamamiento de su Red matriz para que el Grupo de Interés Especial sobre la Seguridad de la Información pasase a ser más activo en el diseño y entrega de soluciones e innovación compartidas. Reconociendo la credibilidad profesional y el considerable volumen de trabajo producido por el Grupo a lo largo de los años, los Inspectores constataron que las soluciones compartidas a gran escala para el sistema no se habían aplicado tal y como estaba previsto en el mandato. Como órgano de coordinación,

el Grupo de Interés Especial sobre la Seguridad de la Información se enfrenta a los mismos retos en este sentido que cualquier otro mecanismo interinstitucional, al carecer de autoridad para tomar decisiones que obliguen a actuar directamente a nivel del sistema, por lo que no sería realista esperar que la aplicación se materializara en el seno de ese foro. La repercusión del Grupo de Interés Especial sobre la Seguridad de la Información se ve en cierto modo limitada por su dependencia del compromiso individual y el seguimiento de las organizaciones que agrupa, por la desigual capacitación de sus miembros dentro de su propia arquitectura institucional y por el hecho de que el Grupo no tiene capacidad operativa para aplicar los acuerdos alcanzados o las recomendaciones formuladas. Además, el Grupo depende de la Red Digital y Tecnológica, lo que es reflejo de la configuración predominante observada en la mayoría de las organizaciones, en la que el responsable de la seguridad de la información depende del jefe o jefa de su respectivo departamento de TIC, con todas las ventajas y limitaciones que dicha configuración implica.

El Centro Internacional de Cálculos Electrónicos de las Naciones Unidas, proveedor esencial de servicios de ciberseguridad para el sistema

El Centro Internacional de Cálculos Electrónicos de las Naciones Unidas lleva varios años prestando servicios de ciberseguridad a unos dos tercios de las organizaciones del sistema de las Naciones Unidas, aunque la base de clientes de cada uno de sus 13 servicios conexos varía mucho. Esta área de su catálogo de servicios, la ciberseguridad, ha experimentado un crecimiento considerable y diverso, aunque sigue representando solo una mínima parte de la actividad del Centro en términos presupuestarios. La evaluación de los servicios de ciberseguridad del Centro Internacional de Cálculos Electrónicos de las Naciones Unidas se consideró desigual entre las organizaciones participantes, reconociéndose que el Common Secure Threat Intelligence es su servicio estrella. Ya en 2019, la Dependencia Común de Inspección abogó por un mejor aprovechamiento del potencial no realizado del Centro, específicamente en lo que respecta a sus servicios en el ámbito de la ciberseguridad. Se alienta a las organizaciones del sistema de las Naciones Unidas y al Centro a encontrar más puntos en común para complementar las capacidades internas existentes de las organizaciones con más servicios compartidos. En este sentido, se invita a los jefes ejecutivos de las organizaciones participantes a que reconsideren los actuales acuerdos institucionales y vuelvan a valorar las posibilidades de utilizar los servicios de ciberseguridad del Centro. Como entidad interinstitucional que opera bajo las normas y el marco administrativo de la Organización Mundial de la Salud, el modelo institucional del Centro Internacional de Cálculos Electrónicos de las Naciones Unidas se basa en un esquema de recuperación de costos y de servicios compartidos. Esta combinación ha resultado ser a la vez un factor de apoyo y un obstáculo para que el Centro se convierta en el centro neurálgico de la ciberseguridad de todo el sistema. Ha creado una situación en la que la oferta de servicios del Centro Internacional de Cálculos Electrónicos de las Naciones Unidas depende de que los clientes aporten una financiación inicial para sufragar los costos de desarrollo de un nuevo servicio con el que satisfacer la demanda, mientras que muchos solo pueden permitirse comprar el servicio así desarrollado una vez que una masa crítica de clientes ya se ha suscrito a él. Teniendo en cuenta los retos que impone la ciberseguridad y los riesgos a los que se enfrentan las organizaciones, se consideró oportuno explorar el uso de contribuciones voluntarias como mecanismo de financiación complementario para proporcionar recursos más directos a fin de preservar la posición general de ciberseguridad del sistema. Los Inspectores consideran que el establecimiento de un fondo fiduciario para complementar los mecanismos de financiación existentes mediante contribuciones voluntarias destinadas a soluciones de ciberseguridad compartidas que sirvan al sistema podría convertirse en un factor de cambio radical a la hora de abordar algunos de los obstáculos a este respecto. El fondo fiduciario no solo permitiría a los Estados Miembros que lo desearan contribuir directamente a las mejoras de la ciberseguridad en todo el sistema, sino que también brindaría la oportunidad, mediante un mecanismo de gobernanza del fondo que sería concebido por los interlocutores pertinentes, de mejorar los vínculos entre la dirección estratégica que puede proporcionar el Grupo de Interés Especial sobre la Seguridad de la Información y la capacidad operativa que ofrece el Centro Internacional de Cálculos

Electrónicos de las Naciones Unidas (recomendación 3). Se invita a la Asamblea General a que tome nota de la recomendación y a que anime a los donantes a contribuir al fondo fiduciario (recomendación 4).

Hacia una mayor armonización de las consideraciones de seguridad física y ciberseguridad

Es bien sabido que el Departamento de Seguridad tiene un mandato a nivel de todo el sistema para establecer la política y orientar las disposiciones operativas en la esfera de la seguridad y protección en todas las entidades a nivel mundial. A pesar de la convergencia entre el espacio físico y el ciberespacio cuando se trata de proteger al personal y los activos de la organización, el mandato del Departamento de Seguridad, tal como fue otorgado por la Asamblea General, se centra en las amenazas concretas a la seguridad y la protección que son de su competencia y, por lo tanto, no contiene ninguna referencia explícita a la ciberseguridad o a la ciberdimensión de los riesgos y amenazas. Es evidente que la necesidad de una mayor armonización entre la seguridad física y la ciberseguridad ha inspirado el debate en varios organismos interinstitucionales durante años, pero ello todavía tiene que madurar antes de arrojar conclusiones aplicables al sistema. Para ayudar a ver más claros las oportunidades y los riesgos asociados a la ampliación al ámbito cibernético del enfoque basado en los riesgos y la respuesta estructurada y centrada en la rendición de cuentas en que se basa el sistema de gestión de la seguridad de las Naciones Unidas, los Inspectores recomiendan que el Secretario General presente un informe a la Asamblea General, en el que se destaque la forma en que puede aprovecharse una protección más holística del personal y los bienes de las Naciones Unidas y se indiquen las medidas necesarias para fortalecer las estructuras existentes consiguientemente, prestando especial atención a la función del Departamento de Seguridad a este respecto. El informe debería basarse en los resultados de las consultas entre los mecanismos de coordinación interinstitucional pertinentes que se ocupan de la ciberseguridad y la Red Interinstitucional de Gestión de la Seguridad, con aportaciones del Centro Internacional de Cálculos Electrónicos de las Naciones Unidas, según proceda (recomendación 5).

Recomendaciones

Recomendación 1

Los jefes ejecutivos de las organizaciones del sistema de las Naciones Unidas deberían preparar, con carácter prioritario y a más tardar en 2022, un informe completo sobre su marco de ciberseguridad que abarque los elementos que contribuyen a mejorar la ciberresiliencia examinados en el presente informe, y presentarlo a sus respectivos órganos legislativos y rectores a la mayor brevedad posible.

Recomendación 2

Los órganos legislativos y rectores de las organizaciones del sistema de las Naciones Unidas deberían examinar los informes sobre los elementos que contribuyen a mejorar la ciberresiliencia preparados por los jefes ejecutivos y, cuando sea necesario, proporcionar orientación estratégica sobre las nuevas mejoras que deban llevarse a cabo en sus respectivas organizaciones.

Recomendación 3

La Dirección del Centro Internacional de Cálculos Electrónicos debería tratar de establecer, a más tardar a finales de 2022, un fondo fiduciario que recogería las contribuciones de los donantes con el fin de complementar la capacidad del CICE para diseñar, desarrollar y ofrecer servicios y soluciones compartidos que mejoren la posición de ciberseguridad de las organizaciones del sistema de las Naciones Unidas.

Recomendación 4

La Asamblea General de las Naciones Unidas debería, a más tardar en su septuagésimo séptimo período de sesiones, tomar nota de la recomendación dirigida a la Dirección del Centro Internacional de Cálculos Electrónicos de establecer un fondo fiduciario destinado al desarrollo de soluciones compartidas de ciberseguridad e invitar a los Estados Miembros que deseen reforzar la posición de ciberseguridad de las organizaciones del sistema de las Naciones Unidas a que contribuyan a dicho fondo.

Recomendación 5

El Secretario General debería presentar a la Asamblea General de las Naciones Unidas, a más tardar en su septuagésimo octavo período de sesiones, un informe en el que se estudien nuevas oportunidades para aprovechar la convergencia entre la seguridad física y la ciberseguridad a fin de garantizar una protección más holística del personal y los bienes de las Naciones Unidas y se indiquen las medidas necesarias para reforzar de forma acorde las estructuras existentes, prestando especial atención a la posible función del Departamento de Seguridad a este respecto.

Estas recomendaciones formales se complementan con 35 recomendaciones oficiosas o indicativas, señaladas en negrita en el cuerpo del presente informe, como propuestas adicionales que, en opinión de los Inspectores, podrían mejorar la posición de ciberseguridad del sistema de las Naciones Unidas.

Índice

Abreviaturas

ACNUR	Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados
CICE	Centro Internacional de Cálculos Electrónicos de las Naciones Unidas
DCI	Dependencia Común de Inspección
FAO	Organización de las Naciones Unidas para la Agricultura y la Alimentación
ISO	Organización Internacional de Normalización
JJE	Junta de Jefes Ejecutivos del Sistema de las Naciones Unidas para la Coordinación
OACI	Organización de Aviación Civil Internacional
OIEA	Organismo Internacional de la Energía Atómica
OIT	Organización Internacional del Trabajo
OMI	Organización Marítima Internacional
OMM	Organización Meteorológica Mundial
OMPI	Organización Mundial de la Propiedad Intelectual
OMS	Organización Mundial de la Salud
OMT	Organización Mundial del Turismo
ONU-Mujeres	Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de la Mujer
ONUSIDA	Programa Conjunto de las Naciones Unidas sobre el VIH/sida
OOPS	Organismo de Obras Públicas y Socorro de las Naciones Unidas para los Refugiados de Palestina en el Cercano Oriente
PMA	Programa Mundial de Alimentos
PNUD	Programa de las Naciones Unidas para el Desarrollo
PNUMA	Programa de las Naciones Unidas para el Medio Ambiente
TIC	tecnologías de la información y las comunicaciones
UIT	Unión Internacional de Telecomunicaciones
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
UNFPA	Fondo de Población de las Naciones Unidas
UNICEF	Fondo de las Naciones Unidas para la Infancia
UNODC	Oficina de las Naciones Unidas contra la Droga y el Delito
UNOPS	Oficina de las Naciones Unidas de Servicios para Proyectos

I. Introducción

A. Contexto

1. **Importancia de la ciberseguridad en la era digital.** En el mundo digitalizado de hoy, la ciberseguridad se ha convertido en una cuestión de importancia para las organizaciones internacionales, y las organizaciones del sistema de las Naciones Unidas no son una excepción. La transformación digital, la creciente dependencia de las tecnologías de la información y las comunicaciones (TIC) y las soluciones cibernéticas, y el hecho de que las amenazas a la ciberseguridad crezcan constantemente, tanto en sofisticación como en potencial de disrupción, se han traducido en un aumento sin precedentes de los riesgos de ciberseguridad a los que se enfrentan las organizaciones del sistema de las Naciones Unidas. Los incidentes que antes se consideraban extraordinarios son cada vez más frecuentes y comunes. Los Inspectores recuerdan una carta dirigida al Secretario General en 2017, en la que los representantes de los comités de supervisión del sistema de las Naciones Unidas, con ocasión de su primera reunión conjunta, señalaron entre las tres preocupaciones fundamentales para las organizaciones del sistema de las Naciones Unidas la necesidad de que la administración preste la debida atención a los riesgos nuevos y emergentes, en particular a las amenazas mundiales e institucionales críticas que enfrenta la ciberseguridad, y los riesgos que surgen de las nuevas modalidades de trabajo a medida que la transformación digital cobra impulso[1]. Con este telón de fondo, las organizaciones participantes en la Dependencia Común de Inspección (DCI) apoyaron un examen de la DCI sobre las políticas y prácticas de ciberseguridad vigentes en el sistema de las Naciones Unidas, que la DCI llevó a cabo en el marco de su programa de trabajo para 2020 y que representa el último de una serie de exámenes de temática tecnológica sobre cuestiones como la gobernanza de las TIC, la gestión de los sitios web de Internet y el uso de los servicios de computación en la nube[2].

2. **El sistema de las Naciones Unidas como objetivo de los ciberataques.** Vistas en su conjunto, las amenazas a la ciberseguridad a las que se enfrentan las organizaciones del sistema de las Naciones Unidas no difieren de las que afectan a otras entidades, en el sentido de que los instigadores, los medios y los objetivos de los ataques —que van de lo financiero a lo simbólico— son los mismos. Una distinción, de haberla, puede detectarse en la forma en que las Naciones Unidas pueden ser consideradas un objetivo preferente frente a otras entidades de los sectores privado y público. Por un lado, el atractivo puede residir en la gran visibilidad y el alcance mundial de las entidades del sistema de las Naciones Unidas, que las convierte en un objetivo de más lucimiento para los jáquers en busca de fama, si se compara con la publicidad que se obtiene al atacar a cualquier gobierno nacional o entidad del sector público. Además, a diferencia de muchos objetivos del sector privado, también pueden ser más atractivos para los "hacktivistas" que se guían por motivos ideológicos y protestan o se oponen a los valores que las organizaciones del sistema de las Naciones Unidas defienden o propugnan. Debido al entorno intergubernamental en el que operan las organizaciones, también existe una innegable dimensión política, que las propias organizaciones solo insinúan pero que, sin excepción, se da por hecho. En resumen, aunque los métodos de los ataques son idénticos, los motivos pueden ser diferentes. Lo que está claro es que se ha producido un aumento exponencial de los ataques, grandes y pequeños, contra las organizaciones participantes en la DCI en los últimos cinco años, como demuestran las cifras consultadas por los Inspectores a partir de diversas fuentes.

3. **Los incidentes de ciberseguridad trascienden la mera interrupción del sistema y pueden afectar a la ejecución del mandato.** Para las organizaciones del sistema de las Naciones Unidas, las posibles consecuencias de una posición débil en materia de ciberseguridad van más allá de la mera interrupción de la capacidad de procesamiento administrativo y de la infraestructura y los sistemas de TIC, y no deben medirse únicamente en función del volumen de la información y los datos que acaban por quedar expuestos. Una

[1] Carta dirigida al Secretario General el 26 de enero de 2017.

[2] JIU/REP/2008/5; JIU/REP/2008/6; JIU/REP/2011/9 y JIU/REP/2019/5.

sola brecha de seguridad puede ser devastadora para la organización si afecta a datos sensibles como la información de identificación personal, los registros médicos del personal, los datos de propiedad intelectual y los archivos históricos y políticos o similares. Además, está en juego la capacidad de las organizaciones para cumplir sus mandatos, así como su credibilidad ante los Estados miembros y beneficiarios. En el ámbito en el que operan estas organizaciones, incluso los incidentes tecnológicamente menores pueden producir efectos dominantes que podrían interferir con los procesos diplomáticos e intergubernamentales, las intervenciones humanitarias o, en el peor de los casos, incluso la paz y la seguridad internacionales. Aunque los ciberataques pueden afectar de forma diferente a organizaciones del sistema de las Naciones Unidas con mandatos y estructuras diversas, la amenaza es real y compartida[3]. Ninguna organización está a salvo de experimentar alguna vez un incidente de ciberseguridad, independientemente de su nivel de preparación y vigilancia. Sin embargo, el impacto en la reputación y las repercusiones operacionales, jurídicas y financieras pueden ser considerables si se desdeñan los riesgos.

4. **Reconocimiento por la comunidad internacional y las Naciones Unidas de la importancia de la ciberseguridad.** El entendimiento de que las actividades hostiles en el ciberespacio suponen una amenaza tanto para la comunidad internacional como para las organizaciones de las Naciones Unidas más concretamente ha quedado documentado en las resoluciones e informes de los órganos legislativos y de gobierno pertinentes y en los mecanismos de coordinación interna, al menos desde principios del decenio de 1990. El debate de fondo sobre la cuestión se ha celebrado en vías paralelas. Por un lado, se acomete entre los gobiernos, en su condición de miembros de los órganos legislativos y rectores de las Naciones Unidas que elaboran la respuesta mundial a la aparición de la ciberdelincuencia y las ciberamenazas (la dimensión "hacia el exterior" de la labor de las Naciones Unidas en materia de ciberseguridad, cuya competencia de coordinación a nivel de todo el sistema recae en el Comité de Alto Nivel sobre Programas de la Junta de los Jefes Ejecutivos del Sistema de las Naciones Unidas para la Coordinación (JJE)), y, por otro lado, se entabla también entre las organizaciones del sistema de las Naciones Unidas que buscan fortalecer su preparación y respuesta corporativa interna a los desafíos conexos, tanto colectiva como individualmente (la dimensión "interna", que corresponde al Comité de Alto Nivel sobre Gestión). El reconocimiento de la doble función del sistema de las Naciones Unidas a este respecto queda de manifiesto en una declaración final realizada por el Secretario General en el contexto de la JJE en fecha tan reciente como 2019, en la que se afirma la "necesidad de que el sistema de las Naciones Unidas asuma un papel de liderazgo y elabore una posición unificada sobre la ciberseguridad y las amenazas conexas, al tiempo que sirva de plataforma de convocatoria para que los Estados Miembros y otras partes interesadas debatan sobre la ciberseguridad en sus diversas dimensiones"[4].

5. **La responsabilidad de los Estados de proteger los activos de las Naciones Unidas incluye los activos digitales en el ciberespacio.** En lo que respecta a las protecciones legales en relación con la ciberseguridad, las organizaciones del sistema de las Naciones Unidas se basan en los privilegios e inmunidades que se aplican a sus propiedades, activos, archivos, documentos y comunicaciones en general[5]. La existencia de esos privilegios e inmunidades obliga a los Estados partes a estar en condiciones, con arreglo a sus respectivas leyes, de proporcionar la protección y la seguridad necesarias para el cumplimiento de los fines de la entidad que goza de esos privilegios e inmunidades, y a garantizar, en particular, la inviolabilidad de los locales, archivos y documentos, "dondequiera que se encuentren y quienquiera los tenga en su poder". En otras palabras, los Estados, y en particular los países anfitriones, tienen el deber de proteger a las organizaciones de ataques hostiles, ya sea en el

[3] Para obtener información de antecedentes sobre los retos a los que se enfrentan las organizaciones del sistema de las Naciones Unidas, véase el folleto *Cascos azules digitales de las Naciones Unidas*, elaborado por la Oficina de Tecnología de la Información y las Comunicaciones de las Naciones Unidas.

[4] CEB/2019/2, párr. 39.

[5] El Artículo 105 de la Carta de las Naciones Unidas; la Convención sobre Prerrogativas e Inmunidades de las Naciones Unidas, de 13 de febrero de 1946; la Convención sobre los Privilegios e Inmunidades de los Organismos Especializados, de 21 de noviembre de 1947; y el Acuerdo sobre Privilegios e Inmunidades del Organismo Internacional de Energía Atómica, de 17 de agosto de 1959.

entorno físico como en la esfera digital. Esta interpretación fue confirmada a los Inspectores por la Oficina de Asuntos Jurídicos y resuelve la cuestión de si los datos electrónicos y los activos digitales están cubiertos por las disposiciones legales existentes. De hecho, en los acuerdos más recientes sobre sedes y países anfitriones celebrados bilateralmente entre las organizaciones y los Estados que las acogen en su territorio, la Oficina de Asuntos Jurídicos indicó que se había definido expresamente que el término "archivos" incluía los mensajes de correo electrónico y los registros informáticos, así como cualquier otro material similar que perteneciera a la organización en cuestión o estuviera en su poder para el desempeño de su función. Asimismo, se ha considerado que la comunicación protegida incluye las comunicaciones electrónicas de datos, mientras que otros acuerdos han previsto más ampliamente la inviolabilidad de cualquiera de los medios de comunicación empleados. En su sentido más lato, esto significa que los Estados tienen la responsabilidad, en virtud del derecho internacional, de proteger los bienes de las Naciones Unidas, incluso en el ciberespacio.

6. **Evolución desde las TIC hacia una perspectiva más amplia.** Tradicionalmente, las consideraciones de ciberseguridad surgieron y se trataron por primera vez en el ámbito de las TIC, que, en los primeros tiempos de la informática, ocupaban un papel menos destacado en las actividades institucionales que en la actualidad. Esta concepción de la ciberseguridad como disciplina centrada en las TIC era el producto lógico de una época en la que las amenazas se limitaban principalmente a la infraestructura informática y afectaban a un conjunto mucho más reducido de activos de información y procesos institucionales. Sin embargo, ahora que las TIC están profundamente imbricadas en la mayoría de las actividades institucionales, y que el panorama de las amenazas ha evolucionado considerablemente rebasando las meras interrupciones técnicas que requieren parches más sencillos y defensas de base tecnológica, ya no parece viable contemplar la ciberseguridad únicamente a través de la lente restrictiva de las TIC. **De hecho, los Inspectores consideran que la ciberseguridad debe enmarcarse en una perspectiva mucho más amplia que incluya varios ámbitos y competencias organizativas, como la gestión del riesgo institucional, la seguridad e integridad físicas, la protección de datos y la privacidad, los conocimientos jurídicos de expertos y la seguridad de la información en el contexto más amplio de la gestión de la información y el conocimiento.**

7. **La planificación de la continuidad de la actividad, clave para un enfoque de la ciberseguridad basado en el riesgo.** Algunas organizaciones ya han empezado a adoptar el concepto de gestión de la resiliencia organizativa, que incluye la ciberseguridad como un aspecto más. La preocupación central de este ámbito de la resiliencia organizativa es evaluar adecuadamente los ciberriesgos con miras a adoptar medidas preventivas, de mitigación de riesgos y de defensa contra las amenazas, por un lado, e introducir protocolos adecuados para orientar las medidas y preservar la continuidad de la actividad en caso de que dichos riesgos y amenazas se materialicen, por otro. La mitigación de riesgos en el ámbito de la ciberseguridad nunca es absoluta, sino más bien una cuestión de grado, y su eficacia debe juzgarse no solo por su éxito a la hora de evitar las amenazas, sino también por la medida en que puede ayudar a restablecer las operaciones después de un ataque exitoso. Por tanto, cuando se producen incidentes graves, es esencial contar con un procedimiento de recuperación de desastres debidamente ensayado para todos los sistemas de información en funcionamiento. Esto solo puede lograrse si los protocolos de recuperación se ensayan periódica y rigurosamente como parte de la planificación regular de la continuidad de la actividad, empleando, de ser posible, pruebas de penetración, que son una poderosa herramienta de la gestión de riesgos. Aunque los procedimientos de recuperación tras desastres informáticos tienen un fuerte componente técnico, deben desarrollarse dentro de los parámetros estratégicos establecidos por la dirección de la organización (incluyendo la tolerancia frente a riegos y la voluntad de asumirlos, los recursos disponibles, etc.) y las limitaciones operativas establecidas (como el tiempo de recuperación aceptable) para que sean eficaces. En consecuencia, la planificación de la continuidad de la actividad, junto con

la gestión de riesgos, se convierte en un pilar indispensable de la resistencia de la organización frente tanto a las amenazas físicas como a las ciberamenazas[6].

B. Objetivos, alcance y metodología

Objetivos

8. Los principales objetivos al realizar la presente revisión son:

a) Identificar y analizar los retos y riesgos comunes en materia de ciberseguridad a los que se enfrentan las organizaciones del sistema de las Naciones Unidas y su respectiva respuesta a los mismos, teniendo en cuenta los puntos comunes y las diferencias pertinentes en los requisitos específicos propios del contexto de las organizaciones y la habilidad para proteger sus activos clave, y manteniendo al mismo tiempo su capacidad de cumplir sus mandatos; y

b) Inventariar los acuerdos interinstitucionales actuales y examinar si son eficaces para facilitar un enfoque de la ciberseguridad a nivel de todo el sistema, así como determinar oportunidades para mejorar la coordinación, la colaboración y el intercambio de información entre las organizaciones del sistema de las Naciones Unidas, cuando proceda.

Alcance

9. **Cobertura de todo el sistema.** El presente examen se realizó a nivel de todo el sistema e incluyó a todas las organizaciones participantes en la DCI, a saber, la Secretaría de las Naciones Unidas, sus departamentos y oficinas, los fondos y programas de las Naciones Unidas, otros órganos y entidades de las Naciones Unidas, los organismos especializados de las Naciones Unidas y el Organismo Internacional de Energía Atómica (OIEA). El Centro de Comercio Internacional no participó en el proceso de examen y, por tanto, no figura en las cifras desglosadas que se incluyen en el presente informe. Además, la DCI examinó el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas (CICE), teniendo en cuenta su función en lo relativo a prestar servicios de ciberseguridad a varias organizaciones del sistema de las Naciones Unidas.

10. **Enfoque centrado en los acuerdos internos de ciberseguridad.** El presente informe se centra en los acuerdos institucionales relativos a la gestión de los marcos de ciberseguridad dentro de las organizaciones del sistema de las Naciones Unidas, que están concebidos para proteger sus activos en el ciberespacio y permitir la realización de las actividades previstas en su mandato (la dimensión "hacia el interior" de la ciberseguridad)[7]. La labor intergubernamental del sistema de las Naciones Unidas en apoyo de los Estados Miembros, en particular mediante la asistencia técnica para crear capacidad nacional en materia de ciberseguridad o combatir la ciberdelincuencia, se describe en el anexo I para dar contexto, pero no fue el objeto central del presente examen. En el anexo se incluye una breve reseña histórica de cómo se ha desarrollado la cuestión en el marco de las distintas líneas de trabajo de la Asamblea General y otros órganos intergubernamentales.

11. **Aspectos técnicos no evaluados en detalle.** Aunque no es una cuestión puramente tecnológica, la ciberseguridad no puede abordarse sin hacer referencia a su dimensión TIC. Sin embargo, los Inspectores no intentaron analizar en profundidad las medidas aplicadas por las organizaciones en cuanto a su pertinencia o solidez tecnológica. Para su examen de las consideraciones técnicas que resultaron indispensables para que el presente informe fuera completo, los Inspectores aprovecharon conocimientos de expertos externos y se limitaron a destacar determinadas áreas para su consideración y posible examen posterior. En particular, no pretenden ofrecer en el presente informe una evaluación exhaustiva, comparativa o no, de la madurez de cada organización del sistema de las Naciones Unidas. Se consideró que una

[6] El programa de trabajo de la DCI para 2021 incluye un examen específico sobre la continuidad de las actividades.

[7] El presente informe se complementa con una carta sobre asuntos de gestión dirigida a los jefes ejecutivos de las organizaciones participantes en la DCI que se centra en los riesgos asociados a la salvaguardia y protección de los documentos y datos jurídicos, normativos, administrativos, políticos e históricos de las organizaciones (JIU/ML/2021/1).

evaluación de este tipo trascendía el alcance del informe, pero también que tenía una utilidad limitada para las organizaciones en cuestión, tanto colectiva o individualmente.

12. **Ámbitos relacionados con los datos que son relevantes para la ciberseguridad pero que quedan fuera del alcance del presente estudio.** Diversos ámbitos de la gestión del conocimiento y de la información, así como de la protección de los datos, la privacidad y otros ámbitos afines, se entrecruzan con la ciberseguridad, pero exceden el alcance del presente estudio. Algunos ya han sido objeto de informes de la DCI (por ejemplo, la clasificación de la información como un subtema de la gestión de expedientes y archivos)[8], mientras que otros se están articulando a nivel de las organizaciones a título individual basándose en la orientación a nivel de todo el sistema (por ejemplo, la traducción de los Principios de Protección de Datos Personales y Privacidad, adoptados por la JJE en 2018, en políticas organizativas y publicaciones administrativas). Además, los desafíos y complejidades asociados a la introducción, en el mismo año, del Reglamento General de Protección de Datos Europeo y los intentos de aplicarlo en relación con las organizaciones del sistema de las Naciones Unidas presentan un conjunto separado de cuestiones con implicaciones para la ciberseguridad que exceden el alcance del presente estudio. Lejos de representar una lista exhaustiva, estas cuestiones ilustran el amplio alcance de la ciberseguridad como ámbito transversal que solo pudo ser abordado de manera somera en este informe. **No obstante, los Inspectores desean señalar que, en particular, el ámbito de la protección de datos y la privacidad de la información personal es una cuestión de gran actualidad y que preocupa mucho, y que sería oportuno y justificado realizar un examen crítico específico de las políticas y prácticas de las organizaciones del sistema de las Naciones Unidas a este respecto.**

Metodología

13. De conformidad con las normas internas y los procedimientos de trabajo de la DCI, los Inspectores utilizaron una serie de métodos de recopilación de datos cualitativos y cuantitativos procedentes de distintas fuentes para garantizar la coherencia, la validez y la fiabilidad de sus conclusiones. La información utilizada en la preparación del presente informe estaba actualizada a fecha de mayo de 2021:

- **Cuestionarios y estudio documental.** La DCI recopiló información mediante dos cuestionarios dirigidos a sus organizaciones participantes. Los Inspectores examinaron los componentes pertinentes de los marcos normativos aplicables (resoluciones de los órganos rectores, estrategias institucionales en materia de TIC y políticas específicas y documentos de orientación sobre procedimientos en materia de seguridad de la información y ciberseguridad, si existían) y consultaron los informes de los órganos de supervisión internos y externos. Varias rondas de consultas al CICE permitieron realizar un examen crítico de su mandato, catálogo de servicios y capacidad institucional y operativa en el ámbito de la ciberseguridad. La Oficina de Asuntos Jurídicos proporcionó aclaraciones por escrito sobre una serie de aspectos legales. El análisis de los informes de los comités y redes de la JJE, principalmente la Red Digital y Tecnológica y su Grupo de Interés Especial sobre la Seguridad de la Información, sirvió para conocer mejor la dinámica interinstitucional y las iniciativas actuales y pasadas de todo el sistema. Los Inspectores también consultaron las normas pertinentes del sector y la bibliografía relacionada con la ciberseguridad como documentación de referencia.
- **Entrevistas.** Basándose en las respuestas a los cuestionarios, los Inspectores realizaron 45 entrevistas con funcionarios encargados de las TIC, y de la ciberseguridad más específicamente, así como con altos funcionarios para ofrecer una perspectiva más amplia a nivel de la organización. Posteriormente se realizaron entrevistas con representantes de los órganos de supervisión, del Departamento de Seguridad, así como de determinadas organizaciones no participantes. Las entrevistas con el Presidente del Grupo de Interés Especial sobre la Seguridad de la Información y con representantes de la secretaría de la Junta de Jefes Ejecutivos del Sistema de las Naciones Unidas para la Coordinación (JJE) permitieron conocer mejor las iniciativas

[8] JIU/REP/2013/2.

interinstitucionales en materia de ciberseguridad. Las entrevistas con representantes del CICE proporcionaron detalles sobre las capacidades de ciberseguridad que ofrece el Centro. Los Inspectores también asistieron a la Conferencia Common Secure 2020, organizada por el CICE y celebrada virtualmente debido a la actual pandemia de enfermedad por coronavirus (COVID-19), para hacerse una idea de las novedades y los retos actuales que se debaten entre los suscriptores de este servicio del CICE. Además, a través de un grupo de debate, los Inspectores se beneficiaron de las opiniones y la experiencia de varios oficiales jefe de seguridad de la información como miembros de una red mundial informal de gobiernos municipales que se enfrentan a retos similares, a través de la cual conocieron las políticas, las prácticas y las lecciones aprendidas de estas entidades locales, que las Naciones Unidas podían tomar como posible referencia en relación con el sector público.

14. **Limitaciones en cuanto a la disponibilidad y confidencialidad de la información.** Los Inspectores encontraron limitaciones relacionadas principalmente con: a) la disponibilidad de la información (dado que los parámetros sobre incidentes de ciberseguridad no se registraban sistemáticamente o, cuando se registraban, no seguían una metodología comúnmente acordada, lo que también limitaba la comparabilidad de los datos); b) la confidencialidad de los datos sobre amenazas, incidentes y, en particular, medidas de respuesta, ya que las organizaciones consideraban que el hecho de compartir dicha información creaba una exposición innecesaria que identificaba y revelaba las vulnerabilidades de sus infraestructuras de seguridad, razón por la cual la información se presentaba principalmente sin desglosar en el texto del informe, sin atribución a entidades específicas a menos que ello se justificara caso por caso, y c) la repercusión de la pandemia de COVID-19 en el proceso de recopilación de datos, que provocó retrasos y obligó a realizar las entrevistas exclusivamente por videoconferencia, lo que podría haber incidido en las posibilidades de acceso de algunos interlocutores, así como su disposición a compartir información sensible que, de otro modo, podría haberse obtenido mediante interacciones personales. Además, aunque los Inspectores trataron de estudiar y reflejar cómo las respuestas de las organizaciones participantes a la pandemia habían sido determinantes para las consideraciones de ciberseguridad, algunas disposiciones y medidas aplicadas en ese contexto podrían haber evolucionado más y, por lo tanto, no haberse tenido plenamente en cuenta durante el proceso de examen.

15. **Agradecimientos.** Los Inspectores desean expresar su agradecimiento a todos los funcionarios de las organizaciones del sistema de las Naciones Unidas y a los representantes de otras organizaciones que colaboraron en la preparación del presente informe, en particular a los que participaron en las entrevistas y compartieron de buen grado sus saberes y conocimientos expertos. Con el fin de garantizar la calidad, se utilizó un método interno de revisión por pares para solicitar las observaciones de los Inspectores de la DCI sobre el proyecto de informe, que posteriormente se distribuyó a las organizaciones interesadas para que formularan observaciones de fondo sobre los resultados, las conclusiones y las recomendaciones, así como para que corrigieran cualquier dato factual erróneo.

16. **Recomendaciones.** El presente informe contiene cinco recomendaciones oficiales, de las cuales una está dirigida a la Asamblea General, otra a los órganos legislativos y rectores, una tercera a los jefes ejecutivos de las organizaciones participantes en la DCI, la cuarta al Secretario General y una quinta al Director del CICE. Para facilitar la tramitación del presente informe y la aplicación de sus recomendaciones y su seguimiento, en el anexo X figura un cuadro en el que se indica si el informe se ha presentado a las organizaciones pertinentes para que adopten medidas o solo a título informativo y se especifica si las recomendaciones requieren la adopción de medidas por parte de los órganos legislativos y rectores de las organizaciones o de los jefes ejecutivos. Las recomendaciones formales se complementan con 35 recomendaciones oficiosas indicadas en negrita, como sugerencias adicionales que, a juicio de los Inspectores, podrían mejorar la posición de ciberseguridad del sistema de las Naciones Unidas.

C. Definiciones

17. **Ausencia de una definición de ciberseguridad universalmente aceptada.** Las normas del sector internacionales y nacionales sobre seguridad de la información suelen incluir una definición de ciberseguridad. Sin embargo, no existe una definición universalmente aceptada ni un consenso mundial sobre lo que abarca exactamente el término. En el contexto de las Naciones Unidas, los Inspectores observaron que ni había una orientación a nivel de todo el sistema por parte de los foros interinstitucionales pertinentes que recomendara unánimemente una definición concreta como autorizada para el sistema[9], ni los propios marcos normativos de las organizaciones trataban sistemáticamente de imponer una definición de ciberseguridad. En el presente informe, los Inspectores decidieron utilizar la definición de ciberseguridad elaborada por la Unión Internacional de Telecomunicaciones (UIT), que se reproduce en el recuadro 1. La gran mayoría de las organizaciones participantes en la DCI confirmaron que la definición reflejaba su enfoque de la cuestión, a menudo complementado por su uso de las normas pertinentes del sector como referencia.

Recuadro 1
Ciberseguridad según la definición de la Unión Internacional de Telecomunicaciones

"El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques de la gestión del riesgo, medidas, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y confidencialidad."

Recomendación UIT-T X.1205 de la Unión Internacional de Telecomunicaciones (UIT), Aspectos generales de la ciberseguridad.

18. **Seguridad de la información frente a ciberseguridad.** Muchas organizaciones utilizan el término "seguridad de la información", que se refiere a la seguridad de la información en todas sus formas y dondequiera que se almacene, y no solo a los datos electrónicos en la ciberesfera. La ciberseguridad, en cambio, puede estar más asociada a la información exclusivamente digital y a la protección de un conjunto más amplio de activos conectados o afectados por el ciberespacio, como se ve en la definición de la UIT. A pesar de las ligeras divergencias conceptuales entre ambos términos, se solapan en gran medida, sobre todo en lo que respecta a los objetivos fundamentales de protección de la disponibilidad, la integridad y la confidencialidad de la información (también conocida como la "tríada de la seguridad de la información", como se ve en el gráfico I). Algunas organizaciones utilizan el término "ciberseguridad" de forma totalmente intercambiable con el de "seguridad de la información". Otras consideran que la "ciberseguridad" ha sustituido al término más tradicional de "seguridad de la información", aunque perdiendo algunas de sus connotaciones más amplias relacionadas con el conocimiento y la gestión de la información en favor de propiedades más centradas en las TIC, y otras más emplean la "ciberseguridad" como un término general que comprende tanto la "seguridad de la información" como el término más restringido (y menos utilizado) de "seguridad de las TIC",

[9] El marco general de las Naciones Unidas sobre ciberseguridad y ciberdelincuencia (véase CEB/2013/2) y el plan de coordinación interna del sistema de las Naciones Unidas sobre ciberseguridad y ciberdelincuencia (2014, anexo) incluían definiciones para establecer un entendimiento común de los términos ciberdelincuencia y ciberseguridad, con la advertencia de que se trataba de definiciones funcionales de trabajo no refrendadas como tales por el sistema de las Naciones Unidas.

que se refiere específicamente a la seguridad de la infraestructura de las TIC (por ejemplo, *hardware*, *software*, redes y procesos técnicos).

Gráfico I
Modelo de la tríada de la seguridad de la información[10]

Fuente: Instituto Nacional de Normas y Tecnología de los Estados Unidos.

19. Se observaron ambigüedades terminológicas similares en la nomenclatura relacionada con las funciones de liderazgo bajo las que se tendía a situar la ciberseguridad en el contexto de un organigrama organizativo. Por ejemplo, el "oficial jefe de seguridad de la información" puede depender de un "responsable de tecnología de la información" o de un "oficial jefe de información", de forma que, o bien estos dos últimos se utilizan como sinónimos para designar al jefe del departamento de TIC, o bien el oficial jefe de información incluye también funciones de gestión de conocimientos y expedientes o de comunicaciones y relaciones públicas. No ha sido posible discernir una pauta coherente que sugiera uso deliberado de conceptos o rigor a la hora de delimitar las diferencias de alcance entre las funciones asignadas a cada término.

20. En todo el informe, los Inspectores utilizan el término "ciberseguridad", tal como se ha definido anteriormente. Siempre que se hace referencia a la "seguridad de la información", se hace deliberadamente con el fin de ser fieles a los documentos fuente al hacer citas directas o para garantizar el uso correcto de términos técnicos, como "oficial jefe de seguridad de la información" o "sistema de gestión de la seguridad de la información". No obstante, los Inspectores consideraron que no era necesario revisarlo ni armonizar su uso, ya que no constituía un impedimento para la comunicación o el intercambio de información conexa entre las organizaciones.

[10] Tal y como la define el Centro para la Seguridad en Internet, la tríada confidencialidad-integridad-disponibilidad es un modelo de referencia en la seguridad de la información diseñado para gobernar y evaluar cómo una organización maneja los datos cuando se almacenan, transmiten o procesan. Cada atributo de la tríada representa un componente crítico de la seguridad de la información, tal como se explica a continuación. La confidencialidad significa que no se debe acceder a los datos ni leerlos sin autorización. Garantiza que solo tengan acceso las partes autorizadas. Los ataques contra la confidencialidad son ataques de divulgación. La integridad implica que los datos no deben ser modificados o puestos en peligro de ninguna manera. Se supone que los datos permanecen en su estado previsto y solo pueden ser editados por partes autorizadas. Los ataques contra la integridad son ataques de alteración. La disponibilidad significa que los datos deben ser accesibles atendiendo a una petición legítima. Esto garantiza que las partes autorizadas tengan acceso sin trabas a los datos cuando lo necesiten. Los ataques contra la disponibilidad son ataques de destrucción.

II. Una instantánea de la ciberseguridad en el sistema de las Naciones Unidas

A. Atención creciente a la ciberseguridad, pero diferentes niveles de madurez en todo el sistema

21. **Creciente conciencia de que la ciberseguridad requiere atención.** En los últimos años, las organizaciones del sistema de las Naciones Unidas han comprendido cada vez más, aunque de forma desigual, que la ciberseguridad requiere atención. La exposición y el atractivo de las organizaciones del sistema de las Naciones Unidas como objetivo de los ciberatacantes es indiscutible, aunque puede variar en función de su mandato o visibilidad. Puede afirmarse que el mandato o el modelo de actividad, así como la información que poseen o gestionan, han influido en el ritmo con el que las organizaciones han ido reconociendo que la ciberseguridad es una cuestión que reviste importancia. Las organizaciones que manejan datos políticamente sensibles con implicaciones para la seguridad internacional o los intereses nacionales o económicos, así como las que gestionan grandes volúmenes de datos legalmente sensibles, incluidos datos personales de poblaciones beneficiarias en su mayoría vulnerables, parecen llevar la delantera en cuanto a mejorar su preparación en materia de ciberseguridad, mientras que las organizaciones con mandatos relativamente poco controvertidos se han puesto al día en la construcción de ciberdefensas a un ritmo más pausado. Además, algunas organizaciones que han estado en el punto de mira de la opinión pública debido a la actualidad de sus mandatos han tenido que redoblar sus esfuerzos de forma significativa en poco tiempo (como la Organización Mundial de la Salud (OMS)), al igual que aquellas organizaciones en las que los ciberataques a gran escala o de gran visibilidad han hecho más apremiante su necesidad de actuar con rapidez y reforzar su ciberresiliencia (como la Organización de Aviación Civil Internacional (OACI)). En general, sin embargo, no hay ninguna organización participante en la DCI que no haya reconocido, de alguna manera, la importancia de mantener una posición sólida en materia de ciberseguridad, acorde con sus requisitos operativos.

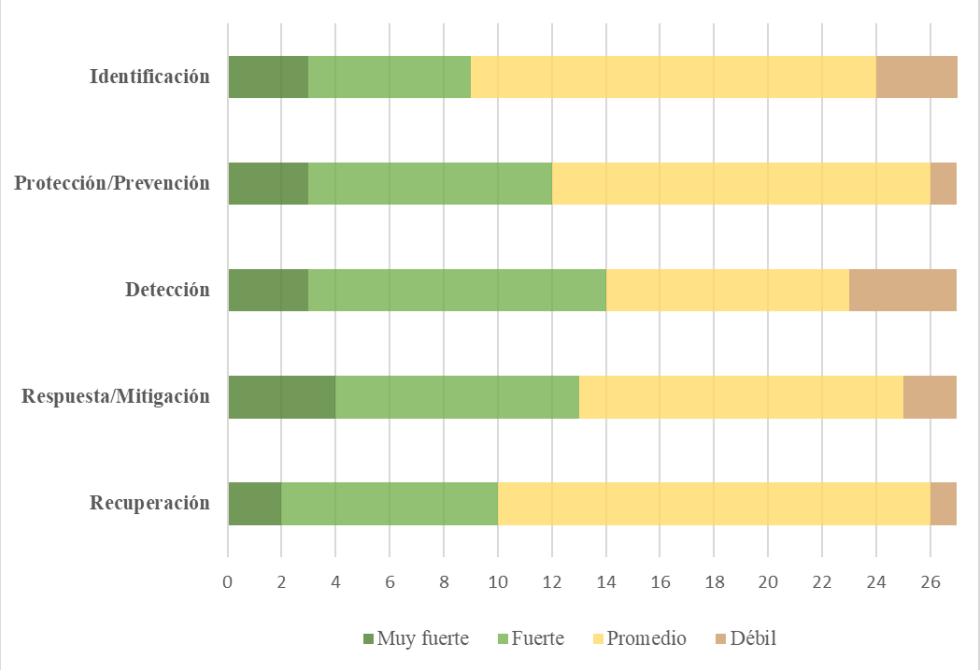
22. **Diferentes niveles de madurez entre las organizaciones de las Naciones Unidas.** Aunque no se constató que ninguna organización participante en la DCI fuera ajena a la necesidad de invertir en su ciberseguridad, se observaron diferencias significativas en los enfoques que las distintas organizaciones habían adoptado en su respuesta a las ciberamenazas. Se constató que el nivel de madurez de los marcos de ciberseguridad de las organizaciones del sistema de las Naciones Unidas variaba significativamente, incluso en ausencia de puntos de referencia comunes o de criterios utilizados uniformemente que pudieran facilitar una comparación metodológicamente fiable y basada en pruebas. Estas diferencias pueden explicarse en razón de: el entorno en el que opera cada organización; los requisitos dictados por el tipo de datos que se conservan; el nivel de comprensión de la ciberseguridad y la prioridad concedida a la misma por los dirigentes; la disponibilidad de recursos; y la disparidad de los sistemas de tecnología de la información, las herramientas y las soluciones de *software* utilizadas, que a menudo son el reflejo de años de decisiones en materia de inversión y de elección de proveedores no coordinadas en la totalidad del sistema. A pesar de los puntos comunes, estructurales y de otro tipo, que sin duda existen en la mayoría de, si no en todas, las organizaciones examinadas por la DCI, los intentos de ofrecer una evaluación definitiva de la madurez general de la ciberseguridad del sistema de las Naciones Unidas en su conjunto no harían justicia a la diversidad que caracteriza a sus miembros. Además, se consideró que tenía un valor práctico limitado, ya que las comparaciones con otras organizaciones o una madurez “mediana” de todo el sistema arrojarían pocas pistas sobre la propia protección.

23. **Las respuestas recogidas sugieren que hay margen de mejora.** En un intento de proporcionar una instantánea aproximada del estado de la cuestión, el gráfico II ilustra cómo las organizaciones participantes autoevaluaron su marco general de ciberseguridad en relación con amplias categorías de dominios funcionales, tal como se definen en el cuestionario de la DCI. A pesar de las evidentes dificultades para interpretar las respuestas recibidas en ausencia de un marco de referencia común o un punto de referencia que permita establecer comparaciones, la panorámica general no parece indicar que exista una posición

que inspire confianza en materia de ciberseguridad en el sistema en su conjunto, ni siquiera en términos subjetivos. El CICE, en su propia evaluación del desempeño general de las organizaciones del sistema de las Naciones Unidas en respuesta a la misma pregunta, y en la medida en que estaba en condiciones de proporcionar información sobre su clientela, otorgó calificaciones que oscilan entre "mediana" y "débil", lo que confirma aún más que hay margen de mejora a nivel de todo el sistema.

Gráfico II

Autoevaluación sobre el rendimiento en amplios dominios de ciberseguridad, por tipo de controles y número de organizaciones participantes en la DCI



Fuente: Cuestionario DCI 2020.

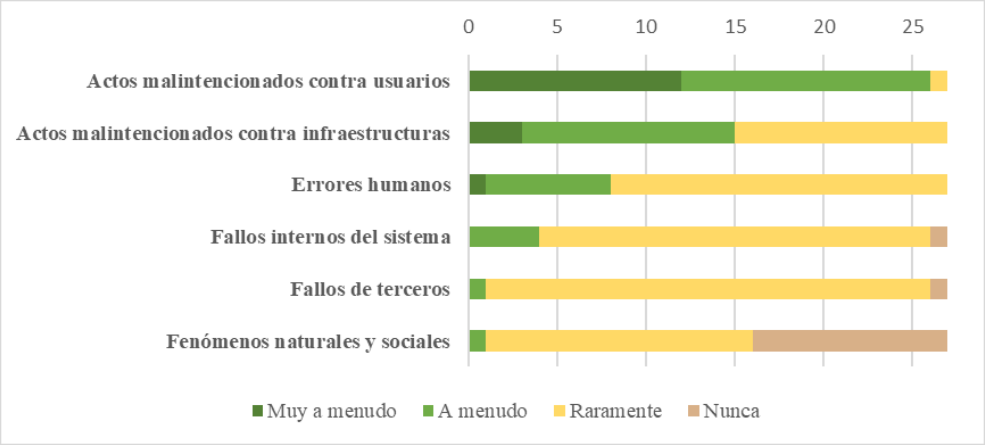
Nota: Las categorías en materia de autoevaluación se inspiraron conceptualmente en las utilizadas en los marcos y normas de referencia reconocidos en el ámbito de la ciberseguridad. Los dominios de ciberseguridad a los que se refiere el cuestionario de la DCI se desglosan de la siguiente manera: identificación (procesos críticos, activos, recursos, riesgos, etc.); protección/prevención (gestión del acceso, concienciación, formación, procedimientos, tecnología, etc.); detección (anomalías y eventos, monitorización continua, proceso de detección, etc.); respuesta/mitigación (planificación, comunicaciones, análisis, mitigación, etc.); y recuperación (planificación, restablecimiento, comunicaciones, mejoras, etc.).

24. **Riesgos para todo el sistema incrementados por una posición individual débil.** La cuestión del nivel adecuado de preparación en materia de ciberseguridad va más allá de la exposición respectiva de las organizaciones a título individual. Durante las entrevistas, los expertos en ciberseguridad confirmaron la opinión de que una organización con defensas vulnerables o débiles representaba un riesgo para las demás entidades del sistema. Una vez que un atacante consigue privilegios de administrador y obtiene un acceso más profundo a los sistemas de información de una organización, dicho acceso puede ser explotado para penetrar en el territorio digital de otra entidad. El movimiento malintencionado lateral de una organización a otra (conocido como "pivoteo") también puede ser más difícil de detectar y contrarrestar, porque puede pasar por tráfico normal. Sobre la base de la información recopilada en el contexto de la infraestructura de una organización, los jáquers pueden adaptar aún más el método de ataque y desplegar un conjunto de técnicas y herramientas diseñadas más a medida para lograr su objetivo. Por lo tanto, que las organizaciones se evalúen individualmente como "débiles" constituye un problema colectivo. Así, podría afirmarse que el sistema de las Naciones Unidas es tan fuerte como su eslabón más débil. Esta dimensión se analiza con más detalle en el capítulo IV del presente informe.

B. Panorama de las amenazas a la ciberseguridad

25. **Fuentes de amenazas y medios de ataque más frecuentes.** Para ofrecer una visión general de la exposición actual a las amenazas de ciberseguridad, el gráfico III incluye las respuestas ofrecidas por las organizaciones participantes en la DCI en relación con la frecuencia de los incidentes que les han afectado en los últimos cinco años, clasificados por fuente de amenaza. Las acciones maliciosas dirigidas a los usuarios de los sistemas de información (mediante *phishing*, robo de identidad, esquemas de "persona entrometida", etc.) o a la infraestructura (*malware*, ataques de denegación de servicio distribuida, etc.) fueron, con mucho, los tipos de amenazas más frecuentes que se denunciaron. Los funcionarios entrevistados confirmaron que los actos malintencionados dirigidos a los usuarios finales eran el tipo de ataque más común y el que más rápidamente había crecido en el pasado reciente. La pandemia, que obligó a muchos usuarios finales a trabajar desde ubicaciones remotas, a menudo utilizando equipos privados que, en muchos casos y en diversos grados, supusieron una carga adicional para las medidas de protección de la ciberseguridad de las empresas (párrs. 39 a 41), solo vino a reforzar este fenómeno.

Gráfico III
Exposición a amenazas de ciberseguridad en los últimos cinco años, por categoría de fuente de amenaza y número de organizaciones participantes en la DCI



Fuente: Cuestionario DCI 2020.

Nota: Las fuentes de amenaza se describieron de la siguiente manera: actos malintencionados contra usuarios (*phishing*, robo de identidad, esquemas de "persona entrometida", etc.); actos malintencionados contra infraestructuras (*malware*, ataques de denegación de servicio distribuida, otras medidas técnicas, etc.); errores humanos (error de configuración, error operativo, incumplimiento de los procedimientos, pérdida de equipos, etc.); fallos internos del sistema (mal funcionamiento del dispositivo o del sistema o fallo del *hardware*, fallo del suministro eléctrico, fallo del enlace de comunicaciones, etc.); fallos de terceros (proveedores de servicios de Internet, red eléctrica, gestión remota de dispositivos, etc.); y fenómenos naturales y sociales (inundaciones, terremotos, atentados, disturbios civiles, incendios, etc.).

26. **Aumento de los ataques de ingeniería social, especialmente durante la pandemia de COVID-19.** Mientras que las amenazas a la ciberseguridad se asocian comúnmente con operaciones técnicas sofisticadas dirigidas a la infraestructura, la comunidad de ciberseguridad de las Naciones Unidas informó de un cambio apreciable, en el que se ha pasado de los piratas informáticos que atacan los servidores, las redes y los dispositivos de usuario final a la piratería que se ceba en las personas mediante el uso de técnicas de ingeniería social destinadas a manipular a los individuos con fines fraudulentos para que divulguen información sensible. La pandemia de COVID-19 exacerbó los riesgos relacionados con la ingeniería social. Más de dos tercios de las organizaciones participantes informaron de un fuerte aumento de las amenazas y vulnerabilidades en materia de ciberseguridad durante los confinamientos mundiales que desconectaron de hecho a muchos usuarios de los recursos de ciberseguridad gestionados de forma centralizada, lo que hizo que el contacto con profesionales capacitados para el asesoramiento sobre correos electrónicos y

sitios web sospechosos fuera menos directo debido al súbito tránsito al trabajo a distancia. Según el CICE, los ciberdelincuentes y adversarios aprovecharon además la confusión y el mayor interés por los contenidos relacionados con la pandemia enviando correos electrónicos de *phishing* con temática de COVID-19 y creando sitios web falsos cargados de *malware* que supuestamente proporcionaban información sobre la enfermedad. Los ataques de *phishing* fueron especialmente exitosos durante este tiempo, que además estuvo marcado por los niveles sin precedentes de la desinformación difundida, a veces con ánimo de explotarla económicamente.

27. **Problemáticas específicas relacionadas con las técnicas de ingeniería social.** A diferencia de los ataques centrados en la infraestructura, que se dirigen directamente a un número limitado de recursos informáticos que podrían ser más fáciles de proteger, la ingeniería social se considera un reto en varios aspectos. Aunque son técnicamente sencillas de aplicar, estas técnicas están diseñadas para llegar a un gran número de usuarios simultáneamente, lo que eleva al máximo la probabilidad de una intrusión. Además, aunque la ingeniería social se dirija a los usuarios finales, estos suelen ser solo el punto de entrada que proporciona una vía de acceso a otros activos críticos. Las intrusiones facilitadas sin saberlo por miembros de la plantilla pueden pasar desapercibidas durante años, proporcionando a los adversarios un acceso ampliado a la arquitectura de seguridad interna y a la información confidencial, lo que a su vez ofrece nuevas oportunidades de ataque. Esto puede incluir el pivoteo, una técnica utilizada para pasar lateralmente del entorno cibernético de una organización al de otra tras la penetración inicial, aprovechando la infraestructura compartida o vinculada. Esta última táctica es especialmente preocupante para las organizaciones del sistema de las Naciones Unidas, muchas de las cuales comparten locales, centros de datos o servidores, ya que hace que las defensas de las organizaciones, incluso las más avanzadas y bien protegidas, sean tan vulnerables como las del eslabón más débil de la cadena. Por lo tanto, es especialmente importante garantizar una formación y sensibilización adecuadas entre toda la población de usuarios para reforzar las prácticas saludables.

28. **Otras amenazas.** Las organizaciones también han identificado los errores humanos como una fuente no despreciable de vulnerabilidades que implican errores de configuración, errores operativos, incumplimiento de los procedimientos, pérdida de equipos o daños involuntarios causados por la falta de concienciación en general. Según se informa, rara vez se producen fallos de terceros, lo cual es alentador, ya que indica que las organizaciones parecen aplicar la suficiente diligencia debida al seleccionar a sus socios comerciales. Las catástrofes naturales, así como otros peligros, incluidas las interrupciones causadas por conflictos o actividades terroristas, fueron las menos frecuentes, aunque constituyen un área importante en la que las consideraciones de seguridad física y de ciberseguridad deben ir de la mano para mitigar el impacto.

29. **Origen de las amenazas.** Tanto en el contexto de las Naciones Unidas como en términos generales, los incidentes de ciberseguridad pueden tener su origen en un amplio abanico de agentes amenazantes (recuadro 2), que pueden ser internos o externos a la entidad, y que pueden actuar de forma voluntaria (ataque deliberado) o involuntaria (por acciones u omisiones inadvertidas o por ser instrumentalizados sin su conocimiento). Algunos grupos delictivos ofrecen sus capacidades a otros actores para que las contraten, externalizando de hecho los ataques mediante una práctica que puede denominarse “ciberdelincuencia a la carta”. En consecuencia, la pregunta de quién está detrás de un ataque concreto (atribución de la amenaza) es difícil de responder, entre otras cosas por la multitud de mecanismos que existen para ofuscar el origen real del ataque (por ejemplo, mediante la suplantación de identidad *(spoofing)*, el pastoreo de bots, etc.). De hecho, varios funcionarios entrevistados admitieron que las organizaciones del sistema de las Naciones Unidas no solo carecían de la capacidad para determinar de forma fiable el origen de un ataque, sino que también eran reacias a tratar de descubrir la autoría, ya que los costos asociados a las pesquisas en esa dirección superaban con creces los beneficios o la utilidad de saber quién estaba detrás de la intrusión. Muchos afirmaron centrar sus esfuerzos en la prevención, detección y respuesta en lugar de invertir tiempo y recursos en perseguir a los adversarios, ya que hacerlo supondría un esfuerzo considerable, e incluso si se lograba parar a los adversarios, no se resolvería el problema, ya que las organizaciones seguirían enfrentándose a otros nuevos. Esto también vale para el fenómeno de las amenazas persistentes avanzadas, que, según confirmaron las

organizaciones, no son desdeñables y tienden a adoptar la forma de intrusión, vigilancia y acción retardada, lo que requiere un nivel de recursos y sofisticación comúnmente asociado a los ataques amparados por Estados.

Recuadro 2
Principales tipos de actores de amenazas en el ciberentorno

- **Jáqueres**. Individuos o grupos que irrumpen en las redes para causar trastornos, daños o caos, sobre todo buscando la fama o la emoción que implica el reto.
- **Hacktivistas**. Jáquers con una motivación específica que ven su actividad como una forma de desobediencia civil o como un medio de autoexpresión política o ideológica.
- **Ciberdelincuentes**. Actores que se dedican a la actividad delictiva cibernética (delitos comunes como el fraude, el robo, la extorsión, etc., ayudados por medios informáticos) o a la actividad delictiva ciberdependiente (por ejemplo, el despliegue de virus o programas malintencionados y otras actividades que solo pueden cometerse por medios informáticos). Según el nivel de sofisticación técnica y la capacidad organizativa, los actores implicados pueden ir desde pequeños grupos hasta grandes redes de delincuencia organizada.
- **Espías industriales**. Considerados a veces como una subcategoría del grupo delictivo, los objetivos de estos actores se concretan en la obtención de secretos industriales, el chantaje en busca de lucro o el sabotaje a la competencia; son delincuentes que se ceban sobre todo con el mundo empresarial.
- **Estados o grupos patrocinados por el Estado.** Actores muy sofisticados y con buenos recursos cuyas actividades tienden a ser difíciles de detectar, rastrear o identificar y que pueden perseguir objetivos complejos, a menudo indirectos y no evidentes, de forma sigilosa, directamente empleados por dependencias públicas o militares, o financiados indirectamente por estas. En el pasado, los Estados habían desarrollado principalmente capacidades de investigación, pero en los últimos años es un hecho ampliamente aceptado que algunos han adquirido además capacidades ofensivas.
- **Internos** *(Insiders)*. Actores que, en virtud de una relación contractual con la organización en cuestión, no se consideran externos, sino que ponen en peligro a la entidad por tener acceso a ella. Puede tratarse de empleados despechados, personal con escasa preparación o proveedores de servicios por contrata, entre otros.

C. Impacto conocido y desconocido de los incidentes de ciberseguridad

30. **Impacto notificado limitado.** Para comprender mejor hasta qué punto el riesgo se ha traducido en incidentes de ciberseguridad que han afectado a sus organizaciones participantes, la DCI les pidió que calificaran el impacto de los incidentes pasados según su gravedad (de insignificante a grave) y la categoría del impacto (financiero, operativo, digital, político o reputacional, material o físico, o relacionado con la productividad). Resulta interesante, y quizás sorprendente, que en sus respuestas las organizaciones participantes informaron invariablemente de que el impacto de los incidentes de ciberseguridad a los que se habían enfrentado fue menor o insignificante, independientemente de la categoría de dicho impacto. Al mismo tiempo, se reconoce que el número y la frecuencia de los incidentes de ciberseguridad evitados es considerable, del orden de miles de eventos al mes, y ha crecido exponencialmente en los últimos años. Esto es revelador del volumen de ciberamenazas al que están expuestas las organizaciones y sus infraestructuras hoy en día. Sin embargo, a primera vista, y teniendo en cuenta la relativa ausencia de recopilación sistemática de datos a este respecto, parece sugerir un impacto relativamente limitado en general.

31. **Áreas más afectadas.** Las organizaciones informaron de que los ámbitos más afectados por los ciberataques (el impacto fue calificado de “moderado” por un número comparativamente mayor, pero aun así limitado, de organizaciones, y de “importante” por una o dos organizaciones, pero en ningún caso de “grave”) habían sido el ámbito digital (principalmente las filtraciones de datos), seguido de los daños políticos y para la reputación

(desinformación, atención desfavorable de los medios de comunicación, interferencia indebida en los procesos intergubernamentales, etc.). Incluso en términos financieros, las pérdidas directas (como las transferencias fraudulentas de fondos) solo supusieron pequeñas cantidades, lo que parece indicar, siendo cautelosos, que las medidas de control habían sido eficaces a ese respecto. Sin embargo, los Inspectores desean destacar otras consecuencias financieras asociadas a los ciberataques (por ejemplo, el tiempo del personal y los costos derivados de la investigación de lo sucedido y la determinación del alcance de los daños causados, los costos de recuperación de activos o equipos, los honorarios de consultoría de las capacidades externas necesarias para resolver las brechas de seguridad, la pérdida de productividad durante los períodos de inactividad del sistema o los costos de las inversiones destinadas a la prevención de futuros problemas), que pueden ser mucho más complejos de cuantificar, pero que sin duda son importantes. En general, a pesar de que la mayoría de las organizaciones participantes autoevaluaron su capacidad de respuesta de ciberseguridad como "mediana" (solo un tercio la consideró "fuerte" o "muy fuerte"), el impacto de los incidentes de ciberseguridad experimentados por el sistema de las Naciones Unidas en la actualidad, tal y como se informó, no parece constituir por sí solo un motivo serio de preocupación.

32. **La realidad se desconoce.** Sin embargo, varios factores indican que está justificado prestar una atención prioritaria a la ciberseguridad. En primer lugar, los datos recogidos implican la existencia de algunos ángulos ciegos, lo que confirma que se desconoce la magnitud exacta de la amenaza y sus consecuencias, como reconocen varias organizaciones en sus respuestas. La mayoría de las veces, especialmente en el caso de los ataques más sofisticados, los adversarios no tienen ningún incentivo para revelar su presencia ni las vulnerabilidades que explotaron, lo que sugiere que es probable que las intrusiones en el sistema y las fugas de datos no detectadas estén muy por encima del nivel notificado. En este contexto, varios interlocutores señalaron que "lo que se sabe que se desconoce" comparado con lo que se conoce sobre la magnitud de la amenaza para la ciberseguridad era mucho, pero que "lo que no se sabe que se desconoce" podría ser aún más preocupante. En segundo lugar, las respuestas pueden (intencionadamente o no) minimizar el impacto, dado que, en una cultura corporativa impulsada por la presentación de informes relacionados con el rendimiento y un agudo sentido de dependencia respecto de los recursos vinculados a dichos informes, el reconocimiento honesto de las debilidades aún no se ha convertido en la norma como parte de la cultura propia de la organización. Esto puede, en consecuencia, sesgar los resultados. Por poner un ejemplo, en su respuesta al cuestionario de la DCI, 11 organizaciones participantes confirmaron oficialmente haber sufrido al menos un ciberataque importante que afectó a sus operaciones en el pasado reciente. Sin embargo, hay entidades de las que se sabe que han sufrido tales ataques, que han sido de dominio público, y que, sin embargo, no lo revelaron en sus interacciones con la DCI. Por lo tanto, cabe suponer que la amenaza real, así como su impacto, supera tanto lo que se conoce como lo que las organizaciones pueden estar dispuestas a divulgar.

33. **Las amenazas pasadas no son un indicador de futuros incidentes.** A pesar de lo anterior, parece haber consenso entre los expertos en que sería un error juzgar la gravedad de la amenaza atendiendo a la medida en que se sabe que dicha amenaza se ha materializado en el pasado. El potencial de daño sigue siendo alto y debe anticiparse con estrategias de respuesta. Por ejemplo, la creciente amenaza del programa secuestrador *(ransomware)*, que se despliega con el fin de extorsionar exigiendo dinero a cambio de los datos robados, parece haber perdonado hasta ahora, con algunas excepciones, a las organizaciones del sistema de las Naciones Unidas. La información aportada por los medios de comunicación confirma que varias entidades conocidas, incluidas grandes empresas del sector privado e incluso entidades gubernamentales locales, se han visto obligadas a pagar rescates para poder acceder de nuevo a sus datos y sistemas de información. Los Inspectores señalan que, en la actualidad, las organizaciones participantes han adoptado una clara postura contraria al pago de cualquier rescate a los delincuentes. En el mismo sentido, cabe señalar que, en este momento, las organizaciones del sistema de las Naciones Unidas no comunicaron haber sufrido ningún ciberataque contra dispositivos conectados, como ascensores, sistemas de ventilación, vehículos autónomos o equipos similares controlados remotamente. El ataque a dispositivos conectados es un área de riesgos de ciberseguridad reciente, pero las entidades deben estar atentas ya que los expertos del sector prevén un aumento significativo de este tipo de

amenazas en el futuro. Estos dos ejemplos muestran la importancia de anticiparse a riesgos para los que hasta ahora puede haber pocos precedentes en el contexto de las Naciones Unidas, y de integrar proactivamente las consideraciones de ciberseguridad en el proceso general de gestión de riesgos de las organizaciones.

34. **Ciberseguro.** Para aumentar la protección proactiva contra las amenazas emergentes, una opción es contratar un ciberseguro para cubrir los daños causados por los ciberataques, así como para, posiblemente, evitar tener que lidiar con la dimensión ética que subyace a la cuestión de pagar o no un rescate. Los proveedores comerciales, en función de cada caso, podrían ser obligados por su cliente a ofrecer un ciberseguro. Durante el examen, ninguna organización del sistema de las Naciones Unidas indicó que hubiera optado por un seguro de este tipo que cubriera los riesgos cibernéticos asociados, aunque algunas indicaron que lo habían estado sopesando. Reconociendo la posición predominante a este respecto en las entidades de las Naciones Unidas, los Inspectores no consideran que el ciberseguro sea un instrumento eficaz para contrarrestar proactivamente los riesgos asociados en la mayoría de los contextos operacionales, en particular porque solo sería una estrategia de mitigación parcial que contribuiría a reducir al mínimo las pérdidas financieras que pudiera causar un ciberataque, mientras que sería poco eficaz a la hora de abordar los daños operacionales o para la reputación. Sin embargo, en **opinión de los Inspectores, la dirección ejecutiva haría bien en prepararse para la eventualidad de tales amenazas, que probablemente aumentarán en el futuro.**

D. Compromiso y cooperación con las autoridades nacionales

35. **Prácticas desiguales y poca predisposición a informar a las autoridades nacionales.** Las organizaciones participantes tienen prácticas diferentes a la hora de notificar las violaciones de la ciberseguridad a las autoridades nacionales que podrían estar en condiciones de investigar y tomar medidas administrativas o judiciales con respecto a un ciberataque. Alrededor de un tercio de las organizaciones participantes declararon haber notificado incidentes a las autoridades nacionales encargadas de hacer cumplir la ley, aunque pocas lo hicieron de forma sistemática o regular. Entre las organizaciones que indicaron haber colaborado con las autoridades nacionales en asuntos de ciberseguridad en el pasado, la mayoría confirmó haberlo hecho caso por caso en vez de actuar en aplicación de la política de la organización o la práctica establecida. Muchas utilizaron relaciones informales a nivel de trabajo en lugar de canales oficiales cuando fue posible, y solo en caso de ataques importantes que hicieran pensar que probablemente el país anfitrión se vería afectado o que la reputación de la organización correría un riesgo importante. Incluso en los casos en los que las capacidades de investigación a nivel nacional fueran excedentes y pudieran así ser un complemento útil de las capacidades internas, a menudo muy limitadas, para perseguir a los presuntos atacantes, pocas organizaciones expresaron su deseo o la necesidad de formalizar o aumentar la interacción sistemática con las autoridades nacionales debido a las brechas de ciberseguridad. El panorama general parece indicar que la voluntad de colaborar plenamente con las autoridades nacionales es escasa y que se prefiere mantener una interacción informal y "sujeta a la necesidad".

36. **Factores que influyen en la práctica de las organizaciones.** Hay varios factores que pueden llevar a las organizaciones a dudar antes de ponerse en contacto con las autoridades nacionales. Uno de ellos es la condición jurídica de las organizaciones como titulares de privilegios e inmunidades, especialmente en relación con la confidencialidad e inviolabilidad de sus datos, que deben estar al margen de cualquier interferencia de carácter legislativo, ejecutivo o judicial. Los profesionales de la ciberseguridad no suelen comprender bien los límites de las obligaciones que impone la ley en este ámbito. De hecho, mientras que los Estados están obligados por ley a ofrecer protecciones, las organizaciones solo tienen el deber de cooperar con las autoridades nacionales en la medida en que dicha cooperación no interfiera con su capacidad de ejercer sus funciones de forma independiente. Por tanto, dicha cooperación es siempre voluntaria. Esta fórmula puede ser, de hecho, una línea fina por la que transitar en la práctica, pero no debería impedir la colaboración voluntaria cuando esté justificada, una vez que se hayan evaluado plenamente los posibles riesgos de la colaboración. En cualquier caso, no existe la obligación de informar de los incidentes a las

autoridades nacionales ni de divulgar datos que se consideren sensibles. Los departamentos jurídicos son los más indicados para asesorar a los responsables de la toma de decisiones a este respecto. Otra consideración a la hora de decidir si se contacta o no con las autoridades nacionales puede estar relacionada con la madurez del propio aparato de ciberseguridad del país respectivo, así como el trato que se da a los ciberdelincuentes una vez remitidos a la jurisdicción nacional. Estas preocupaciones pueden agravarse en los casos en que el propio personal de las organizaciones esté implicado en la puesta en peligro de la ciberseguridad de la organización (amenazas procedentes de *insiders*). En estos casos, el procedimiento estándar prevé el levantamiento de los privilegios e inmunidades y la entrega de la persona a su Estado de nacionalidad para su investigación y posible enjuiciamiento. Sin embargo, esto sigue siendo un hecho comparativamente raro, sobre todo en lo que respecta al uso cibernético malintencionado. Desde 2007, año en el que se empezaron a recopilar y publicar estadísticas al respecto, solo un caso de mala conducta del personal que se ha remitido a través de la Oficina de Asuntos Jurídicos a las autoridades nacionales para su posterior investigación estaba relacionado con una violación de la seguridad de la información[11]. Además de las consideraciones expuestas anteriormente, la gravedad del incidente, la utilidad y la probabilidad de conseguir atribuir los ataques a un autor concreto, la posibilidad de que se exponga indebidamente información confidencial o delicada, y el posible impacto de una investigación en las actividades operativas fueron algunas de las consideraciones que se citaron con más frecuencia a la hora de decidir si se recurría o no a las autoridades nacionales. Algunos funcionarios también reconocieron que, a menudo, la denuncia a las autoridades nacionales simplemente estaba descartada.

37. **Proceso de toma de decisión para informar a los homólogos nacionales.** Como se ha mostrado anteriormente, la decisión de iniciar o no el contacto con las autoridades nacionales implica dimensiones que van más allá de las competencias de los expertos en ciberseguridad. Entra en juego una combinación de consideraciones políticas, jurídicas, probatorias y prácticas, por lo que dicha decisión debe implicar a una serie de partes interesadas. En las organizaciones en las que los Inspectores encontraron pruebas de un enfoque más establecido en materia de colaboración con las autoridades nacionales, la distribución de responsabilidades reflejaba el abanico de consideraciones implícitas, lo que se consideró una buena práctica. Más concretamente, la oficina de programas o la dependencia sustantiva afectada evaluaría la gravedad de la intrusión, sopesando los riesgos programáticos y los beneficios que se derivarían de contactar con las autoridades nacionales. La oficina jurídica evaluaría y asesoraría sobre las posibles ramificaciones de carácter jurídico, dado el estatus especial de las organizaciones y su personal en las jurisdicciones afectadas, incluida la posible necesidad de levantar privilegios e inmunidades y, en su caso, remitir al personal implicado a su país de nacionalidad. El papel del departamento de TIC o de los expertos en ciberseguridad sería proporcionar pruebas forenses de la infracción en la medida en se dispusiera de ellas. La decisión de proceder a plantear el asunto al país anfitrión correspondería a la dirección ejecutiva, con la aportación de todas las partes interesadas anteriormente mencionadas. Una vez que se ha tomado la decisión de implicar a las autoridades nacionales a causa de un incidente, los mecanismos para hacerlo son normalmente las líneas de comunicación establecidas entre las oficinas pertinentes de las organizaciones de las Naciones Unidas, la misión permanente del Estado concernido y las autoridades pertinentes del país anfitrión en cuestión. Habida cuenta de algunas observaciones críticas formuladas sobre la eficacia del proceso establecido, puede haber margen para estudiar algunas vías alternativas o complementarias, algunas de las cuales se describen en otra parte del presente informe (párrs. 161 a 163).

E. Preparación tecnológica – problemas concretos que exigen atención

38. **Capacidades técnicas básicas bien desarrolladas, áreas que requieren mayor atención destacadas.** Los Inspectores formularon una serie de preguntas a las organizaciones participantes con el fin de examinar el estado general de su preparación tecnológica para abortar las ciberamenazas. Con ello, no se pretendía realizar una evaluación exhaustiva de la

[11] A/75/217, anexo I.

solidez de sus disposiciones operativas o de su infraestructura técnica, sino más bien comprender las capacidades generales existentes y aislar algunas cuestiones comunes que podrían merecer especial atención. Teniendo en cuenta las limitaciones inherentes a la información recopilada principalmente a través de la autoevaluación, así como la considerable disparidad en el nivel de detalle compartido con los Inspectores, las respuestas indican que las organizaciones participantes consideran que los aspectos técnicos básicos de la ciberseguridad han sido bien comprendidos y se ha invertido en ellos, de acuerdo con sus respectivas capacidades. Por ejemplo, dos tercios de las organizaciones participantes indicaron que disponían de herramientas de supervisión de la red. Además, la mayoría de las organizaciones indican que han instalado cortafuegos u otros sistemas de prevención de intrusiones, mientras que 13 organizaciones afirman haber implantado un sistema de gestión de información e incidencias de seguridad. En las áreas que han sido objeto de un desarrollo tecnológico más dinámico en el pasado reciente es donde el panorama parece más matizado y puede justificar cierta atención por parte de las organizaciones participantes. En esta sección, por razones de seguridad, no se identifican disposiciones concretas de organizaciones, para evitar que se extraigan conclusiones que puedan poner en peligro la seguridad de las entidades en cuestión.

Gestión de dispositivos de usuario final y herramientas que facilitan el trabajo a distancia

39. **La pandemia de COVID-19 puso de relieve la gestión de los dispositivos de punto final.** La pandemia obligó a poner en marcha acuerdos de trabajo alternativos y flexibles a una escala mucho mayor que la practicada antes en casi todos los grupos ocupacionales, tanto en la sede como sobre el terreno. En este contexto, la capacidad de las organizaciones para operar fuera de las instalaciones, con un acceso físico limitado a los locales y a los equipos informáticos conectados de forma centralizada, ha sido sometida a una prueba de estrés sin precedentes, y las herramientas que facilitan el trabajo a distancia han sido objeto de un mayor escrutinio desde la perspectiva de la ciberseguridad. Por un lado, esto incluye la capacidad de los empleados para acceder de forma segura a los recursos informáticos a distancia, que dos tercios de las organizaciones indicaron que facilitaban mediante el uso de redes privadas virtuales, y el resto de las organizaciones utilizaban servicios basados en la nube a los que se accedía mediante protocolos de Internet cifrados a través de la red pública sin necesidad de redes privadas virtuales. Por otro lado, la capacidad de operar fuera de las instalaciones implica la gestión de dispositivos de usuario (ordenadores de sobremesa y portátiles, así como otros dispositivos móviles), para lo cual las respuestas indican un nivel de cobertura más variado.

40. **La gestión de dispositivos de usuario se queda rezagada.** Aunque la mayoría de las organizaciones mencionan algún grado de gestión centralizada de los dispositivos, varias de ellas no parecen ofrecer una cobertura completa. En algunos casos, la cobertura se limita a los equipos ubicados en la sede, y siete organizaciones señalan que sus oficinas exteriores siguen prácticas de gestión de dispositivos separadas y, en otros casos, solo los ordenadores conectados permanentemente están cubiertos de forma centralizada, mientras que alrededor de un tercio de las organizaciones participantes no gestionan ni protegen los dispositivos móviles de forma centralizada en absoluto, aunque unas pocas están en proceso de desplegar plataformas con este fin o tienen previsto hacerlo en un futuro próximo. Solo dos respuestas mencionan el cifrado de los dispositivos de usuario, que es una medida importante para evitar el robo y la fuga de datos, especialmente en el nivel de los dispositivos portátiles de los usuarios al final de la cadena, que suelen ser más propensos a la pérdida y el robo. Las respuestas pusieron de relieve que las organizaciones eran conscientes de la necesidad de gestionar los dispositivos de la empresa, pero mostraron que la gestión de los equipos móviles se estaba quedando rezagada. Las vulnerabilidades existentes en este sentido se agudizaron por el uso de dispositivos móviles personales, no corporativos, como ordenadores portátiles privados, una práctica que ha aumentado de forma importante durante la pandemia.

41. **Introducción de importantes medidas de ciberseguridad o aceleración de dichas medidas.** A pesar de los numerosos problemas encontrados, la llegada de la pandemia también provocó algunos avances positivos. Las entidades de las Naciones Unidas se vieron obligadas a examinar más detenidamente sus marcos de gestión de la seguridad, y los proyectos corporativos de TIC previstos empezaron a materializarse, impulsados por la

necesidad inmediata. Puede decirse que el cambio masivo, adoptado con muy poca antelación, a la modalidad de trabajo a distancia llevó a muchas organizaciones a acelerar sus esfuerzos para mejorar la seguridad del acceso remoto y, a juzgar por las respuestas a los cuestionarios de la DCI, puede haber proporcionado un impulso más que necesario a las iniciativas en esta dirección. De hecho, la mayoría de las entidades pusieron en marcha un sistema de autenticación multifactorial para el acceso remoto, desplegaron herramientas para la colaboración en línea y el intercambio de datos hasta niveles nunca vistos, institucionalizaron mejor el uso de la firma electrónica y ampliaron las oportunidades de formación en seguridad de la información. En cierto sentido, la pandemia se convirtió en un catalizador para la transformación de las TIC de varias entidades de las Naciones Unidas y las empujó en la dirección de la digitalización y las prácticas de trabajo digitales avanzadas, un factor que tiene implicaciones no solo en el ámbito de la ciberseguridad, sino también, en términos mucho más amplios, en la forma de trabajar de las organizaciones, así como en la manera de gestionar los activos y las instalaciones.

Sistemas heredados

42. **Vulnerabilidades específicas creadas por los sistemas heredados.** Varias organizaciones participantes señalaron que la actualización o la retirada de los sistemas heredados que envejecen, y que las aplicaciones de última generación ya no soportan, estaba planteando importantes retos de ciberseguridad. Se dijo que la presencia continuada de estos sistemas heredados representaba una fuente importante de vulnerabilidad, ya que muchos de ellos estaban diseñados para ser utilizados únicamente a nivel local, en redes privadas —de área local o amplia—, que se habían considerado entornos seguros. Debido principalmente a la evolución del acceso remoto y al mayor uso de la computación en la nube, estas aplicaciones están ahora mucho más expuestas a los riesgos derivados de la mayor interconexión de los sistemas y datos a nivel más global, siendo así que no han sido construidas para resistir formas de ataque más actuales. Algunas de las vulnerabilidades creadas a resultas de ello podrían ser registradas y señaladas por los sistemas de gestión de vulnerabilidades, pero sigue existiendo la posibilidad de que algunas aplicaciones propietarias heredadas no sean detectadas automáticamente. Incluso cuando se detecten, no necesariamente se podrán aplicar parches inmediatamente y pueden propiciar una exposición indebidamente prolongada de las entidades afectadas. Además de los riesgos para las propias aplicaciones heredadas, estas vulnerabilidades también suponen un riesgo para otras aplicaciones y datos que puedan compartir la misma infraestructura, ya que las primeras pueden utilizarse para el movimiento lateral a través de sistemas y aplicaciones que ya han quedado comprometidos.

43. **Está justificada una cuidadosa revisión de los sistemas heredados.** Por lo tanto, es importante que las organizaciones del sistema de las Naciones Unidas hagan un seguimiento y trabajen activamente en la actualización o sustitución de esos sistemas. Teniendo en cuenta que algunos de estos sistemas heredados son grandes y complejos (como los sistemas de planificación de los recursos institucionales), y que muchos de ellos fueron creados internamente durante largos períodos de tiempo, esta tarea puede ser compleja para muchos, y requerir más recursos financieros y esfuerzos para obtener y mantener la aceptación de las dependencias institucionales que habían invertido en el desarrollo de soluciones adaptadas que ahora se consideran inseguras. **Los Inspectores sugieren que los jefes ejecutivos, en estrecha colaboración con expertos en TIC y ciberseguridad, así como con las unidades de la institución afectadas, pongan en marcha una cuidadosa revisión de la cuestión de los sistemas heredados dentro de su organización, si es que no la han iniciado ya.** Las consideraciones de ciberseguridad deberían ocupar un lugar destacado en su análisis, al igual que la consideración estratégica y oportuna de las consecuencias en materia de recursos y las repercusiones inmediatas y a más largo plazo del desmantelamiento de esos sistemas en las operaciones, que deberían abordarse mediante una planificación adecuada para la institución de medidas temporales de mitigación, cuando sea posible.

Seguridad en la nube

44. **La protección ofrecida por los proveedores de servicios externos de computación en la nube mejoró considerablemente según la comunidad de expertos en ciberseguridad.** Desde 2019, cuando la DCI publicó su informe sobre la computación en la

nube[12], tanto el uso de servicios basados en la nube por parte de sus organizaciones participantes como el alcance y la madurez de dichos servicios han experimentado un crecimiento considerable. Su ubicuidad, elasticidad (la capacidad de adaptar continuamente la asignación de recursos informáticos a la demanda real de esos recursos en tiempo real) y rentabilidad, así como su creciente sofisticación tecnológica, han inspirado la confianza de los usuarios en su solidez y seguridad, aumentando aún más su atractivo para el sistema de las Naciones Unidas. Las organizaciones siguen migrando sus actuales aplicaciones a servicios basados en la nube, y la decisión de hacerlo sigue correspondiendo a cada organización. A este respecto, los Inspectores reconocen el creciente reconocimiento por parte de la comunidad de expertos en ciberseguridad de que las capacidades y garantías de la computación en la nube que ofrecen los líderes de la industria comercial superan hoy en día el nivel de seguridad de los datos, de confidencialidad y de ciberresiliencia que podían ofrecer hace tan solo uno o dos años. Según los expertos, es probable que las protecciones que ofrecen actualmente estos proveedores también superen la capacidad de cualquier organización para lograr un grado de seguridad comparable utilizando soluciones desarrolladas internamente. Solo se encontró un ejemplo durante la presente revisión en el que una organización participante optó por renunciar completamente a las soluciones basadas en la nube en relación con una parte pequeña y particularmente sensible de los datos que gestionaba. Sin embargo, cabe señalar que esta elección se hizo en lo que respecta a un conjunto de datos limitado y se basó en la capacidad de esa organización —en particular la capacidad financiera— para ofrecer una alternativa viable, lo que no se aplica automáticamente a la mayoría de las organizaciones.

45. **Se justifica una vigilancia continua al usar servicios externos de computación en la nube.** Incluso en el contexto de los importantes avances logrados en los últimos años en relación con la seguridad de la computación en la nube, las recomendaciones a los jefes ejecutivos formuladas en el informe de la DCI mencionado siguen siendo válidas en lo que respecta a lo siguiente: la necesidad de ajustar los servicios de computación en la nube a las necesidades institucionales para proporcionar valor a la inversión; las evaluaciones exhaustivas de los riesgos y la gestión cuidadosa de los proveedores en la contratación de proveedores externos de servicios en la nube; y las estrategias para mitigar el riesgo de que los proveedores no puedan prestar los servicios contratados. También persiste la preocupación por los riesgos de monopolización y concentración excesiva de los datos de las Naciones Unidas en manos de unos pocos gigantes tecnológicos. En consecuencia, las organizaciones no pueden permitirse el lujo de bajar la guardia al utilizar aplicaciones basadas en la nube o desplegar sus aplicaciones y datos en la nube, sobre todo teniendo en cuenta el riesgo de acceso no autorizado a datos confidenciales o sensibles. Deben seguir actuando con la debida diligencia y mantener unas prácticas de ciberseguridad sólidas cuando confíen en los servicios de computación en la nube, en particular exigiendo pruebas del cumplimiento por sus proveedores de los requisitos en materia de auditoría independiente y la presentación de los certificados pertinentes, como los informes de controles de sistemas y organizaciones, en particular los conocidos como “informes SOC 2”, o garantías similares que gocen de amplio reconocimiento entre los expertos del sector. La exigencia de estas garantías externas e independientes adquiere importancia si se tiene en cuenta el hecho de que la competencia de la auditoría interna y otros mecanismos de supervisión de la organización pueden cesar cuando se contratan proveedores externos. Por lo tanto, se recomienda solicitar la opinión del departamento de auditoría interna cuando se celebre un contrato de este tipo de servicios, con el fin de garantizar que se incluyan las disposiciones pertinentes para proporcionar una garantía razonable de cumplimiento de las normas de control interno adecuadas en relación con la recopilación, el almacenamiento y el uso de la información proporcionada. También es aconsejable consultar a la oficina jurídica. Por lo tanto, las organizaciones deben encontrar alternativas aceptables para reafirmar un nivel de control que se considere adecuado, por ejemplo, incluyendo disposiciones en los acuerdos contractuales con los proveedores externos de servicios en la nube que permitan a la entidad ejercer la supervisión y el control del cumplimiento. Además, las instalaciones comerciales basadas en la nube pueden cambiar de propietario, incluso a nivel internacional, lo que puede, en algunos contextos, agravar aún más el riesgo de exposición de los datos conservados o

[12] JIU/REP/2019/5.

gestionados por dichas instalaciones en caso de que se intente iniciar un procedimiento judicial en la jurisdicción nacional correspondiente. En tales situaciones, se harán valer y se mantendrán las prerrogativas e inmunidades con respecto a todos los datos conservados en nombre de las organizaciones del sistema de las Naciones Unidas. Sin embargo, las organizaciones deben permanecer vigilantes y tomar las precauciones necesarias para gestionar estos riesgos en la medida de lo posible.

46. **El riesgo cero es inalcanzable, se requiere un análisis detallado.** Independientemente de la rentabilidad y los beneficios en materia de seguridad que puedan obtenerse, los Inspectores recuerdan que tanto las soluciones basadas en la nube como los enfoques tradicionales de los centros de datos están expuestos a las amenazas de ciberseguridad y nunca pueden pretender ser inexpugnables. Por lo tanto, no es realista aspirar a una eliminación completa de los riesgos en ninguno de los dos entornos. Independientemente de que el riesgo se transfiera, en cierta medida, a entidades externas que gestionan el entorno informático correspondiente, la responsabilidad de las consecuencias de los ciberataques sigue siendo interna. En consecuencia, es aconsejable que las organizaciones realicen un análisis detallado antes de decidir si están dispuestas a confiar la protección de su información a terceros y, en caso afirmativo, qué aspectos. En este sentido, las evaluaciones de protección de datos deben garantizar que las salvaguardias de los servicios de computación en la nube se ajusten a los requisitos de las organizaciones y sean proporcionales al tipo y la sensibilidad de los activos de datos en cuestión. Consideraciones similares se aplican a cualquier decisión sobre la subcontratación y, por tanto, no se limitan únicamente al contexto del uso de la seguridad en la nube.

Gestión de la vulnerabilidad

47. **La práctica entre las organizaciones participantes es desigual.** La gestión de la vulnerabilidad se considera uno de los principales retos de la ciberseguridad en las organizaciones internacionales en la actualidad. Casi a diario se descubren nuevas vulnerabilidades en programas informáticos de uso generalizado, incluidos los utilizados por las organizaciones del sistema de las Naciones Unidas. Aunque los proveedores de dispositivos y *software* desarrollan y ofrecen constantemente los parches correspondientes, estos se traducen en una cantidad considerable de información que hay que procesar y suponen una carga de trabajo importante al aplicar los parches en entornos técnicos complejos. Para hacer frente a este reto, más de la mitad de las organizaciones participantes informaron de que disponían de algún tipo de solución de gestión de vulnerabilidades. Por ejemplo, algunas utilizan suscripciones a múltiples fuentes de información para conocer continuamente cuáles son las nuevas amenazas y defenderse de ellas, en particular las nuevas vulnerabilidades, mientras que otras han optado por implantar soluciones de seguridad integradas procedentes de proveedores comerciales que incluyen la gestión de vulnerabilidades. Algunas organizaciones destacaron que la detección y la aplicación de parches a las vulnerabilidades es una actividad de ciberseguridad muy exigente. Otras observaron que los intentos malintencionados de encontrar vulnerabilidades en sus redes y sistemas aumentaban con el tiempo, mientras que el carácter disperso de su red de TIC dificultaba la gestión centralizada del proceso de aplicación de parches de vulnerabilidad, en particular en múltiples ubicaciones sobre el terreno. Varias organizaciones también informaron de que los gastos de parcheo de vulnerabilidades figuraban entre los costos más importantes asociados a sus programas de ciberseguridad.

48. **Se debe llevar a cabo una gestión continua de la vulnerabilidad.** Los Inspectores llaman la atención sobre el hecho de que hay una diferencia significativa en la eficacia entre las evaluaciones *ad hoc* (por ejemplo, anuales) de la vulnerabilidad y un proceso continuo de gestión de la vulnerabilidad y aplicación de parches. Si los parches no se aplican con regularidad, los sistemas de TIC permanecen expuestos a *exploits* malintencionados durante demasiado tiempo, y el riesgo de exposición aumenta considerablemente. La información recabada de las organizaciones participantes a este respecto no permitió confiar debidamente en que esta problemática se estuviera abordando de forma adecuada y coherente. Las respuestas al cuestionario de la DCI de varias organizaciones parecen sugerir más bien la existencia de un enfoque más *ad hoc* de las evaluaciones de la vulnerabilidad (realizadas anualmente o incluso con menor frecuencia), mientras que otras organizaciones, como el Organismo de Obras Públicas y Socorro de las Naciones Unidas para los Refugiados de

Palestina en el Cercano Oriente (OOPS), el Programa Mundial de Alimentos (PMA), la Organización de Aviación Civil Internacional (OACI) y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) cuentan con una gestión eficaz y continua de la vulnerabilidad entre las buenas prácticas de sus organizaciones. **Hay margen de mejora en esta esfera, y los Inspectores instan a los jefes ejecutivos a que presten suficiente atención y asignen recursos adecuados para permitir la realización de evaluaciones periódicas de la vulnerabilidad, con miras a establecer la gestión de la vulnerabilidad como un ejercicio sistemático en las organizaciones del sistema de las Naciones Unidas.**

Tecnologías de la información en la sombra

49. **Razones para recurrir a las tecnologías de la información en la sombra.** El término tecnologías de la información en la sombra *(shadow IT)* se refiere a las aplicaciones o soluciones de TIC desarrolladas o adoptadas en el seno de una organización, pero fuera de su marco oficial de TIC, normalmente gestionado de forma centralizada. En la mayoría de los casos, las TI en la sombra son el resultado de que los usuarios intentan resolver un problema práctico utilizando herramientas que son fácilmente accesibles en el mercado a bajo coste o gratuitamente, cuando consideran que las soluciones disponibles a través de los canales establecidos y las capacidades estructuradas de las TIC no satisfacen sus necesidades en materia de puntualidad o costo o no se adaptan a las necesidades del cliente. También puede ser el resultado de un deseo de innovar rápidamente en respuesta a la evolución de las necesidades o para garantizar la armonización o la compatibilidad con las herramientas utilizadas por los socios de ejecución, que pueden no ser las mismas que las sancionadas corporativamente por una organización. Algunos ejemplos son la apertura de cuentas gratuitas con proveedores de servicios que ofrecen soluciones de almacenamiento de datos, transferencia de archivos, diseño web o gestión de contenidos, o el desarrollo de aplicaciones internas para su uso por parte de departamentos individuales u oficinas sobre el terreno o en el marco de un proyecto. Normalmente, estas soluciones no se someten a un examen de conformidad con las políticas y procedimientos de ciberseguridad establecidos por la autoridad oficial y centralizada a nivel corporativo, por lo que puede considerarse que operan en un entorno no autorizado, o "en la sombra".

50. **Riesgos asociados al uso de las TI en la sombra.** En algunas organizaciones, se dice que el fenómeno ha proliferado, sobre todo en las oficinas exteriores o en los departamentos que están más alejados del control central por otros motivos. Los riesgos en estos entornos suelen verse amplificados por el hecho de que los departamentos centrales de TIC y de ciberseguridad tienen un conocimiento limitado de las actividades individuales de desarrollo de TIC. Una vez más, la pandemia de COVID-19, al crear una repentina necesidad de realizar muchas funciones a distancia, agudizó aún más este problema, ya que muchos usuarios comenzaron a utilizar herramientas para la colaboración en línea, incluida la celebración de conferencias, al margen de las soluciones que ofrecen los paquetes de *software* corporativos. Sin embargo, muchos de los servicios a los que los usuarios recurrían como posibles alternativas no habían sido evaluados ni autorizados por los expertos en ciberseguridad de las organizaciones para su uso masivo, lo que podía poner en riesgo a las organizaciones (por ejemplo, al adherirse a normas diferentes a las recomendadas a nivel de la entidad en materia de autenticación o confidencialidad). Por ejemplo, el uso de una popular plataforma de videoconferencia en línea fue estudiado por el Grupo de Interés Especial sobre la Seguridad de la Información en los primeros días de la pandemia para evaluar si se ajustaba a las organizaciones del sistema de las Naciones Unidas de forma que pudieran usarla, pero los expertos en ciberseguridad no pudieron llegar a una recomendación concluyente e inequívoca —a favor o en contra— que pudiera considerarse válida para el sistema en su conjunto. En su lugar, formularon una serie de opciones junto con advertencias y medidas de precaución a tener en cuenta al utilizar la plataforma en línea en entornos específicos.

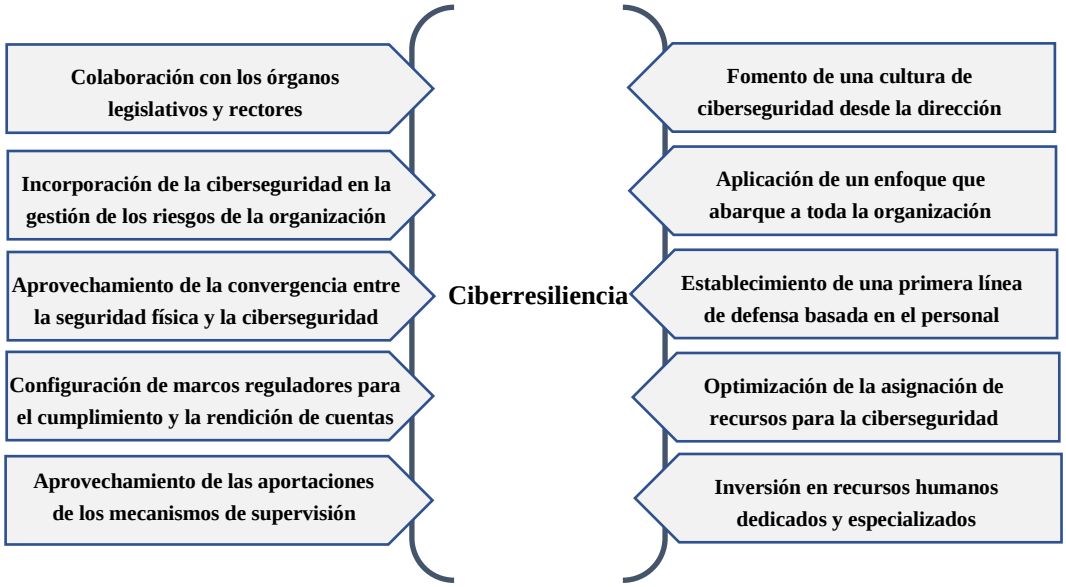
51. **Algunas sugerencias para una gestión más atenta de las TI en la sombra. Los Inspectores consideran que hay que prestar más atención a los problemas de ciberseguridad relacionados con las prácticas de las TI en la sombra, equilibrando la necesidad de control en un entorno propenso a los ciberriesgos con las necesidades legítimas y la motivación constructiva de los usuarios para innovar y recurrir a soluciones alternativas cuando estén disponibles.** De hecho, se abogó por no descartar

automáticamente como comportamiento indeseable el impulso de algunos usuarios de recurrir a soluciones informáticas en la sombra, ya que se consideró un signo saludable de una disposición a innovar, para la que las unidades de negocio deberían disponer en general de cierto espacio y capacidad, idealmente en un entorno informático seguro y vigilado. Entre las ideas que se pueden aprovechar a tal efecto se encuentran las siguientes: crear o ampliar entornos seguros para la innovación digital; mejorar la visibilidad del desarrollo de las TIC distribuidas que se produce en entornos más descentralizados a través de los puntos focales de las TIC locales; y mejorar las medidas de formación y concienciación de los usuarios finales de forma que incluyan información sólida y clara sobre los aspectos de seguridad y riesgo que conlleva el uso de servicios de terceros al margen de los procedimientos y prácticas normalizadas, junto con información sobre las alternativas corporativas aprobadas, así como recomendaciones para un uso más seguro de dichas soluciones.

III. Factores que contribuyen a aumentar la ciberresiliencia

52. **La ciberresiliencia como consecuencia lógica de una cultura de ciberseguridad.** Además de una preparación tecnológica que incluya la identificación de soluciones digitales y fuentes de datos para la protección de los recursos institucionales, una posición de ciberseguridad sólida es el resultado de un enfoque multifacético en el que intervienen todos los niveles de la organización, incluidos los órganos legislativos y rectores, los mecanismos de supervisión, la dirección ejecutiva, las dependencias sustantivas o institucionales y los directores de programas, el personal en general, así como los asociados en la ejecución y los proveedores de servicios externos. Dicho de otro modo, es indispensable adoptar un enfoque que abarque a toda la organización para crear las condiciones que permitan aumentar la ciberresiliencia. Además, la ciberseguridad afecta a varios ámbitos y competencias de la organización, como las TIC, la gestión de riesgos, la seguridad física y la gestión de la información y del conocimiento en sentido más amplio. La multiplicidad de consideraciones y la sensibilización de todas las partes interesadas respecto a su papel y la importancia de su contribución para elevar el listón de la ciberseguridad de cada organización pueden considerarse aspectos de una cultura de la ciberseguridad que, una vez instituida y puesta en práctica, ayuda a conseguir ciberresiliencia en la organización. En este capítulo, los Inspectores presentan sus conclusiones sobre el grado en que los marcos y prácticas de las organizaciones participantes reflejan los factores que contribuyen a aumentar la ciberresiliencia (perspectiva vertical), que se resumen en el gráfico IV, y sugieren posibles mejoras.

Gráfico IV
Factores que contribuyen a aumentar la ciberresiliencia



Fuente: Elaborado por la DCI.

Nota: Según una de las principales normas del sector, la ciberresiliencia es la capacidad de anticipación, resistencia, recuperación y adaptación respecto de condiciones adversas, tensiones, ataques o riesgos en sistemas que utilicen recursos cibernéticos o se basen en estos.

A. Colaboración con los órganos legislativos y rectores

A los órganos legislativos y rectores les corresponde proporcionar orientaciones estratégicas y recursos

53. **La ciberseguridad merece la atención de los órganos legislativos y rectores.** La DCI ha señalado repetidamente que los órganos legislativos y rectores de las organizaciones intergubernamentales pueden desempeñar un papel decisivo proporcionando orientaciones estratégicas y recursos adecuados para que cualquier organización pueda llevar a cabo las actividades previstas en su mandato. Como se indica en un reciente informe de la DCI sobre

la gestión de los riesgos institucionales[13], los órganos legislativos y rectores deberían participar y, como mínimo, conocer los principales riesgos estratégicos de la organización, así como las estrategias y los marcos establecidos para gestionarlos. **En opinión de los Inspectores, para ello se requiere participación y orientaciones en el ámbito de la ciberseguridad, dado el carácter crítico que esta tiene en relación con la gestión de riesgos y como factor clave para el cumplimiento de los mandatos de las organizaciones.** En el recuadro 3 se sugieren formas concretas en las que los respectivos órganos pueden reforzar su compromiso y apoyar los esfuerzos institucionales en ese terreno. No obstante, dado que la ciberseguridad se sigue percibiendo como una cuestión predominantemente técnica y, por tanto, operacional más que estratégica, hasta la fecha en la mayoría de las organizaciones apenas se ha apelado a los órganos legislativos y rectores para que se impliquen en el tema, y estos raramente han hecho llamamientos a la participación.

Recuadro 3
Oportunidades de participación de los órganos legislativos y rectores en las cuestiones relativas a la ciberseguridad

- Formular una declaración explícita sobre la tolerancia y el apetito de la organización con respecto al riesgo de ciberseguridad que refleje adecuadamente el nivel de riesgo que se considera aceptable en su contexto específico. Apenas constan declaraciones de ese tipo en las organizaciones participantes, con la excepción del Programa de las Naciones Unidas para el Desarrollo (PNUD) y la Organización Mundial de la Propiedad Intelectual (OMPI), donde se había aplicado una compleja y bien desarrollada metodología para expresar adecuadamente el apetito de riesgo.
- Proporcionar una orientación estratégica de alto nivel sobre los aspectos prioritarios en relación con la ciberseguridad. Un buen ejemplo de esa orientación es la sección sobre "seguridad de la información" incluida en la estrategia de tecnología de la información y las comunicaciones de la Secretaría de las Naciones Unidas, que fue aprobada por la Asamblea General en 2014 (A/69/517).
- Asignar recursos financieros suficientes sobre la base de un estudio de viabilidad sólido, presentado por la dirección ejecutiva, que permita la implementación de los objetivos formulados en la orientación estratégica ofrecida por los órganos legislativos y rectores en consonancia con el apetito de riesgo.

54. **La participación de los órganos legislativos y rectores en la práctica.** El alcance y el nivel de implicación de los órganos legislativos y rectores en materia de ciberseguridad difieren, al depender en gran medida del mandato y las necesidades operacionales de la organización. Pocas organizaciones han reconocido, y mucho menos aprovechado, el potencial de la cooperación activa con los órganos legislativos y rectores en materia de ciberseguridad, y entre las que sí lo han hecho, en la mayoría de los casos fue después de que un ataque importante requiriera una mayor atención e interacción desde un punto de vista político. Aunque las modalidades de cooperación difieren y no haya un nivel o grado de interacción "correcto", ya empieza a reconocerse que el intercambio regular de información entre los responsables de la ciberseguridad de una organización y sus miembros constituyentes no solo es beneficioso, sino que puede resultar necesario. A continuación, los Inspectores establecen una distinción entre los mecanismos de información periódica sobre ciberseguridad y los procedimientos que deben seguirse para comunicar incidentes a los órganos legislativos y rectores.

Mecanismos de presentación de informes y comunicación a los órganos legislativos y rectores

55. **Mecanismos existentes para la presentación de informes.** Los Inspectores constataron que solo una minoría de las organizaciones incluían algún tipo de informe periódico sobre ciberseguridad destinado a sus órganos legislativos y rectores. Esos informes adoptan diferentes formas: a) algunas organizaciones pueden incluir información relevante

[13] JIU/REP/2020/5.

sobre el presupuesto por programas y el rendimiento (normalmente en un apartado relacionado con las TIC, que puede o no incluir explícitamente la ciberseguridad); b) otras organizaciones elaboran informes específicos a petición del órgano legislativo y rector, por ejemplo para mostrar los avances en la aplicación de las estrategias u hojas de ruta aprobadas o adoptadas, y c) hay organizaciones que se basan en los informes anuales de sus órganos de supervisión interna y externa, y los utilizan como canal principal para defender que se preste una mayor atención al tema.

56. **Los parámetros relacionados con la ciberseguridad no se miden ni se presentan sistemáticamente.** También hay disparidad en cuanto al contenido de esos informes a los órganos legislativos y rectores, y son pocas las organizaciones que comparten aspectos concretos de los parámetros que miden y analizan internamente en relación con su exposición y rendimiento en materia de ciberseguridad. Por un lado, esta falta de uniformidad en la presentación de informes puede deberse a las legítimas dudas de muchas organizaciones sobre la conveniencia de crear un registro público o incluso reservado de parámetros de ciberseguridad que pueda revelar vulnerabilidades y, por tanto, aumentar la exposición al riesgo. Por otro lado, quizá refleje el hecho de que a las organizaciones todavía les cuesta determinar el nivel de detalle adecuado y la selección más pertinente de parámetros de los que se debe informar, así como los que hay que medir en primer lugar por ser más significativos. La mayoría de las organizaciones participantes presentan datos relacionados principalmente con el número de incidentes de ciberseguridad que se producen durante un período de tiempo, su frecuencia y su gravedad, que se reúnen con fines internos, y algunas organizaciones todavía no han establecido o formalizado sistemas más específicos de recopilación de estadísticas al respecto. No obstante, el tipo de datos que se reúnen y analizan varía mucho de una organización a otra, y la forma de procesar esos datos para que sirvan de orientación en la toma de decisiones, ya sea a nivel interno o en los órganos legislativos y rectores, en muchos casos aún no se ha definido. Dado que esos parámetros proporcionan uno de los principales elementos sobre los que se puede explicar el apetito de riesgo de una organización, **los Inspectores consideran prudente seguir estudiando diferentes conjuntos de parámetros de ciberseguridad en los foros pertinentes y desarrollar una metodología básica que pueda adaptarse al contexto de cada organización según las necesidades.**

57. **Comunicación de incidentes a los órganos legislativos y rectores y ventajas de la transparencia con respecto a estos.** Cuando se produce un incidente de ciberseguridad, no se informa sistemáticamente a los órganos legislativos y rectores, según se evidencia en las respuestas al cuestionario de la DCI ofrecidas por las organizaciones participantes. Además, los Inspectores constataron que había pocas pruebas de que se hubieran predefinido procesos de comunicación a los órganos legislativos y rectores ante ese tipo de eventualidades. La decisión de trasladar la información a esos órganos se suele tomar caso por caso. La experiencia de las organizaciones que han tenido la oportunidad, a menudo forzada por un suceso importante que afectaba a la ciberseguridad, de poner a prueba sus canales de comunicación con los órganos rectores apunta a que deben tenerse especialmente en cuenta los siguientes factores para determinar si se transmite o no la información a las instancias superiores: a) la gravedad del incidente; b) el impacto en las operaciones; c) el impacto en los procesos intergubernamentales, y d) si es probable que el incidente se haga público. Otras consideraciones decisivas son el momento en que debe notificarse el problema y la precaución de no revelar vulnerabilidades específicas ni detalles sobre la capacidad de respuesta de la organización que puedan atraer más atención hacia el objetivo. Los expertos en ciberseguridad entrevistados consideraron, en general, que un buen momento para notificar el incidente sería antes de que se resolviera completamente, o más bien, tan pronto como se comprendiera lo bastante de qué se trataba. Hacerlo inmediatamente después de que se descubra la intrusión puede resultar prematuro y comprometer las medidas que se estén adoptando para su resolución, aumentando así inadvertidamente la exposición. Al mismo tiempo, retrasar la notificación del problema hasta el momento en que el incidente esté completamente resuelto puede arrojar dudas sobre la fiabilidad o la voluntad de la dirección ejecutiva de actuar con transparencia y asumir responsabilidades ante posibles lagunas de ciberseguridad. En líneas generales, el mensaje de las organizaciones participantes que se habían “abierto” a sus órganos legislativos y rectores en relación con incidentes y deficiencias de sus ciberdefensas era que no se tuviera miedo de comunicarlos, ya que el costo para la

reputación, así como la pérdida de confianza por parte de los Gobiernos donantes, superaba con creces la posible vergüenza y el impacto perjudicial —incluido el financiero indirecto— de un ataque.

58. **Necesidad de prever protocolos de notificación a los niveles jerárquicos superiores y a los órganos legislativos y rectores. En opinión de los Inspectores, es importante definir de antemano el mecanismo a través del cual se pondrán en conocimiento de los órganos legislativos y rectores los ciberataques que sean de consideración.** Dado que es posible anticipar la probabilidad de que se produzcan ese tipo ataques, se deduce que se puede hacer lo mismo con el protocolo para la notificación a las instancias superiores. En concreto, los criterios (lo que desencadena la notificación) y la mecánica que rige quiénes son los actores, qué pasos se deben dar, en qué orden y con qué aportaciones no tienen por qué depender de un proceso de toma de decisiones reactivo. Si ante una crisis aguda se cede a la improvisación, es más probable que esa toma de decisiones se vea lastrada por la presión de tener que ejercer un control de daños *ad hoc* en lugar de seguir globalmente un protocolo establecido que permita además centrarse en la gestión de las variables específicas del caso que sean ineludibles. Además, tener que idear esas medidas en una situación de crisis deja el proceso más expuesto a influencias indebidas en un entorno ya complejo y potencialmente politizado, lo que podría evitarse en gran medida adoptando un enfoque proactivo. Por último, y sin perjuicio de los protocolos internos habilitados para la notificación a instancias superiores, tal vez sea prudente que los órganos legislativos y rectores se planteen un debate sobre sus propias normas de actuación en este tipo de asuntos, en previsión de que se les notifiquen casos graves de ciberataques para que los examinen y procedan en consecuencia. Este enfoque prospectivo puede ayudar a que, tras un examen detenido, se acuerde establecer algunos límites a la acción de los órganos legislativos y rectores, que pueden facilitar la despolitización y la toma de decisiones bien fundadas en un terreno potencialmente resbaladizo.

B. Incorporación de la ciberseguridad en la gestión de los riesgos de la organización

59. **Ventajas de un enfoque basado en la gestión de riesgos para la ciberseguridad.** En un reciente informe de la DCI se caracterizaba la gestión de los riesgos institucionales como un proceso estructurado, integrado y sistemático de identificación, análisis, evaluación, tratamiento y supervisión de los riesgos en toda la organización para lograr los objetivos de esta[14]. Las funciones básicas asociadas a la ciberseguridad (que, normalmente, son variaciones de las tareas de identificación, prevención, detección, respuesta y recuperación) reflejan las principales etapas y objetivos de la gestión de riesgos. Tratar la ciberseguridad como una cuestión de gestión de riesgos de nivel institucional también tiene ventajas prácticas concretas. Por un lado, al ser reconocida como una preocupación estratégica para toda la organización, la ciberseguridad se convierte en un asunto que concierne a todas las dependencias institucionales y a todos los empleados, lo que fomenta y respalda un enfoque que abarca a toda la organización y la aceptación a través de la responsabilidad distribuida con respecto a los riesgos. **Además, los Inspectores afirman que la incorporación formal de la ciberseguridad en el marco de gestión de los riesgos institucionales de la organización contribuye a priorizar el tema y proporciona un punto de referencia formal, sobre cuya base los órganos legislativos y rectores y el personal directivo superior pueden abrir conjuntamente un cauce para gestionar de la mejor manera posible los principales riesgos.** Dado que estos marcos tienden a conceptualizarse como documentos vivos, también ofrecen la oportunidad de reconsiderar, adaptar y ajustar de forma sistemática y recurrente las medidas de mitigación de riesgos atendiendo a la rápida evolución de las necesidades de la organización.

60. **El paradigma de la gestión de riesgos ya ha sido reconocido en parte.** La utilidad de abordar la ciberseguridad a través del prisma de la gestión de riesgos ya ha sido reconocida en diversos foros, aunque en la práctica las implicaciones de ver la ciberseguridad desde ese punto de vista todavía no han sido plenamente comprendidas y asimiladas en muchas partes

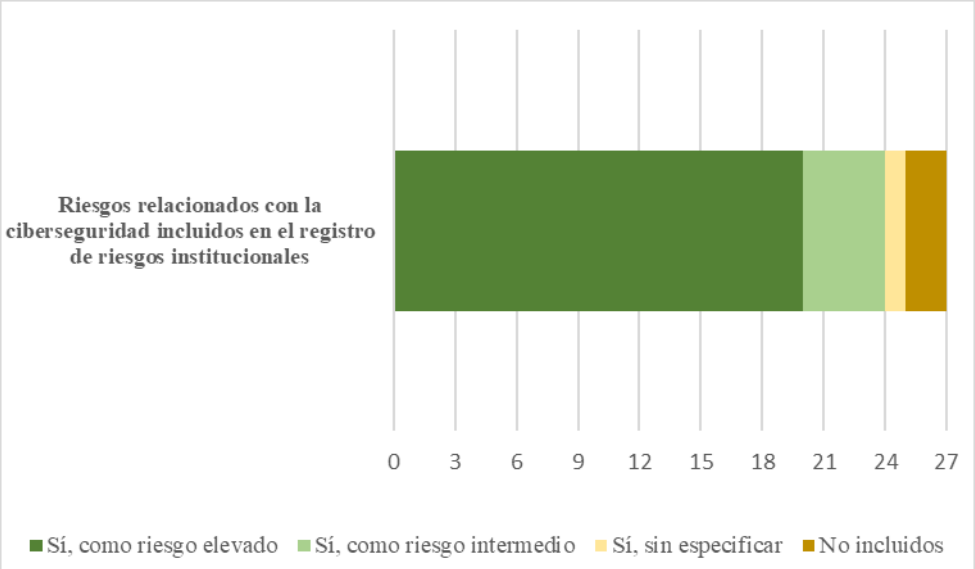
[14] JIU/REP/2020/5.

del sistema. Por ejemplo, las actas de las reuniones de los recientes simposios del Grupo de Interés Especial sobre la Seguridad de la Información a las que asistieron expertos en ciberseguridad incluían varios puntos del orden del día relativos a la gestión de riesgos, entre ellos un llamamiento a sus miembros para que trabajaran con los representantes de sus respectivas organizaciones que formaban parte del Comité de Alto Nivel sobre Gestión del Foro de Gestión de Riesgos, con el fin de que se incluyeran los riesgos de ciberseguridad en las perspectivas que contribuyen al modelo de madurez en la gestión de riesgos del Foro[15]. Los comités de auditoría y supervisión de varias organizaciones también subrayaron la necesidad de incluir consideraciones de ciberseguridad en los marcos más amplios de gestión de riesgos institucionales y de continuidad de las operaciones. De hecho, la mayoría abordaron la ciberseguridad como parte de su mandato sobre la gestión de los riesgos institucionales y destacaron la necesidad de que hubiera una mayor integración entre las funciones de TIC y gestión de riesgos. Además, las normas sobre ciberseguridad más recientes, como la ISO 27001, los Objetivos de Control para la Tecnología de la Información y Tecnologías Conexas y el marco del Instituto Nacional de Normas y Tecnología de los Estados Unidos, tratan los riesgos de ciberseguridad como riesgos empresariales o institucionales, que van mucho más allá del ámbito de la infraestructura informática, y destacan la dimensión estratégica de la mejora de la posición de ciberseguridad de las organizaciones, que se considera que es más fácil conseguir cuando se correlaciona plenamente con la gestión de riesgos a nivel institucional.

61. **Atención a la gestión de riesgos en las organizaciones participantes.** El grado en que la ciberseguridad se asume como una cuestión relacionada con la gestión de riesgos varía en las organizaciones participantes encuestadas por la DCI. En sus respuestas, la gran mayoría (24 de 27) declararon que los riesgos relacionados con la ciberseguridad se incluían oficialmente en su registro de riesgos institucionales. De estas, 20 confirmaron que el nivel de riesgo asignado era “elevado” (gráfico V), y 19 habían incluido en su registro de riesgos institucionales medidas específicas de mitigación de riesgos de ciberseguridad. Solo 11 organizaciones participantes facilitaron a los Inspectores documentación interna sobre la gestión de riesgos y, de manera confidencial, compartieron extractos de sus registros de riesgos. Dado que el conjunto de datos era incompleto, las conclusiones extraídas deben considerarse preliminares. No obstante, al comparar algunas de las muestras de los registros de riesgos proporcionadas, se pudieron apreciar ciertas diferencias en la evaluación, categorización y planificación de los riesgos de ciberseguridad. Por un lado, algunas organizaciones hicieron hincapié en los aspectos estratégicos, como el impacto potencial de los incidentes de ciberseguridad en la reputación, la productividad y las finanzas de la organización. En el otro extremo del espectro, hay ejemplos de registros de riesgos que se centran casi por completo en la seguridad de las TIC, y en los que se da prioridad al mantenimiento de la disponibilidad de la información, más que en su confidencialidad e integridad. El cumplimiento de estos dos últimos objetivos tiende a requerir medidas más complejas que las políticas que se orientan a evitar únicamente los problemas técnicos y el “tiempo de inactividad”, lo que puede explicar que estos aspectos se hayan abordado en menor medida en la documentación examinada. Un inconveniente de los registros de riesgos que se centran principalmente en los aspectos técnicos de la ciberseguridad es que pueden pasar por alto la relación que pueda existir entre estos y ciertas consecuencias de mayor alcance para la organización.

[15] CEB/2019/HLCM/DTN/02.

Gráfico V
Inclusión de la ciberseguridad en los registros de riesgos institucionales, en número de organizaciones participantes



Fuente: Cuestionario de la DCI, 2020.

62. **Las medidas de mitigación requieren más atención.** Un aspecto que se puso de relieve, incluso con los limitados datos de que disponían los Inspectores, fue el nivel de articulación de las medidas de mitigación de riesgos de ciberseguridad, ya fuera en un marco de gestión de riesgos o fuera de este. De acuerdo con lo señalado por los comités de auditoría y supervisión, las medidas de mitigación suelen describir el *status quo* (por ejemplo, se detallan las medidas ya aplicadas, en lugar de ofrecerse proactivamente una previsión de acciones ante posibles riesgos específicos), lo que da lugar a un proceso interesado de fijación de objetivos ya alcanzados que tiene por finalidad mejorar la presentación de información, no a un esfuerzo serio por concebir acciones de mitigación significativas que puedan tomarse como referencia para una implementación gradual. Conscientes de que algunas organizaciones pueden haber optado deliberadamente por presentar sus medidas de mitigación en términos poco precisos para proteger las defensas de la entidad, **los Inspectores opinan que en el futuro se debería hacer hincapié en la formulación de medidas de mitigación de una manera prospectiva que siga reflejando las limitaciones y debilidades existentes, reconociendo el hecho de que esto puede implicar un esfuerzo adicional para alcanzar los objetivos recién establecidos, así como un período de transición en la presentación de informes que puede mostrar objetivos que no se hayan alcanzado plenamente.**

63. **Hojas de ruta.** En algunas organizaciones, las evaluaciones de los riesgos de ciberseguridad condujeron a la adopción de una hoja de ruta institucional cuyo objetivo era aumentar la ciberresiliencia de la organización. La preparaba la dirección a partir de las opiniones y comentarios de todas las partes interesadas internas pertinentes y, en muchos casos, se presentaba a los órganos legislativos o rectores para su aprobación. Los Inspectores consideraron que esas hojas de ruta resultaban más valiosas cuando se diseñaban como un plan plurianual vinculado a hitos e indicadores de progresos, junto con un cambio en la asignación de recursos para que las medidas de mitigación pudieran implementarse. En el momento en que se redactó el presente informe, esos procesos de elaboración de hojas de ruta ya habían concluido o se estaban llevando a cabo en varias organizaciones (la OACI, la Organización de las Naciones Unidas para la Agricultura y la Alimentación (FAO), el Fondo de Población de las Naciones Unidas (UNFPA), la Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), la Oficina de las Naciones Unidas de Servicios para Proyectos (UNOPS) y la Organización Mundial de la Propiedad Intelectual (OMPI)) y se consideraban una buena práctica para optimizar las acciones de mejora en toda la organización.

64. **Transición del conocimiento a la gestión proactiva de los riesgos.** En conclusión, aunque muchas organizaciones participantes se han dado cuenta de la importancia de las consideraciones acerca de la ciberseguridad y han intentado incluirlas, con distintos grados de articulación, en sus marcos generales de gestión de riesgos, el panorama en el conjunto del sistema sigue siendo desigual y se requiere más atención para pasar de la conciencia sobre los riesgos de ciberseguridad a una verdadera gestión de estos según los requisitos de cada entidad, a sabiendas de que en este ámbito no se puede eliminar totalmente el riesgo. **Por lo tanto, los Inspectores coinciden con los expertos en ciberseguridad y se hacen eco de la cautela que estos piden: es mucho lo que está en juego y se requiere un enfoque basado en los riesgos (anexo II).** En el futuro hay que hacer hincapié en el desarrollo de medidas de mitigación de riesgos que sean coherentes y eficaces, así como en una sólida planificación de la continuidad de las operaciones. La contribución de los expertos en ciberseguridad y su plena participación en los procesos internos de gestión de riesgos, desde el diseño hasta el seguimiento, pasando por la implementación, serán cruciales para alcanzar esos objetivos.

C. Aprovechamiento de la convergencia entre la seguridad física y la ciberseguridad

65. **Líneas difusas entre la seguridad física y la ciberseguridad.** La cuestión, en cierto modo filosófica, de si la ciberseguridad debía considerarse predominantemente una cuestión "cibernética" —es decir, impulsada por la tecnología— o una cuestión de seguridad (comparable a la seguridad física, pero trasladada al ámbito digital) surgió pronto, incluso durante la fase de conceptualización del presente estudio, y suscitó un intenso debate entre las partes interesadas que entrevistaron los Inspectores. Aunque las organizaciones del sistema de las Naciones Unidas han tratado tradicionalmente la seguridad física y la ciberseguridad como esferas separadas, ambas se orientan a la protección del personal y de otros activos de las organizaciones. Para cumplir esos objetivos, en los dos ámbitos se gestionan la incertidumbre y el riesgo anticipando ataques, ofreciendo protección ante estos y ofreciendo respuestas cuando se producen, de modo que la gestión de riesgos es un denominador común de estas esferas. La seguridad física y la ciberseguridad también comparten la premisa de que incluso las mejores medidas de protección no impedirán por completo que algún ataque sortee las defensas de una organización, por muy avanzadas o sólidas que sean. Por último, al evocar escenarios que podrían ilustrar dónde termina la ciberseguridad y dónde empieza la seguridad física o viceversa, en seguida se puso de manifiesto que quizá no sea tan fácil de separar los ámbitos físico y digital como pudiera parecer a primera vista.

66. **La seguridad física y la ciberseguridad se cruzan en la práctica.** En la actualidad, los sistemas de apoyo a las tareas de seguridad y protección que funcionan sin depender de algún modo del uso de las TIC son la excepción, no la regla. Por ello, es probable que las consecuencias de los problemas de ciberseguridad que afectan a estos sistemas se materialicen en el mundo físico, a veces hasta el punto de exponer a un considerable peligro la vida o la integridad física de las personas. No faltan ejemplos de cómo se entrecruzan en la práctica la ciberseguridad y la seguridad física. Por ejemplo, los piratas informáticos pueden tomar el control de una puerta de seguridad, aprovechar las debilidades de los protocolos de seguridad para introducir programas espía en dispositivos electrónicos o para descargar información confidencial en dispositivos portátiles, obtener acceso en línea a planos de oficinas con el fin de determinar cuál es el mejor objetivo para un ataque armado, o participar en un robo de identidad virtual con el fin de engañar a otras personas, que terminan poniéndose en peligro involuntariamente por dar crédito a fuentes que normalmente serían confiables y que han sido suplantadas por los ciberdelincuentes. Además, unas medidas de seguridad insuficientes que comprometan la protección de locales, centros de datos, salas de servidores o puntos de acceso digital frente a accesos no autorizados u otras formas de interferencia indebida asociadas a peligros físicos (naturales o provocados por el hombre) pueden tener repercusiones adversas directas que se perciban en la esfera digital. La convergencia de los dos mundos puede ser aún más pronunciada sobre el terreno, en lugares que tienden a estar más alejados de los mecanismos centrales de control y supervisión de la ciberseguridad y que son también un objetivo potencialmente más atractivo, dado que la información que albergan es esencial para la seguridad vital y la integridad física. Un ejemplo

serían los datos sobre el paradero o los movimientos del personal en las zonas menos protegidas.

67. **La institucionalización de vínculos entre la seguridad física y la ciberseguridad sigue siendo esporádica.** En las organizaciones participantes, las respuestas a los cuestionarios de la DCI y las posteriores entrevistas con funcionarios revelaron un grado variable de comprensión de las interrelaciones entre el ámbito físico y el ciberespacio. Únicamente la arquitectura institucional de dos organizaciones refleja una integración efectiva de los marcos de gestión de la seguridad física y la ciberseguridad, ya sea mediante la inclusión de las dos funciones en un departamento que depende directamente de un cargo de nivel ejecutivo adjunto con un mandato general para la seguridad de la Organización (OMPI), o mediante la articulación estratégica de ambas funciones como dos elementos contribuyentes, entre otros muchos, a un "marco de gestión de la resiliencia de la organización" más amplio que combina defensas contra toda clase de amenazas, ya sean físicas, digitales, políticas, naturales o de otro tipo (UIT). Otras organizaciones han reconocido que hay puntos de convergencia y que se pueden lograr sinergias y han formalizado en cierta medida las actividades de coordinación e intercambio de información entre las dos funciones, por ejemplo mediante líneas de comunicación con supervisores indirectos, sesiones informativas conjuntas para la alta dirección o reuniones con participación mixta, así como estableciendo que ambas funciones contribuyan en condiciones de igualdad en procesos tales como la gestión de riesgos o la planificación de la continuidad de las operaciones, o en situaciones de respuesta ante emergencias en que se requieran aportaciones de ambas esferas. Asimismo, ya se está colaborando en medidas específicas de carácter operacional (por ejemplo, la consolidación de información sobre amenazas cibernéticas y físicas para alertar a los viajeros en misión o el desarrollo conjunto de soluciones tecnológicas avanzadas para la identificación del personal y tarjetas de acceso a instalaciones), que se han traducido en beneficios tangibles en las condiciones de seguridad de las organizaciones en cuestión. Incluso en partes del sistema en las que la seguridad física se considera aparte del ciberespacio y en gran medida ajena a este, las organizaciones han documentado la existencia de contactos ocasionales e informales entre ambas esferas. Sin embargo, para la mayoría de las organizaciones encuestadas sobre ese particular, la realidad sigue siendo que el vínculo entre la seguridad física y la ciberseguridad se subestima o se reconoce solo marginalmente, lo que también ocurre en el conjunto del sistema (párrs. 159 a 164).

68. **Ampliación de la capacidad en ciberseguridad dentro de la función de seguridad física.** En opinión de los Inspectores, se puede aprovechar la convergencia entre la seguridad física y la ciberseguridad para progresar en las dos esferas y aumentar la resiliencia de las organizaciones en general. Una opción consistiría en explorar la posibilidad de desarrollar la capacidad interna mejorando las cualificaciones y ampliando el perfil de un número crítico de profesionales de la seguridad y la protección e incorporar aspectos relativos a la ciberseguridad en su futuro conjunto de aptitudes, en particular reformulando las descripciones de los puestos de trabajo (por ejemplo, añadiendo elementos de procesamiento de información sobre ciberamenazas, modelado de amenazas y capacidades analíticas similares). La percepción de que la ciberseguridad es intrínsecamente ajena a las funciones de estos profesionales y está disociada de ellas puede deberse en parte a que, tradicionalmente, el personal que se contrata procede de las fuerzas policiales y militares, y a que no se reconoce que estas últimas ya han desarrollado capacidades modernas en los dominios requeridos. La especialización existe, y está a disposición de las organizaciones del sistema de las Naciones Unidas, que pueden obtenerla a través de la selección de personal. Una vez creada, esta capacidad adicional complementaría, en lugar de sustituir, la avanzada y bien engrasada maquinaria de la actual fuerza de trabajo tradicional dedicada a la seguridad, y le permitiría interactuar más eficazmente con una capacidad dedicada a la ciberseguridad dentro de las respectivas organizaciones del sistema de las Naciones Unidas. Los Inspectores reconocen que en los dos ámbitos hay capacidades distintas y altamente especializadas que se han diseñado con solidez para cumplir los respectivos objetivos de protección, y que, por lo tanto, no parece prudente intentar fusionar esas esferas en una misma estructura ni incluir una en la otra sin un estudio más detenido. No obstante, la ampliación de las capacidades existentes para mejorar la articulación entre los dos ámbitos puede ser uno de los aspectos

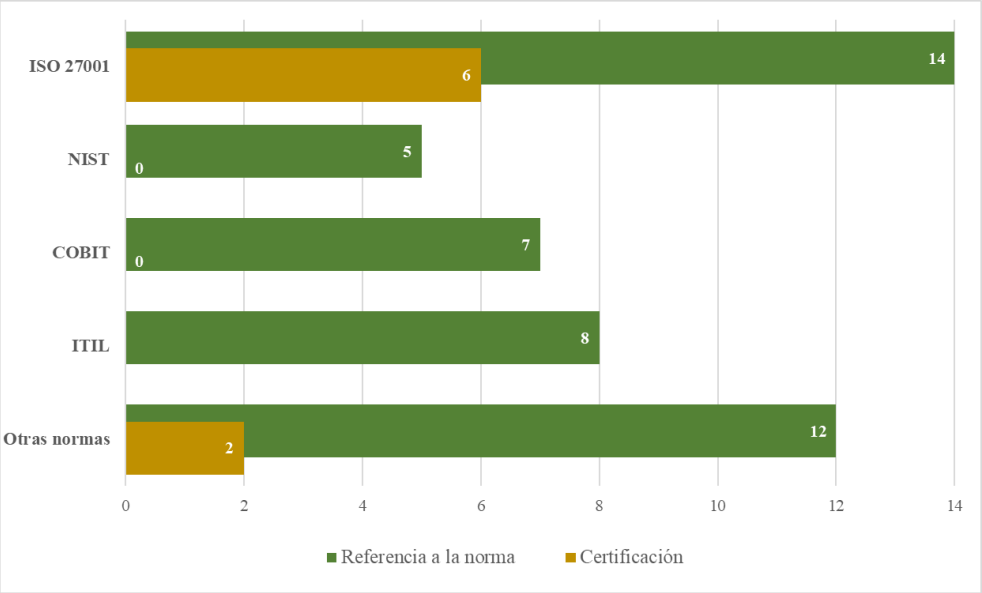
que convendría explorar, con miras a un enfoque más holístico de la protección del personal y los activos de las organizaciones, como se prevé en la recomendación 5.

D. Configuración de marcos reguladores para el cumplimiento y la rendición de cuentas

Normas del sector sobre la seguridad de la información

69. **Normas utilizadas en las organizaciones participantes.** La ciberseguridad es un ámbito para el que se ha desarrollado una serie de normas industriales nacionales e internacionales que proporcionan orientación y criterios de referencia con el fin de crear sistemas de gestión de la seguridad de la información resilientes. El término, acuñado por la ISO, se refiere al conjunto de medidas —de gestión, reglamentarias y tecnológicas— que reflejan el enfoque de una entidad en materia de ciberseguridad. Comprende un complejo conjunto de controles, que incluye normas y documentos de política, herramientas y procesos de gestión, conceptos de seguridad y estrategias de gestión de riesgos, entre otros. Las organizaciones participantes mencionaron una amplia gama de normas de este tipo, a veces más de una, que, según indicaron, fueron seleccionadas en función de su relevancia para el entorno y los requisitos específicos de cada organización, y se optimizaron registrando los controles de una norma concreta que eran más relevantes en una "declaración de aplicabilidad" adaptada. Los Inspectores recuerdan que, hace ya un decenio, en 2011, la Red de Tecnología de la Información y las Comunicaciones avaló que los organismos del sistema de las Naciones Unidas siguieran la norma ISO 27001[16], y en 2017, el Grupo de Interés Especial sobre la Seguridad de la Información reafirmó esta posición. En el presente examen se confirma que la mayoría de las organizaciones del sistema de las Naciones Unidas cuentan ya con la certificación ISO 27001, prevén obtenerla, o han optado por adaptar voluntariamente su marco con arreglo a esta sin solicitar una certificación oficial. Además de la norma ISO 27001, las organizaciones del sistema de las Naciones Unidas utilizan otras, que se indican en el gráfico VI y se describen con más detalle en el anexo III. Solo tres Organizaciones no han mencionado ninguna norma o no han transmitido información al respecto.

Gráfico VI
Principales normas del sector utilizadas por las organizaciones participantes en la DCI



Fuente: Cuestionario de la DCI (2020) y entrevistas.

Abreviaturas: NIST *(National Institute of Standards and Technology)*, Instituto Nacional de Normas y Tecnología de los Estados Unidos; COBIT *(Control Objectives for Information and*

[16] CEB/2011/HLCM/ICT/16.

Related Technology), Objetivos de Control para la Tecnología de la Información y Tecnologías Conexas; ITIL *(Information Technology Infrastructure Library)*, Biblioteca de Infraestructura de Tecnología de la Información.

70. **La certificación oficial frente a la referencia a las normas.** En relación con la utilidad de la certificación oficial frente a otras modalidades más flexibles para el cumplimiento voluntario, los Inspectores constataron que había opiniones divergentes entre los expertos. De hecho, de la dirección depende la decisión de procurar una certificación para ofrecer garantías a los órganos legislativos y rectores, así como a los socios externos, sobre la base de la formalidad procedimental y la declaración que contiene la certificación, así como del rigor observado al requerirse auditorías anuales de entidades independientes para mantenerla. También puede servir como detonante recurrente de la innovación, habida cuenta de la exigencia de mostrar continuas mejoras. Al mismo tiempo, algunas organizaciones sostienen que la certificación puede resultar demasiado costosa y compleja, y que por ello no se justificaría la inversión. También critican su gran dependencia de un cumplimiento formal, que puede incentivar la presentación de informes deliberadamente favorables en lugar de realistas. Los Inspectores reconocen que tanto la certificación como la adhesión a normas pueden ser opciones útiles, especialmente en diferentes etapas en el contexto de una ampliación gradual de las ciberdefensas. Resulta especialmente cierto en este caso, dado que las normas pueden aplicarse de diferentes maneras, entre ellas como base de referencia o marco con fines de auditoría, como hoja de ruta interna para realizar mejoras, como incentivo adicional para el cumplimiento de los controles o como inspiración o herramienta de referencia para enfoques adaptados.

71. **Las ventajas de remitirse a las normas.** Los Inspectores se abstienen de abogar por una determinada norma del sector o por un enfoque armonizado al respecto para todo el sistema, ya que diferentes normas pueden ser válidas para diferentes propósitos y ofrecer opciones adecuadas para diferentes niveles de madurez. Así pues, no existe una norma correcta ni un enfoque correcto con respecto a la ciberseguridad, pero hay razones de peso para inspirarse —de manera “oficial” o no— en las normas pertinentes del sector a la hora de establecer y gestionar un marco regulador propio. Por ello, las organizaciones participantes tienen que identificar la norma adecuada y, en esta, los controles más pertinentes en función del nivel de protección requerido atendiendo a su situación, de acuerdo con los requisitos y los riesgos identificados tras las correspondientes evaluaciones de riesgos de ciberseguridad específicos de la organización. Los Inspectores observan, sin pronunciarse al respecto, que la decisión institucional sobre ese particular puede tener también consecuencias en el conjunto del sistema, donde el uso del mismo marco o norma puede facilitar la comparabilidad y proporcionar un lenguaje común para todos. Por otra parte, en el contexto de los mecanismos interinstitucionales, una variedad de enfoques puede ofrecer más oportunidades para el debate entre organizaciones, la puesta a prueba de supuestos, un examen más crítico de las propias opciones frente a las de los demás, y el aprendizaje mutuo en general, lo que en última instancia beneficia a todas y cada una de las organizaciones.

Marcos y procedimientos normativos

72. **La prerrogativa de crear un marco regulador adecuado corresponde a cada entidad.** Aparte de la variedad de normas del sector antes mencionadas, no hay orientaciones autorizadas de aplicación universal sobre cómo regular los asuntos relacionados con la ciberseguridad. La ausencia de un marco o instrumento jurídico internacional en este ámbito puede atribuirse al hecho de que es multifacético y difícil de delimitar, por lo que su regulación resulta compleja, incluso en el contexto del derecho interno de un solo Estado. Si se traslada esta complejidad al plano internacional, resulta aún más difícil definir un marco común que rija las relaciones entre los Estados y otras partes interesadas del sector público y privado que operan en el ciberespacio. En este momento, no existe un instrumento jurídicamente vinculante en el derecho internacional ni un marco único para las organizaciones del sistema de las Naciones Unidas que regule específicamente la ciberseguridad. En consecuencia, se puede describir el marco de gobernanza internacional del ciberespacio como un mosaico de instituciones y normas oficiales y oficiosas compuestas por estándares técnicos, contratos, leyes y decisiones intergubernamentales que se entrecruzan y superponen. A falta de un marco coherente que pueda servir de modelo, cada

entidad conserva la prerrogativa —dentro de los límites de los parámetros dictados por su instrumento constitutivo y las decisiones de los órganos legislativos y rectores asociados— de formular sus propias normas con relativa autonomía y elegir su proyecto de ciberseguridad.

73. **La ciberseguridad se menciona habitualmente en las estrategias sobre las TIC.** La forma en que la ciberseguridad se contempla en los marcos reguladores existentes, es decir, el contexto normativo en el que se desempeñan las funciones de la organización varía y tiende a reflejar la evolución histórica de la ciberseguridad como un ámbito que se originó en la esfera de las TIC y que terminó convirtiéndose en una disciplina autónoma. Algunas organizaciones articulan la ciberseguridad de forma totalmente independiente de las TIC, tratándola como una cuestión aparte y en las mismas condiciones que la seguridad física (OMPI) o como parte de una visión más amplia de la gestión de la resiliencia de la organización (UIT), pero esos enfoques siguen siendo la excepción. La mayoría de las organizaciones participantes han elaborado un documento estratégico institucional plurianual en el que exponen su visión con respecto a las TIC y, en su gran mayoría, en esa visión incorporan consideraciones relativas a la ciberseguridad. Dicho esto, algunas estrategias solo contienen una referencia básica, a veces complementada por una orientación más elaborada de nivel inferior, mientras que otras incluyen capítulos enteros dedicados al tema. **Independientemente del grado de elaboración de las orientaciones sobre ciberseguridad en las estrategias más amplias de las organizaciones en materia de TIC, los Inspectores consideraron que la existencia de referencias a la cuestión en esas estrategias de TIC era un primer paso en la buena dirección.**

74. **En muchas organizaciones participantes existen políticas específicas de ciberseguridad o se están elaborando.** Merece la pena señalar que uno de los requisitos de los documentos básicos de varias importantes normas del sector es que haya políticas específicas y procedimientos documentados con respecto a la ciberseguridad como pilar fundamental de los controles en los que debe apoyarse el sistema de gestión de la seguridad de la información de una entidad[17]. En el presente examen se constató que muchas organizaciones habían elaborado ese tipo de orientaciones específicas, y que la mayoría de las que no lo habían hecho estaban preparándolas. En concreto, se comprobó que 17 organizaciones habían implementado instrumentos normativos específicos en materia de ciberseguridad (3 de los cuales están en proceso de revisión), mientras que 4 confirmaron que estaban elaborando nuevas políticas. Solo 3 organizaciones indicaron que no habían formulado ni empezado a formular políticas ni reglamentos específicos referidos a la ciberseguridad y explicaron que se basaban en sus políticas y procedimientos de TIC para abordar la cuestión. Así pues, salvo en contados casos, se puede decir que las organizaciones han reconocido la importancia de contar con un marco de referencia articulado para orientar su enfoque en el ámbito de la ciberseguridad. En el anexo IV se enumeran los principales instrumentos que rigen la ciberseguridad en el marco regulador de las organizaciones participantes.

75. **Los marcos suelen ser complejos y heterogéneos y presentar varios niveles.** Independientemente de si se han establecido marcos reguladores más elaborados en materia de ciberseguridad o si las organizaciones en cuestión se remiten a los que se aplican a las TIC de forma más general, la mayoría de los marcos que observaron los Inspectores estaban dispersos en una serie de documentos de orientación estratégica, de política, sobre procedimientos y técnica. La terminología asociada a estos documentos varía de una organización a otra, de modo que se habla, por ejemplo, de estrategias, manuales de estrategias, declaraciones de misión, políticas, instrucciones administrativas, procedimientos operativos estándar, directrices, manuales y protocolos. A menudo, estos términos se superponen conceptualmente o incluso se utilizan de manera indistinta. El CICE ha

[17] La norma ISO 27001, en su lista normativa de objetivos de control, comienza con el control A.5, "Políticas de seguridad de la información", indicando que se debe establecer un conjunto de políticas y comunicar estas a los empleados y a las partes externas pertinentes. El Instituto Nacional de Normas y Tecnología de los Estados Unidos, en su documento básico "Framework for Improving Critical Infrastructure Cybersecurity" (Marco para la mejora de la ciberseguridad de infraestructuras críticas), especifica en relación con la categoría de gobernanza que "las políticas, procedimientos y procesos" deben informar "la gestión de los riesgos de ciberseguridad".

desarrollado un modelo para representar en distintos niveles los diferentes componentes normativos de un sistema de gestión de la seguridad de la información, en que el nivel más alto de abstracción se sitúa en la parte superior y el de mayor detalle en la parte inferior, y ha apoyado a varias organizaciones del sistema de las Naciones Unidas en la evaluación y mejora de sus marcos reguladores y de gobernanza. Sobre la base de ese modelo, en el anexo IV se ofrece una visión general de los objetivos, formatos y contenidos que suelen encontrarse en los documentos sobre ciberseguridad y TIC de las organizaciones que han examinado los Inspectores, pues se reconoce que un análisis cualitativo detallado de los contenidos de todas las organizaciones participantes excedería el alcance del presente examen.

76. **Adaptación al contexto y revisión periódica.** Para que las políticas reflejen las particularidades de una organización puede ser necesario ajustarlas de manera que reproduzcan exactamente los controles que requieren las normas del sector que la organización haya decidido seguir, si procede. Ejemplos de esta situación se encontraron en el PMA y en el Programa de las Naciones Unidas para el Desarrollo (PNUD), donde, para cada control técnico de la norma ISO 27001 que la organización había elegido incluir en su "declaración de aplicabilidad", en el marco regulador figuraba la declaración de política correspondiente. También puede suponer la regulación de aspectos de especial interés que quizá sean más relevantes para algunas organizaciones, como la orientación sobre prácticas seguras para el desarrollo de sitios web, bases de datos o aplicaciones internas. Así pues, la variedad de políticas y las diferencias observadas en la configuración de los marcos reguladores pueden explicarse, al menos en parte, por la adaptación de estos al contexto de la organización, y no ser indicio de la ausencia de un enfoque sistemático con respecto a la regulación. Además, en el ámbito de la ciberseguridad, que evoluciona muy rápidamente, es aún más importante que las orientaciones normativas sean adaptables y pertinentes, lo que algunas organizaciones han tratado de conseguir revisando periódicamente dichas orientaciones. Al respecto, puede considerarse que es una buena práctica indicar en esos documentos de orientación y políticas plazos dentro de los cuales deban ser revisados y, en caso necesario, modificados, así como designar a los responsables de la puesta en marcha de ese proceso.

77. **La existencia de orientaciones es importante, independientemente del alcance, el grado de elaboración o el entorno de la organización.** Dada la gran variedad de asuntos relacionados con la ciberseguridad que pueden ser objeto de regulación, es difícil cartografiar, y mucho menos prescribir con exactitud, los tipos de políticas o procedimientos que permitirían apuntalar mejor el marco regulador de la ciberseguridad. Basta con decir que la existencia de una orientación, aunque sea básica, en este ámbito, a menudo muy técnico y poliédrico, es importante para asegurar la coherencia y la regularidad en la aplicación de medidas de seguridad, independientemente del tamaño de la organización o de los recursos de que disponga.

Integración de la ciberseguridad

78. **Integración.** Detenerse únicamente en las políticas específicas de TIC y ciberseguridad a la hora de diseñar un marco regulador orientado a aumentar la ciberresiliencia de las organizaciones demostraría escasa perspectiva. El mantenimiento de las ciberdefensas de una organización es una responsabilidad que comparten muchos departamentos, y su integración generalizada puede contribuir en gran medida a que, de manera natural, sin imposiciones, se adopte un enfoque que abarque a toda la organización (párrs. 92 a 95). Varias organizaciones muestran signos de haber comenzado a integrar consideraciones relativas a la ciberseguridad en sus diferentes políticas. No obstante, evaluar el grado de integración de la ciberseguridad en los marcos reguladores generales de las organizaciones participantes requeriría un análisis de mucho mayor alcance y un estudio más profundo de lo que permite el presente examen. Los Inspectores ofrecen algunas sugerencias que cabría tener en cuenta y que se enumeran en el recuadro 4.

Recuadro 4
Sugerencias para integrar la ciberseguridad en los marcos reguladores de las organizaciones

- Se pueden incorporar elementos relevantes para la ciberseguridad directamente en las políticas, procesos y prácticas que guían el trabajo de departamentos como los de recursos humanos, compras, comunicaciones o servicios jurídicos. Dos ejemplos serían la inclusión en el manual de adquisiciones de requisitos específicos de investigación previa a la contratación de proveedores de servicios externos, y la especificación de los pasos que se deben seguir en la gestión de los riesgos cibernéticos a lo largo del ciclo de vida de un proyecto en el modelo de documento de proyecto o en los documentos de orientación programática utilizados por las dependencias institucionales en su trabajo cotidiano.
- Las funciones y responsabilidades de los departamentos o las funciones que no están directamente relacionadas con las TIC o la ciberseguridad se pueden asignar y reflejar de manera expresa en los principales instrumentos reguladores vigentes. Por ejemplo, en la documentación sobre la política institucional de seguridad de la tecnología de la información del PMA se detallan las funciones y responsabilidades de diferentes categorías de usuarios y partes interesadas, como los propietarios, custodios y usuarios de la información, los supervisores y el personal en general. La OMPI ofrece otro ejemplo.
- Pueden establecerse vías a través de las cuales se solicite a todas las partes interesadas, no solo al personal de TIC y ciberseguridad, que contribuyan regularmente a la formulación de esos instrumentos, así como a su implementación (por ejemplo, incluyendo en los órganos de gobernanza interna que corresponda a representantes de las partes interesadas o previendo un proceso de autorización cuando las políticas requieran consultas con esas partes interesadas antes de la aprobación del texto final).

Fuente: Elaborado por la DCI.

Cumplimiento y rendición de cuentas

79. **La accesibilidad como requisito previo al cumplimiento.** El marco regulador mejor articulado será tanto más eficaz cuanto mayor sea el grado de cumplimiento de las partes interesadas. El cumplimiento puede verse influido por varios factores, entre ellos la accesibilidad de los materiales que establezcan en términos claros lo que se exige a cada parte interesada y miembro del personal y por qué. Este último aspecto fue subrayado por un oficial principal de seguridad de la información entrevistado por los Inspectores, quien señaló que el problema no era tanto la falta de orientaciones por escrito como el hecho de que muchos usuarios no supieran por qué existían esas orientaciones, qué protegían y de qué manera podía afectar a la persona y la organización no conocerlas. La importancia de contar con esa información se explica más detalladamente en otro apartado del presente informe (párrs. 97 a 103) y tiene que ver, entre otras cosas, con la necesidad de utilizar un lenguaje y unos mensajes sencillos, no técnicos y atractivos, que se centren en hacer palpables para el usuario las consecuencias de un comportamiento cibernético de riesgo. En la Secretaría de las Naciones Unidas, a través de un enlace directo desde la página principal de la intranet de la Oficina de Tecnología de la Información y las Comunicaciones, se halló un ejemplo de repositorio bien estructurado y completo que contenía material de orientación sobre ciberseguridad, con vídeos explicados en lenguaje sencillo, carteles, artículos breves sobre procedimientos, preguntas frecuentes y un conjunto completo de reglamentos y políticas aplicables, clasificados por temas y complementados con notas explicativas.

80. **La respuesta actual al incumplimiento de las disposiciones de ciberseguridad puede ser inadecuada.** Un factor importante que tiene muchas probabilidades de influir en el grado de cumplimiento es la posibilidad de aplicar medidas ejecutivas. Lo ideal es que, además, se reforzasen con el conocimiento y la expectativa de que toda falta de cumplimiento será sancionada. Pocas políticas examinadas por los Inspectores contenían menciones específicas a sanciones por infracciones de ciberseguridad. Incluso en los casos en que sí se

contemplan en las políticas pertinentes, la información recopilada en relación con su implementación en la práctica sugiere que rara vez se aplican y, como consecuencia de ello, los empleados que incurren en conductas de riesgo no suelen rendir cuentas. En la mayoría de las organizaciones participantes, en la política sobre el uso aceptable de recursos de TIC pueden figurar detalles sobre sanciones por faltas en relación con las TIC, lo que generalmente incluye las infracciones de ciberseguridad. Por lo general, esas infracciones están sujetas al mismo tipo de medidas disciplinarias que las que se aplican a la contravención de cualquier otra norma o reglamento del personal. No obstante, se sabe que los procesos estándar, incluso cuando se invocan y llevan a cabo con éxito, son lentos, engorrosos y requieren muchos recursos. Además, normalmente solo se ponen en marcha ante faltas de conducta muy graves en relación con las TIC.

81. **Es necesario considerar un sistema de sanciones más matizado.** En el caso de las infracciones de ciberseguridad, que a menudo se deben simplemente a ignorancia o descuido, **los Inspectores opinan que unas sanciones más fáciles de aplicar, menos formales e invasivas, pueden constituir un enfoque más prometedor.** Con sanciones así se trataría el problema de una manera más directa e inmediata, y acorde con la gravedad de la infracción. No obstante, es necesario alcanzar un equilibrio para que las consecuencias de los comportamientos no conformes sigan siendo debidamente percibidas por quienes incurren en ellos, con el fin de fomentar una mayor ciberhigiene y una conducta más responsable. El reconocimiento implícito de este hecho puede detectarse en la práctica de algunas organizaciones, que en las políticas de ciberseguridad pertinentes distinguen entre faltas menores e infracciones graves. Sin embargo, resultaba menos evidente si habían logrado traducir esa distinción en sanciones adaptadas para responder a las infracciones menores sin perder eficacia. Por ejemplo, en algunas políticas se prevé informar a los superiores jerárquicos o al jefe del departamento de TIC, lo que puede representar la única presión "blanda" que se puede ejercer para procurar el cumplimiento, pero no se sugiere ninguna consecuencia más que la posible vergüenza para el infractor. Un contraejemplo digno de mención, por su especificidad y la repercusión directa que tiene en el usuario, sin que esta sea excesivamente punitiva, es el del OIEA, que prevé en su política una sanción explícita y no disciplinaria en forma de revocación del derecho de acceso a los sistemas de información a las personas que incumplan la normativa. Además, cabe destacar que en la política se reconoce la necesidad de actuar con proporcionalidad a la hora de exigir el conocimiento de las normas antes de poder sancionar a alguien por una infracción y se busca un equilibrio entre la protección eficaz de los activos de la organización y un control que no se traduzca en una vigilancia estricta del personal. En la práctica, la revocación se aplica de forma temporal y tras repetidas advertencias. Los Inspectores desean subrayar que no se puede aplicar ningún mecanismo de sanción serio sin el apoyo explícito del jefe ejecutivo, un requisito que contribuye al éxito del ejemplo citado. **En opinión de los Inspectores, los jefes ejecutivos también deberían estudiar la posibilidad de ofrecer incentivos para que se notificaran los incidentes y de animar a los usuarios a que asuman su responsabilidad por prácticas poco seguras o arriesgadas.** Para ello, será importante encontrar formas de conciliar el objetivo de disuadir mediante sanciones más matizadas con el de incentivar la notificación de incidentes sin temor a las repercusiones.

E. Aprovechamiento de las aportaciones de los mecanismos de supervisión

82. **Auditoría y supervisión en todos los ámbitos interesados en la ciberseguridad.** Los Inspectores examinaron la forma en que los órganos de supervisión habían abordado las consideraciones relativas a la ciberseguridad en el contexto de sus respectivas esferas de interés, ya fuera en el terreno de la auditoría interna (destinada principalmente a evaluar el cumplimiento de las políticas y los procedimientos), de las auditorías externas (que se ocupan principalmente de la auditoría financiera y del cumplimiento, y en ocasiones de la del rendimiento en las esferas administrativas y de gestión) o en el ámbito de los comités de auditoría y supervisión (que asesoran principalmente sobre cuestiones de organización más generales relativas a la atención y adopción de medidas prioritarias por parte de la alta dirección, así como de los órganos legislativos y rectores). Los Inspectores se congratulan de

que, en cada uno de estos ámbitos, la ciberseguridad haya figurado como tema de interés en los últimos cinco años, y en algunas organizaciones incluso desde hace más tiempo.

Órganos de supervisión que se ocupan de la ciberseguridad

83. **Las auditorías internas y externas se centran principalmente en las TIC, e incluyen en cierta medida la ciberseguridad.** Las cuestiones relacionadas con las TIC suelen estar bien integradas en la planificación de las auditorías internas basada en los riesgos. No obstante, durante su investigación la DCI constató que en los últimos cinco años solo un número limitado de tareas de auditoría se centraban específicamente en la ciberseguridad. En cuanto a la capacidad para llevar a cabo este tipo de tareas, pocas son las organizaciones que cuentan con personal experto en auditoría de TIC, y la mayoría recurren a la contratación externa de especialistas. Este enfoque parece ser en general satisfactorio. Desde hace años, las TIC también han centrado la atención de los auditores externos de muchas organizaciones participantes, que han abordado temas como la continuidad de las operaciones, la evaluación y la gestión de riesgos, las políticas de TIC y la gestión de activos de TIC. Globalmente, los directivos consultados por los Inspectores mostraron en sus respuestas que las recomendaciones resultantes eran aceptadas. Asimismo, indicaron las medidas adoptadas para su aplicación.

84. **Los comités de auditoría y supervisión no dejan de prestar atención a la ciberseguridad.** En 2016, los representantes de los comités de supervisión de 19 entidades del sistema de las Naciones Unidas "señalaron, entre otras cosas, los riesgos asociados a la seguridad cibernética en un entorno digital como una esfera de interés, y convinieron en cuestionar la comprensión y preparación por parte de la administración"[18]. De hecho, el análisis de los informes de estos comités muestra que la atención se ha mantenido centrada en el fortalecimiento de los aspectos de gobernanza y gestión de riesgos de la ciberseguridad, a pesar de que en ningún caso se incluyeran referencias específicas a la ciberseguridad en el correspondiente mandato, y solo en cuatro se incluían referencias a las TIC. Los comités abordaron estas cuestiones principalmente en el marco de sus mandatos sobre la gestión de los riesgos institucionales o, en algún caso, en el seguimiento del estado de implementación de recomendaciones de auditorías internas o externas relacionadas con las TIC. En el presente examen se muestra que no en todos los comités de auditoría y supervisión había miembros con conocimientos especializados (aparentemente, solo era así en cuatro comités), y en la mayoría de los casos se recurría a asesoramiento externo cuando era necesario, como suele ocurrir en las auditorías internas. Es encomiable que estos comités se dediquen proactivamente a trabajar en este tema, no solo porque al hacerlo pueden apoyar a la administración en la búsqueda de un enfoque en relación con la ciberseguridad basado en los riesgos, sino también como medio de informar a los órganos legislativos y rectores acerca los riesgos de ciberseguridad relevantes, lo que les permite contribuir a la mitigación de los riesgos para la organización.

Valor de las recomendaciones de los órganos de supervisión para mejorar la posición de ciberseguridad de las organizaciones

85. **Recomendaciones de los órganos de supervisión que impulsan cambios estructurales positivos.** Las organizaciones participantes informaron de que los cambios estructurales de gran calado en su enfoque con respecto a la ciberseguridad tenían su origen en observaciones formuladas por órganos de supervisión, lo que pone de manifiesto el valor agregado de esos mecanismos. Durante las entrevistas, los funcionarios responsables de las áreas de TIC y ciberseguridad valoraron en general los informes de supervisión como impulsores del cambio, al concienciar a la alta dirección de la necesidad de prestar mayor atención a la solidez de la posición de ciberseguridad. De hecho, los Inspectores encontraron ejemplos en los que las recomendaciones surgidas de una auditoría interna contribuyeron directamente a aumentar la ciberseguridad en la organización en cuestión, como fue el caso de la OMPI. Otros ejemplos los encontramos en la OACI y en el UNFPA, donde una recomendación de los auditores condujo a la elaboración de una hoja de ruta plurianual; en la UNESCO, donde se creó un puesto de oficial principal de seguridad de la información, o

[18] Véase A/72/295, párrs. 40 a 43.

en la Secretaría de las Naciones Unidas, donde el grado de cumplimiento de la formación en seguridad de la información aumentó considerablemente. También fueron auditores externos quienes formularon recomendaciones sobre asuntos relacionados con la ciberseguridad para 16 organizaciones participantes en los últimos cinco años, especialmente en relación con el cumplimiento de las obligaciones de formación en seguridad de la información, la recuperación de datos, el control de acceso de los usuarios y los recursos que deben dedicarse a la ciberseguridad. La utilidad de las recomendaciones procedentes de las auditorías parece ponerse más de manifiesto cuando se va más allá de un enfoque orientado al cumplimiento de los aspectos operacionales y técnicos y se proponen mejoras estratégicas, lo que supone un reconocimiento de que el simple cumplimiento de los marcos reguladores no es equiparable a la protección. Al mismo tiempo, muchas organizaciones han expresado su preocupación por el hecho de que, en ocasiones, en esas recomendaciones no se han tenido suficientemente en cuenta las limitaciones de recursos y las circunstancias operacionales, que en algunos casos han limitado las posibilidades para que sean aplicadas.

86. **Conocimientos en ciberseguridad para conformar sistemáticamente la función de supervisión.** Para que los órganos de supervisión aporten el máximo valor desde el punto de vista de la ciberseguridad, es importante que tengan acceso a toda la información pertinente relativa a los riesgos, capacidades y limitaciones de una organización, y que comprendan bien esa información. A fin de hacerlo con la mayor eficacia posible, conviene asegurarse de que los conocimientos y la experiencia de los expertos en ciberseguridad de una organización puedan informar y alimentar la labor de supervisión. Al respecto existen varias opciones, algunas de las cuales ya han arraigado en la práctica o incluso en los marcos reguladores de las organizaciones participantes, ya sea por separado o de forma combinada, y pueden considerarse buenas prácticas. Entre ellas se encuentran las siguientes: a) para la planificación de la auditoría de riesgos es imperativo consultar al oficial principal de seguridad de la información o a la unidad que corresponda, que participarán plenamente en la determinación de los controles e indicadores pertinentes; b) la información sobre ciberseguridad se transmite a los órganos de supervisión con arreglo a las necesidades de los respectivos mandatos, ya sea a través de la notificación de indicadores de incidentes, de reuniones informativas *ad hoc* o periódicas, o por otros medios; c) cualquier informe de auditoría o recomendación que se refiera a la ciberseguridad se comparte con el oficial principal de seguridad de la información o con la unidad correspondiente para recabar comentarios antes de su finalización, con objeto de aliviar la preocupación de que las recomendaciones no se basen suficientemente en las realidades de la organización y, por tanto, resulten inaplicables.

F. Fomento de una cultura de ciberseguridad desde la dirección

87. **La dirección tiene que animar a que se reconozcan los errores y las vulnerabilidades.** Como ya se ha dicho, la posición de ciberseguridad de una organización también depende en gran medida de la existencia de una cultura interna sólida, que parte de la atención y la prioridad que le da la dirección ejecutiva al asunto, es decir, de las pautas que se marcan desde el nivel jerárquico más alto. No obstante, no se detiene ahí y tiene que llegar a todos los miembros del personal. Para ello, es necesario un compromiso y una implicación continuos de la dirección, que no debe limitarse a simples declaraciones en las que se describa la ciberseguridad como una prioridad institucional. Un factor clave sería fomentar una cultura interna en la que el reconocimiento de que se producen incidentes no se perciba como un fracaso, sino como un punto de partida para abordar un problema común y para proteger mejor la organización y sus activos, demostrando compromiso y rindiendo cuentas de manera conjunta y a título individual por errores y puntos débiles. A este respecto, se puede aprender algo de la cultura de las fuerzas del orden en el ámbito de la seguridad física, donde se da por sentado que se producirán incidentes y se espera que se notifiquen y traten como algo natural, sin juzgarlos. **Los Inspectores consideran que es responsabilidad de los jefes ejecutivos inculcar esa cultura en todas las funciones y en todos los lugares en que esté presente la organización, ya que los sistemas de información están interconectados y son interdependientes y un ataque o una intrusión en cualquier parte podría suponer un riesgo global.**

88. **Sensibilización y rendición de cuentas de la dirección ejecutiva como punto de partida.** El primer paso para inculcar una nueva mentalidad y cultura consiste en que el propio personal directivo sea consciente de los riesgos asociados a la ciberseguridad y se interese más por el tema para saber lo que implican la falta de acción y una mala ciberhigiene. Con esos objetivos en mente, se puede pedir que los funcionarios pertinentes de las organizaciones —como los expertos en ciberseguridad, los oficiales de gestión de riesgos y los representantes de los órganos de supervisión— organicen sesiones informativas periódicas, y que se emprendan iniciativas de formación y sensibilización dirigidas específicamente a los directivos superiores. Desde 2020, en la Secretaría de las Naciones Unidas, los pactos celebrados entre el Secretario General y los altos funcionarios contienen disposiciones destinadas a fomentar la sensibilización y la rendición de cuentas en este terreno. La coherencia y efectividad de los pactos y los indicadores de rendimiento que contienen exceden el alcance del presente estudio, pero la inclusión de los objetivos de ciberseguridad en las evaluaciones de rendimiento de los funcionarios superiores es un paso en la buena dirección para mejorar la rendición de cuentas y marcar la pauta desde el nivel jerárquico más alto. Además, deben promoverse iniciativas como la presentación realizada en el contexto del Comité de Alto Nivel sobre Gestión para alertar a los altos directivos de los efectos persistentes que tienen en las operaciones los riesgos relacionados con la ciberseguridad, no solo por los posibles trastornos que pueden causar en los sistemas administrativos, las redes y las infraestructuras, sino también porque pueden poner en peligro la ejecución de los mandatos sustantivos, incluso en el seno de cada organización participante[19].

89. **El dinero no basta para crear una cultura de ciberseguridad.** Hay muchas formas en las que la dirección ejecutiva puede incentivar acciones e influir de manera concreta en las actitudes a lo largo de la cadena de mando. Por un lado, la importancia que se da a la ciberseguridad puede expresarse mediante una asignación adecuada de recursos. Ahora bien, el dinero por sí solo no puede resolver el problema de la preparación en materia de ciberseguridad, ni comprar una cultura de ciberseguridad. En particular, el apoyo financiero no exime a la dirección ejecutiva de su responsabilidad de asumir un liderazgo comprometido con la ciberseguridad, como se insiste en un reciente informe del conocido centro de estudios sobre ciberseguridad Gartner[20]. De hecho, las muestras de apoyo que se circunscriben al ámbito financiero pueden trasladar la responsabilidad de la gestión ejecutiva al nivel jerárquico inmediatamente inferior, donde las decisiones sobre el gasto quizá no vayan acompañadas de una visión estratégica global. La asignación de recursos y las inversiones correspondientes han de decidirse en un contexto institucional y no desde un punto de vista puramente tecnológico o de gestión de riesgos, y la dirección ejecutiva es la más indicada para tomar una decisión informada sopesando debidamente todos los factores (párrs. 108 y 109).

90. **Medios no monetarios de mostrar apoyo desde el nivel ejecutivo.** Entre las buenas prácticas de las organizaciones participantes en lo que respecta al apoyo no monetario por parte de la alta dirección cabe citar las siguientes acciones llevadas a cabo por los jefes ejecutivos: participar visiblemente en los programas de sensibilización, por ejemplo grabando en vídeo declaraciones de apoyo; dirigirse al personal para tratar acerca de asuntos de ciberseguridad en reuniones generales de la organización; compartir con el personal experiencias personales relacionadas con ataques a la ciberseguridad; presentar modelos de comportamientos recomendados; apoyar que se lleven a cabo con frecuencia campañas periódicas de simulación de *phishing* para todo el personal, incluidos los altos directivos; asegurarse de que la responsabilidad se transmita en cascada presionando para que los altos directivos participen directamente en la formación y responsabilicen a sus equipos del cumplimiento de las políticas y la adopción de conductas adecuadas, y apoyar la aplicación de sanciones proporcionadas, especialmente para los "reincidentes" que sigan infringiendo las normas y procedimientos de ciberseguridad. Como ya se ha dicho, reconocer que se producen errores y aprender de ellos, así como afrontar sus consecuencias conjuntamente, como organización, es el punto de partida.

[19] Véase CEB/2017/HLCM/ICT/9.

[20] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, febrero de 2020.

91. **Un cambio de mentalidad requiere tiempo, mensajes coherentes y apoyo de alto nivel.** Para que calen hondo en las actitudes de todo el personal y poder formar así una cultura de ciberseguridad institucional, estas medidas tendrán que repetirse y se tardará un tiempo en ver resultados. La experiencia demuestra que las posibilidades de éxito aumentan y se suceden con mayor frecuencia cuando desde los niveles superiores de la organización se transmite un mensaje coherente con el que se señala que la ciberseguridad es importante y no puede depender de esfuerzos aislados. Como se dijo en el octavo simposio del Grupo de Interés Especial sobre la Seguridad de la Información en 2019, "cambiar el comportamiento humano es difícil y requiere una exposición repetida y consistente a mensajes con nueva información y un reaprendizaje periódico, así como la comprensión de los riesgos latentes que presenta la tecnología y las consecuencias de un mal comportamiento al usar la informática"[21].

G. Aplicación de un enfoque que abarque a toda la organización

92. **El papel de los departamentos administrativos.** De acuerdo con la convicción, cada vez más extendida, de que la responsabilidad sobre la ciberseguridad no puede recaer únicamente en los departamentos de TIC, la mayoría de las organizaciones participantes han reconocido, de un modo u otro, que tanto los departamentos administrativos como los sustantivos tienen un importante papel que desempeñar. En la mayoría de las organizaciones, esa convicción resultaba más evidente en las respuestas a los cuestionarios de la DCI referentes a los departamentos administrativos. De hecho, independientemente de si se hace constar o no en los respectivos marcos reguladores, existe una serie de departamentos administrativos que contribuyen habitualmente a la protección general de las organizaciones en lo tocante a la ciberseguridad. Entre estos figuran los siguientes: los de recursos humanos que ofrecen programas de formación en ciberseguridad; los de servicios de adquisiciones que gestionan las relaciones con los proveedores de servicios externos, lo que comprende un examen previo en materia de ciberseguridad; los de servicios jurídicos que proporcionan asesoramiento sobre cuestiones normativas, contractuales o de cumplimiento, y los departamentos de comunicación que gestionan aspectos relativos a las relaciones públicas con partes interesadas externas. Más allá de sus contribuciones específicas por las funciones que desempeñan, se espera que la mayoría de estos departamentos estén naturalmente predispuestos a incorporar consideraciones relativas a la ciberseguridad en sus actividades cotidianas, dado que su actividad principal incluye el tratamiento de información confidencial, que incluye datos personales y financieros. No resulta obvio, a partir de la documentación que ha examinado la DCI, si esto ocurre en suficiente medida en la práctica y si se puede considerar que refleja que esos departamentos comprenden efectivamente su papel privilegiado como custodios de información confidencial. Quizá este aspecto merezca mayor atención por parte de los responsables de esos departamentos y de los auditores internos y, en su caso, podría incorporarse a las evaluaciones de ciberseguridad que realicen proveedores externos.

93. **El papel de los departamentos sustantivos.** En contraste con lo señalado acerca de los departamentos administrativos, la información recopilada durante la preparación del presente estudio sugiere que, salvo las organizaciones participantes cuyos mandatos exigen que en el desempeño de su labor mantengan una estricta confidencialidad de los datos, los gestores de los departamentos sustantivos suelen considerar la ciberseguridad como una carga administrativa y una limitación para las operaciones. Parece ser que las oficinas de programas no eran lo suficientemente receptivas a la necesidad de incluir los requisitos de ciberseguridad y resiliencia en el diseño y la ejecución de sus proyectos y actividades. Un oficial principal de seguridad de la información señaló en una entrevista que "las políticas y procedimientos de ciberseguridad se consideran a menudo un impedimento para obtener resultados con rapidez, en lugar de escudos protectores para la reputación y los activos de las organizaciones, así como para la eficiencia de sus operaciones". Con ese telón de fondo, es especialmente importante que los jefes ejecutivos contrarresten activamente la percepción de

[21] CEB/2019/HLCM/DTN/02.

que las medidas destinadas a reforzar la ciberseguridad afectan a la agilidad de las operaciones o dificultan la consecución de los objetivos encomendados.

94. **La integración y la asunción de las funciones y responsabilidades como clave para la consecución de un enfoque que abarque a toda la organización.** Como ya se ha dicho (párr. 78), la integración de las consideraciones acerca de la ciberseguridad en las políticas por las que se rige la labor de los respectivos departamentos y sus prácticas sería de por sí un reconocimiento de que cada función de una organización tiene que contribuir a la consecución de un enfoque que abarque a toda la organización. A la luz de la reciente tendencia a la descentralización y la delegación de autoridad en los mandos intermedios observada en muchas organizaciones, la integración contribuiría también a una asunción de responsabilidad y a una rendición de cuentas más directas en toda la organización, al definir las responsabilidades correspondientes, de modo que se facilitaría la consulta por cada parte interesada en la función respectiva. Hacer más explícitas las dimensiones relativas a la ciberseguridad de las funciones programáticas y administrativas mediante la integración puede contribuir a que haya menos malentendidos y a que no dejen de asumirse responsabilidades. Por ejemplo, los Inspectores observaron cierta tensión entre expertos en ciberseguridad y representantes de otras dependencias orgánicas como consecuencia de sus respectivas percepciones de las funciones propias para la consolidación de una posición de ciberseguridad. **En este contexto, los Inspectores subrayan que los departamentos sustantivos, en particular, tienen que asumir una mayor responsabilidad en la dimensión de su labor relativa a la ciberseguridad.** No obstante, la participación de las dependencias institucionales no debe implicar que se les transfieran responsabilidades exclusivamente en calidad de propietarias del riesgo. Los expertos en ciberseguridad tampoco pueden ser los únicos responsables de proteger los activos de la organización: las dependencias institucionales deben compartir una parte significativa de esa carga. Será importante alcanzar un equilibrio adecuado, y la integración de las consideraciones relativas a la ciberseguridad en todos los ámbitos de la organización puede sentar las bases para establecer a este respecto expectativas mutuas ajustadas entre los distintos departamentos y sus respectivas funciones.

95. **La formación basada en funciones debe seguir ampliándose.** Una práctica alentadora que se observó en varias organizaciones participantes fue la disponibilidad de oportunidades de formación en ciberseguridad basadas en funciones y medidas de sensibilización, que deberían ampliarse para dotar óptimamente a todas las partes interesadas a fin de que puedan realizar las aportaciones a la ciberresiliencia que de ellas se espera. Para el conjunto del sistema, la Red de Tecnología de la Información y las Comunicaciones ya ha animado a dirigirse a grupos de usuarios específicos atendiendo a sus responsabilidades funcionales. Por ejemplo, oficiales de planificación de recursos institucionales, especialistas en finanzas y contabilidad, oficiales de adquisiciones y directores ejecutivos. Algunas organizaciones también han preparado sesiones a medida para el personal que tiene encomendadas misiones delicadas o que se encuentra sobre el terreno y se enfrenta a determinados riesgos específicos asociados a la ubicación o la infraestructura. Entre estos destinatarios especiales, quizá merezca la pena dar prioridad a los directores ejecutivos y superiores, por un lado, y a los gestores de programas, por otro, ya que es probable que su propia comprensión y actitud hacia la ciberseguridad se transmita en cascada en el seno de sus respectivas organizaciones o dependencias y tenga una considerable influencia en el surgimiento —o no— de una cultura de ciberseguridad.

H. Establecimiento de una primera línea de defensa basada en el personal

96. **El “factor humano”: amenaza, defensa y pilar de la cultura de la ciberseguridad y la resiliencia.** La mayoría de las organizaciones del sistema de las Naciones Unidas han aplicado importantes medidas tecnológicas y operacionales destinadas a prevenir y mitigar el riesgo de ciberataques (párr. 38). No obstante, muchos expertos en ciberseguridad coinciden en que persiste el reto de sensibilizar a cada miembro del personal sobre su papel en la protección de la información y los activos digitales de la organización, así como sobre la importancia de adherirse a las políticas, procedimientos y mejores prácticas en materia de

ciberseguridad. En muchos sentidos, el "factor humano" ha cobrado importancia en el panorama global de las amenazas a la ciberseguridad, como se refleja en la creciente preocupación de las organizaciones participantes por el hecho de que cada vez más los usuarios finales individuales sean objeto de ataques basados en técnicas de ingeniería social (párrs. 26 y 27). También ha demostrado ser especialmente difícil de gestionar como fuente de riesgo. Además de ser la primera línea de defensa y, al mismo tiempo, el eslabón más débil de la red de seguridad digital de una organización, cada uno de los miembros del personal es un importante pilar de la cultura de ciberseguridad y de la resiliencia de la organización. Las consecuencias adversas de las malas prácticas cibernéticas son múltiples y a menudo se manifiestan en forma de amenazas internas de consideración. Pueden ser causadas por diversos factores: errores cometidos por usuarios poco atentos o no comprometidos; falta de sensibilización o de precaución (que con frecuencia se aprovecha en los ataques de *phishing*); malas prácticas con respecto a la protección de datos, como el empleo de contraseñas poco seguras o el uso compartido de credenciales de acceso entre varios usuarios; el uso de *software* no autorizado o desfasado; el desarrollo de aplicaciones fuera de los entornos de TIC gestionados por la organización, y omisión de actualizaciones o mantenimiento negligente de sistemas. Esos comportamientos representan probablemente las amenazas más habituales que afrontan a diario las organizaciones. Por lo tanto, resulta evidente que es imprescindible facultar a los usuarios para que desempeñen un papel activo en el aumento de la ciberresiliencia de las organizaciones.

97. **La alfabetización digital es el punto de partida innegociable.** Para que cada usuario entienda cómo su manera de abordar la ciberseguridad afecta a la organización, es ineludible partir de una alfabetización digital básica de todos los miembros del personal. Ser capaz de operar en el entorno digital ya no es opcional para ninguna persona que esté asociada de algún modo a las Naciones Unidas y a su labor en el siglo XXI. Hay que dar por hecho que todos los usuarios de la infraestructura digital de las organizaciones, ya sean empleados, personal afiliado, expertos en misión, delegados de conferencias o cualquier otra persona que se conecte con los recursos cibernéticos internos o los utilice, deben poder utilizar con soltura los distintos equipos electrónicos y aplicaciones estándar. Solo después, una vez cumplido ese requisito fundamental, se puede recordar a los empleados que preservar la confidencialidad, la integridad y la disponibilidad de la información y los activos institucionales es una parte indispensable de la labor y responsabilidad de todos. No obstante, el salto más difícil puede ser la transición del conocimiento de las normas, responsabilidades y herramientas relacionadas con la ciberseguridad y las orientaciones sobre prácticas cibernéticas saludables a un cambio de comportamiento sostenible y una modificación de las actitudes individuales y colectivas.

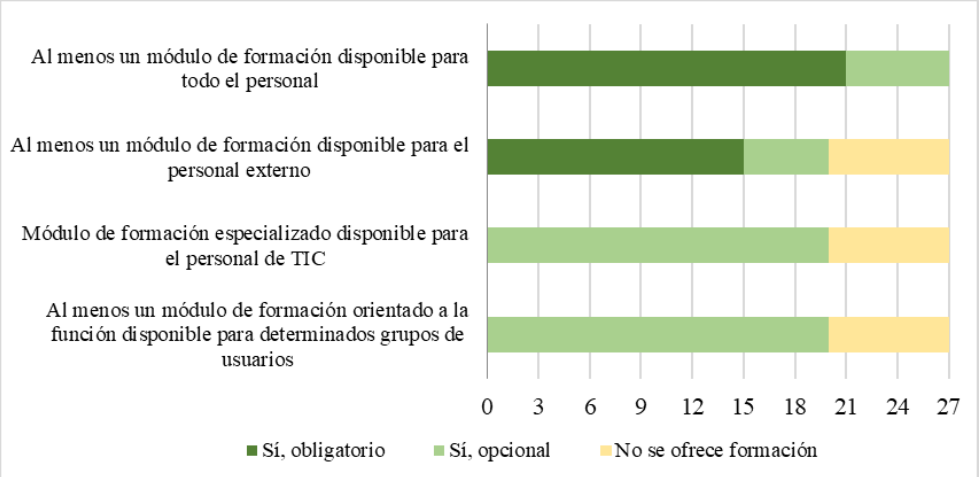
98. **Se reconoce la importancia de la formación.** Una de las vías para inspirar un cambio de mentalidad hacia el reconocimiento de los riesgos cibernéticos y el desarrollo de una actitud sana con respecto a la ciberseguridad es a través de programas de formación y sensibilización sólidos. Esta propuesta se ha destacado en la literatura especializada y en los informes de los comités de auditoría y supervisión dirigidos a la dirección ejecutiva de varias organizaciones del sistema de las Naciones Unidas. En cierta medida, se da una paradoja: a menudo existen mecanismos de protección amplios y estratificados de carácter técnico para la infraestructura y los sistemas, pero la capacidad de todos los miembros del personal para demostrar un conocimiento profesional de su uso y capacidades parece ir rezagada, al menos en algunas organizaciones, según los funcionarios entrevistados. Cuanto más sólido es el sistema, más se desplaza el riesgo hacia los usuarios, y entre estos, hacia los que observan una menor ciberhigiene. Según el Comité Asesor de Auditoría Independiente de la Secretaría de las Naciones Unidas, "la falta de concienciación podría poner en peligro los sistemas de tecnología de la información y las comunicaciones, la confidencialidad y la integridad de la información"[22].

[22] A/73/304, párr. 51.

99. **El análisis de las oportunidades de formación para el personal muestra una situación alentadora.** La Red de Tecnología de la Información y las Comunicaciones ha insistido a lo largo de los años en la importancia de la formación en materia de seguridad de la información para la comunidad de las Naciones Unidas, y las organizaciones participantes han procurado reforzar su oferta en este sentido[23]. En el gráfico VII se representa la información recogida en relación con cuatro categorías de destinatarios. Se confirma la existencia de sesiones de formación obligatorias para los miembros del personal en la mayoría de las organizaciones, pero también se muestra que en algunas organizaciones esas sesiones siguen siendo opcionales. El contenido de esta formación suele centrarse en el uso adecuado de las cuentas de correo electrónico para asuntos profesionales y no personales, los riesgos de abrir archivos adjuntos de origen desconocido, la orientación sobre la elección y el tratamiento de las contraseñas, o los comportamientos seguros a la hora de entrar en sitios web externos. En los últimos años, varios comités de auditoría y supervisión han alertado a las organizaciones participantes sobre la necesidad de elevar el grado de cumplimiento de los cursos de formación obligatorios, lo que en principio es un avance positivo. No obstante, los Inspectores desean subrayar que, por sí solo, el cumplimiento de la formación obligatoria no suele ser un buen indicador del grado de sensibilización, ni proporciona suficientes garantías sobre el logro de un cambio real de comportamiento. Un indicador más relevante, aunque probablemente más difícil de seguir y analizar, podría ser la comparación del número de usuarios que muestran comportamientos desaconsejados (por ejemplo, que hacen clic en enlaces o en archivos adjuntos de mensajes de correo electrónico de *phishing*) a lo largo del tiempo, especialmente antes y después de que se hayan realizado campañas de formación o sensibilización. Algunas de las buenas prácticas observadas en relación con la formación obligatoria incluyen la fijación de una fecha límite de realización para el personal que se incorpore a la organización, con el fin de limitar el período en que aumentan los riesgos por desconocimiento o inexperiencia, así como la exigencia de que el personal reciba sesiones de actualización anualmente para prolongar el efecto del aprendizaje.

Gráfico VII

Formación sobre seguridad de la información en 2020, por módulo de formación y número de organizaciones participantes en la Dependencia Común de Inspección



Fuente: Cuestionario de la DCI, 2020.

100. **Es necesario prestar especial atención a otras categorías de personal y a los usuarios ocasionales.** Aproximadamente la mitad de las organizaciones participantes también hicieron obligatoria para otras categorías de personal la formación sobre seguridad de la información, mientras que la otra mitad ofrecía esa formación como módulo opcional o simplemente no la ofrecía. La atención a las categorías distintas del personal interno es realmente crucial. Quienes se encuentran en esas categorías se ven a menudo obligados, por limitaciones de recursos, a utilizar sus dispositivos personales para conectarse a la infraestructura de las organizaciones. Además, es menos probable que los usuarios menos

[23] Véanse, por ejemplo, los documentos CEB/2011/3 y CEB/2018/HLCM/ICT/10.

habituales de los sistemas e infraestructuras institucionales estén familiarizados con su uso correcto y seguro de acuerdo con las políticas y prácticas de la organización. La falta de mecanismos efectivos para asegurar el cumplimiento de las personas que no están empleadas directamente y que, por tanto, quedan fuera del ámbito de la plena jurisdicción disciplinaria de las organizaciones, puede desincentivar y deteriorar aún más el cumplimiento, ya de por sí escaso. Estos retos pueden acentuarse aún más en las organizaciones cuyo personal se compone en gran medida de consultores, contratistas y empleados con contratos de corta duración. **Los Inspectores recuerdan que las iniciativas de formación y sensibilización deben incluir a todo el personal. Las amenazas no discriminan entre tipos de usuarios. Por ello, los Inspectores sugieren que los jefes ejecutivos de las organizaciones que no hayan hecho obligatorios estos módulos tomen las medidas oportunas.**

101. **Desafíos relativos a la formación.** Se comunicó a los Inspectores que existía una serie de desafíos a los que se enfrentan las organizaciones participantes y que pueden afectar a la aplicación de un programa eficaz de formación en ciberseguridad. Varias organizaciones señalaron que las restricciones financieras limitaban su capacidad para proporcionar acceso a oportunidades de formación o desarrollarlas, y algunas se vieron obligadas a seleccionar entre categorías de usuarios para que recibieran formación, lo que resultaba preocupante. Los aspectos financieros se ven acentuados por la rápida evolución de la cuestión, que puede provocar que el contenido del curso quede rápidamente obsoleto y se requieran actualizaciones y ampliaciones, a menudo costosas. Otro desafío es el cansancio de los usuarios, que puede afectar a la eficacia del programa. La elevada rotación del personal y la falta de autoridad sobre determinadas categorías de empleados complican aún más las cosas. Las entidades que trabajan sobre el terreno pueden tener dificultades específicas, al igual que con cualquier otra oportunidad de aprendizaje. No obstante, ese aspecto no se pudo explorar a fondo en el contexto del presente examen. Por último, los responsables de ciberseguridad señalaron la ausencia general de medidas ejecutivas en caso de incumplimiento de los requisitos de formación y correlacionaron la posible ineficacia de muchos programas de formación con la ausencia de sanciones, que hacía que incluso la formación obligatoria fuera en la práctica opcional. **Los Inspectores sugieren que, para lograr un mayor grado de cumplimiento, los jefes ejecutivos consideren la posibilidad de instituir un vínculo formal entre la realización de la formación en materia de seguridad de la información y otros procedimientos de autorización institucionales.** En ese sentido, quizá sea necesario vincular la autorización de seguridad para el despliegue sobre el terreno y la concesión o ampliación de derechos de acceso al sistema de TIC a la acreditación de que se ha seguido la formación, incluidos los cursos de actualización. Ya existe un precedente de este enfoque en relación con la seguridad física antes de los viajes en comisión de servicio, en que la autorización para viajar está supeditada a la realización de una formación básica de seguridad sobre el terreno, sin la cual se denegará.

102. **Iniciativas de sensibilización en todo el sistema de las Naciones Unidas.** En el sistema de las Naciones Unidas existen múltiples iniciativas de sensibilización sobre los riesgos de ciberseguridad y las medidas recomendadas. Un ejemplo es la semana de octubre sobre la seguridad de la información, una iniciativa en la que participan varias organizaciones de todo el mundo y que incluye sesiones informativas e interactivas y juegos. Se han considerado especialmente innovadores y eficaces los programas de la Organización Internacional del Trabajo (OIT) y de la OMPI, y así se ha reconocido en el contexto de varias auditorías externas. Otras ideas interesantes consisten, por ejemplo, en celebrar sesiones de sensibilización sobre los riesgos cibernéticos que afectan a la esfera privada (por ejemplo, los riesgos para los niños o las fotos familiares que se toman para pedir un rescate) con la esperanza de suscitar más interés y que las lecciones aprendidas se extiendan de forma natural a la esfera profesional. Algunas organizaciones realizan para el personal nuevo sesiones informativas presenciales con el oficial principal de seguridad de la información, mientras que otras refuerzan las lecciones aprendidas distribuyendo breves mensajes de vídeo a los empleados que han sido víctima de un ciberataque. Las campañas con ataques de *phishing* simulados constituyen uno de los medios de sensibilización más populares y, al parecer, dan resultados (recuadro 5).

Recuadro 5
Las campañas de *phishing* simulado dan resultados

Se entiende por *phishing* el envío de mensajes de correo electrónico fraudulentos que dicen provenir de una fuente fiable para inducir al destinatario a revelar información confidencial. Los atacantes utilizan después esa información para obtener acceso no autorizado a los sistemas de la organización, con el fin de estafarla para obtener beneficios económicos o por otros motivos que pueden causar perjuicios.

En las campañas de *phishing* simulado se reproducen las estrategias que emplean los *hackers* en la vida real, lo que ayuda a determinar qué usuarios tienen más probabilidades de ser engañados para que hagan clic en enlaces malintencionados o abran archivos adjuntos infectados. Estos simulacros también se utilizan con el fin de poner a prueba las habilidades adquiridas en los cursos de formación. Para que sean más eficaces, deben ir acompañados de servicios orientados al usuario, como puntos de contacto claros y procedimientos sencillos y ampliamente conocidos para avisar en caso de recepción de algún mensaje sospechoso. Por ejemplo, algunas organizaciones participantes han incluido un mecanismo para informar de posibles mensajes de *phishing* pulsando un botón directamente en la aplicación de mensajería electrónica utilizada por los empleados.

Las cifras compartidas con los Inspectores demuestran la utilidad de este tipo de campañas de *phishing* simulado, ya que los oficiales de seguridad de la información observaron en general que, como resultado de varias campañas sucesivas, se reducía el porcentaje de usuarios que abrían mensajes y archivos adjuntos sospechosos. Para contextualizar, la proporción comúnmente aceptable de usuarios internos que no cumplían con las normas era de alrededor del 5 % del personal, según algunos oficiales de ciberseguridad.

Con frecuencia, las campañas de *phishing* simulado se llevan a cabo en el marco de un conjunto de pruebas de penetración más amplio. Estas pruebas, que en inglés también se conocen con la forma abreviada de *"pen testing"*, constan de una serie de ejercicios prácticos dirigidos a la red, los sistemas y los recursos humanos de una organización para detectar vulnerabilidades, medir los niveles de cumplimiento de las políticas y los procedimientos y evaluar la eficacia de las defensas y los procedimientos de recuperación.

103. **La transición de los módulos de formación a un programa coherente de sensibilización.** En lugar de seguir ofreciendo a todos los usuarios módulos individuales sin guiarse por una visión estratégica, **los Inspectores aconsejan a las organizaciones que procuren desarrollar un programa integral de formación y sensibilización con objetivos claros para cada categoría de partes interesadas, de acuerdo con los riesgos que puedan representar para la organización.** Siguiendo este modelo, las organizaciones podrían dejar de centrarse en el porcentaje de finalización como indicador de cumplimiento y, en su lugar, utilizar la formación como una herramienta proactiva para cambiar la cultura interna con respecto a la ciberseguridad. Lo ideal es que el programa se aplique utilizando métodos de ejecución innovadores que combinen múltiples enfoques y mensajes adaptados a cada tipo de usuario. Para potenciar la implicación y facilitar la asimilación del aprendizaje en este ámbito, las organizaciones pueden considerar además la posibilidad de establecer un sistema de apoyo entre pares e identificar a empleados en todos los departamentos que podrían recibir formación para contribuir a implementar el programa y proporcionar asistencia práctica a otros miembros del personal cuándo y dónde sea necesario.

I. Optimización de la asignación de recursos financieros para la ciberseguridad

Estimación del actual nivel de recursos dedicados a la ciberseguridad

104. **El volumen de recursos de ciberseguridad disponibles en el sistema de las Naciones Unidas es, por lo general, menor que el de las entidades externas, aunque resulta difícil de cuantificar.** Es casi un lugar común decir que las organizaciones del

sistema de las Naciones Unidas tienen menos recursos a su disposición para asignarlos a las TIC en general y a la ciberseguridad en particular que otras entidades de tamaño comparable del sector público y del privado. No obstante, es difícil cuantificar la diferencia, tanto en términos absolutos como relativos. Por ejemplo, se estimó que "menos del 1 % del gasto de las Naciones Unidas se destina a las TIC, y menos del 1 % se reserva para la seguridad de la información, en contraste con el promedio anual del 7 % en la industria"[24]. Con objeto de ofrecer una instantánea de la situación basada en datos, la DCI encuestó a sus organizaciones participantes sobre la asignación de recursos a las TIC y a la ciberseguridad. Tal vez no resulte sorprendente que los Inspectores llegaran a la misma conclusión que la que se refleja en las actas de las reuniones del simposio celebrado en 2018 por el Grupo de Interés Especial sobre la Seguridad de la Información, a saber, que las cifras relativas al sistema en conjunto seguían siendo inciertas.

105. **Complejidad y utilidad de la estimación del gasto en ciberseguridad.** Resulta difícil determinar qué recursos hay disponibles para la ciberseguridad debido a varios factores. Los costos de la ciberseguridad (recuadro 6) no suelen ser objeto de seguimiento como una partida presupuestaria o una categoría de gasto independientes. La financiación relacionada con la ciberseguridad puede estar incluida en una o varias partidas presupuestarias (por ejemplo, costos operacionales, de personal o de infraestructura y equipamiento) o áreas temáticas (por ejemplo, dentro o fuera de la dotación para TIC). La dificultad de localizar información sobre los recursos y los niveles de gasto en materia de ciberseguridad en los documentos presupuestarios y los estados financieros se ve agravada por la diversidad de estructuras presupuestarias, que se refleja en la coexistencia de presupuestos ordinarios y contribuciones voluntarias (extrapresupuestarias), algunas de las cuales pueden incluir fondos de inversiones de capital independientes utilizados para proyectos de infraestructura de la organización de gran escala. Varias organizaciones también distinguen los costos de inversión (puntuales) y los operacionales (recurrentes), lo que añade más matices al panorama. En una organización se observó incluso que una gran parte de los recursos de TIC estaban federados en los presupuestos de los programas de las dependencias institucionales que mantenían competencias de TIC. En este contexto, es casi imposible hacer una afirmación fiable acerca del total de recursos disponibles para la ciberseguridad. En cualquier caso, resultaría desproporcionadamente complejo en relación con su utilidad: el nivel de recursos asignados a la ciberseguridad en una organización tiene un valor indicativo limitado respecto al nivel de protección que ofrece.

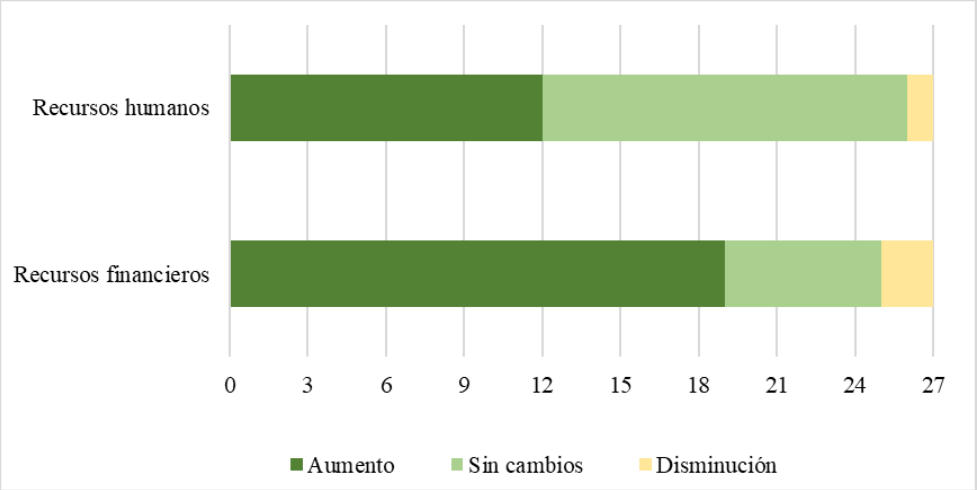
Recuadro 6
Costos de la ciberseguridad

- **Costos directos.** Los costos evidentes (directos) de la ciberseguridad van desde los gastos de personal (empleados y contratistas) y los relacionados con la infraestructura, como la compra de equipos y programas informáticos (costos de inversión y mantenimiento y de licencias), hasta los servicios (por ejemplo, suscripciones a sistemas de información acerca de amenazas y servicios externalizados de proveedores comerciales o del Centro Internacional de Cálculos Electrónicos de las Naciones Unidas (CICE)). La distribución proporcional de estos costos varía y refleja la elección de cada organización en lo que se refiere al equilibrio entre capacidad interna y subcontratación.
- **Costos indirectos.** Además, existen otros costos (indirectos) que hay que tener en cuenta a la hora de ponerle precio a la ciberseguridad. De hecho, se tiende a asociar un considerable impacto financiero a las medidas de control de daños tras un incidente, que incluyen la movilización de capacidades según se requiera para restablecer los servicios afectados, la aplicación de parches a las vulnerabilidades que se hayan descubierto, la pérdida de productividad mientras los sistemas están fuera de servicio, la formación del personal para prevenir intrusiones y responder mejor cuando estas se producen, y el mantenimiento de los recursos especializados existentes (tanto humanos como tecnológicos).

[24] CEB/2018/HLCM/ICT/4.

106. **Tendencia reciente: la financiación ha aumentado, pero sigue habiendo limitaciones de capacidad.** Los Inspectores señalan que la mayoría de las organizaciones participantes indicaron que en los últimos años se habían incrementado las asignaciones de recursos a la ciberseguridad (gráfico VIII). A primera vista, puede parecer una tendencia prometedora. Sin embargo, como se evidencia en el gráfico, el aumento de los recursos financieros no parece haberse traducido automáticamente en un aumento de capacidad en lo que respecta a los recursos humanos. De hecho, la gran mayoría de las organizaciones participantes advirtieron que el nivel actual de recursos disponibles seguía constituyendo un obstáculo para la creación de un marco de ciberseguridad eficaz, y en una de ellas se llegó a afirmar que los costos de seguridad y protección contra las crecientes ciberamenazas se habían triplicado en los dos últimos bienios. En las evaluaciones de las propias organizaciones, se constató que las limitaciones de recursos eran las que más afectaban a la capacidad relativa a los recursos humanos y a la disponibilidad de conocimientos técnicos internos, a la capacidad de realizar inversiones adecuadas en infraestructuras de TIC y a la de sustituir aplicaciones obsoletas. Además, en aquellas organizaciones que operan con serias limitaciones de recursos o con presupuestos congelados, las recientes partidas destinadas a la ciberseguridad pueden obedecer a redistribuciones internas, quizá a expensas de otras inversiones (sobre todo, aunque no exclusivamente, en TIC). Dado que esta práctica puede resultar insostenible a largo plazo, a los Inspectores les preocupa que los recursos disponibles, incluso en los casos en que han crecido, no hayan aumentado al mismo ritmo que la sofisticación tecnológica de los atacantes y la presencia de las TIC en la labor de las organizaciones del sistema de las Naciones Unidas. Como se dijo acertadamente en el contexto del Grupo de Interés Especial sobre la Seguridad de la Información, la creciente dependencia de los servicios cibernéticos no se ha visto compensada por un incremento de la dotación de recursos para las actividades relacionadas con la seguridad de la información[25].

Gráfico VIII
Evolución de los recursos para la ciberseguridad según la información facilitada por las organizaciones participantes en la DCI (2015-2020)



Fuente: Cuestionario de la DCI, 2020.

107. **Fuentes de financiación.** Según la información recopilada, en la mayoría de las organizaciones participantes los recursos para la ciberseguridad proceden principalmente del presupuesto ordinario. En algunas de ellas se recurre a una combinación de recursos ordinarios y extrapresupuestarios, y en muy pocas se utilizan exclusivamente estos últimos. La relativa previsibilidad de los recursos del presupuesto ordinario puede contribuir a la sostenibilidad de las capacidades en materia de ciberseguridad, pero se requiere una planificación estratégica para que los recursos presupuestarios necesarios estén disponibles en el momento en que se necesiten. Al mismo tiempo, los recursos extrapresupuestarios pueden permitir una mayor flexibilidad y ser una opción más atractiva para los donantes que deseen destinar medios específicamente a la ciberseguridad. Algunas organizaciones

[25] *Ibid.*

mantienen un fondo especial, ya sea dedicado a la infraestructura de las TIC (OMS) o reservado para grandes proyectos institucionales (OMPI y OIEA). Como se ha apuntado en el contexto de las hojas de ruta a largo plazo para la mejora del marco de ciberseguridad de las organizaciones, las inversiones en este ámbito suelen tener, por su propia naturaleza, una dimensión plurianual. Así pues, los ciclos presupuestarios actuales quizá resulten demasiado breves para que arraiguen consideraciones estratégicas a largo plazo, pero no lo suficientemente ágiles como para que se puedan destinar rápidamente fondos a cubrir necesidades específicas y a corto plazo que puedan surgir en el ámbito tecnológico, en un panorama de amenazas que evoluciona tan rápidamente como el de la ciberseguridad. Los fondos especiales pueden llenar un vacío en ese aspecto, siempre que lo permitan sus principios de gobernanza y las condiciones acordadas por sus órganos legislativos y rectores.

Hacia la optimización de las inversiones en ciberseguridad

108. **Se necesita un estudio de viabilidad para justificar las solicitudes de recursos a los órganos rectores.** Es evidente que las organizaciones no pueden esperar que prosperen sus solicitudes de asignación de recursos a los órganos rectores si no se justifica debidamente la prioridad de las inversiones en ciberseguridad sobre otros gastos de la organización. **Como punto de partida, los Inspectores recomiendan basar las solicitudes de recursos en una evaluación exhaustiva de los riesgos y en un estudio de viabilidad en que se detallen los costos, los beneficios, los riesgos y los ahorros previstos y se señalen las posibles consecuencias financieras de no realizar la inversión.** Este enfoque es más eficaz cuando va acompañado de una propuesta de plan y de calendario de implementación, por ejemplo en forma de hoja de ruta, como se propone en otro apartado del presente informe, y cuando se informa periódicamente de los progresos realizados. Los Inspectores observaron que, cuando la dirección ejecutiva presentaba un estudio de viabilidad convincente en el que se exponían un objetivo y unos parámetros de mejora claros y se demostraba la importancia de la inversión, los órganos rectores solían estar más dispuestos a apoyar el esfuerzo asignando recursos específicos. Así ha sido en los últimos años en la OACI, la OIT, el ACNUR, la OMPI y otras organizaciones, y es una práctica alentadora, ya que es probable que la creciente sofisticación de las amenazas a la ciberseguridad siga requiriendo más recursos, no menos.

109. **El gasto en ciberseguridad puede y debe ser reestructurado.** Huelga decir que un marco de ciberseguridad sólido y bien protegido tiene un precio y, si las organizaciones del sistema de las Naciones Unidas se toman en serio la protección de su información, sistemas y activos digitales, deben dotar de recursos suficientes sus marcos de ciberseguridad. Los intentos de determinar el nivel adecuado de recursos para la ciberseguridad como porcentaje de los presupuestos institucionales de TIC no dieron resultados significativos. No obstante, no hay que sobrevalorar la idea de expresar en términos monetarios la suficiencia de recursos, ya que solo con dinero no se resolverá el problema. Gartner lo expresó sin rodeos: el gasto en ciberseguridad no refleja el nivel de protección[26]. Más importante que cuánto debe gastarse en ciberseguridad es dónde deben asignarse los recursos para que tengan el mayor impacto posible. Las respuestas a los cuestionarios de la DCI dan a entender que existen incoherencias en los enfoques para priorizar el gasto en ciberseguridad, lo que aumenta el riesgo de que unos recursos ya de por sí escasos se utilicen de un modo ineficiente. Para reestructurar las inversiones en ciberseguridad, una opción que es muy persuasiva, aunque resulta algo compleja y debe adaptarse específicamente a cada caso, consiste en seguir una metodología rigurosa, como la Arquitectura de Seguridad Empresarial Aplicada de Sherwood (o una herramienta equivalente), que se basa en la noción de trazabilidad bidireccional. Según este enfoque, la arquitectura de seguridad de la organización se configura de manera que cada requisito de la actividad institucional se verifique mediante al menos un control de seguridad, y que se pueda establecer una correspondencia entre cada control de seguridad y un requisito institucional que se haya declarado en relación con la seguridad[27]. La OMPI ya utiliza esta metodología, que también ha debatido el Grupo de Interés Especial sobre la Seguridad de la Información y que, **en opinión de los Inspectores, merece la pena seguir explorando como**

[26] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, febrero de 2020.

[27] Se puede obtener más información sobre la Arquitectura de Seguridad Empresarial Aplicada de Sherwood en: https://sabsa.org/sabsa-executive-summary.

medio para que las inversiones en ciberseguridad se fundamenten siempre en las necesidades institucionales y estén vinculadas a prácticas de gestión del riesgo sólidas, a fin de evitar tanto el exceso de inversión como la falta de recursos en un terreno clave para la continuidad de las operaciones.

Recuadro 7
Las soluciones de código abierto pueden ofrecer alternativas rentables

El *software* de código abierto ofrece un modelo de desarrollo y distribución de programas informáticos que se ha convertido en parte esencial del sector de las TIC. Algunas herramientas basadas en *software* de código abierto se utilizan ampliamente en el ámbito de la ciberseguridad y cubren aspectos tales como el intercambio de información sobre amenazas, la gestión de identidades y accesos, el análisis de redes, la detección y prevención de intrusiones, la respuesta a incidentes y el análisis forense. Algunos recursos de *software* de código abierto son incluso reconocidos como los más destacados en sus respectivas categorías.

Aunque las respuestas al cuestionario de la DCI sugieren que algunas organizaciones participantes ya están complementando las soluciones que han adquirido comercialmente y las que desarrollan internamente con *software* de código abierto, puede haber margen para que las entidades de las Naciones Unidas recurran más a estas opciones. Pueden ofrecer soluciones adecuadas, especialmente para organizaciones que operan en circunstancias marcadas por la escasez de recursos.

Al igual que con cualquier producto amparado por un derecho de propiedad intelectual, las soluciones de código abierto deben evaluarse por sus propios méritos, pero en general hay ciertas ventajas que suelen verse asociadas a los productos de *software* de código abierto de los que se realiza un buen mantenimiento, como la transparencia, la seguridad, el menor costo en licencias y cuotas, el uso de estándares abiertos y el escaso riesgo de dependencia del proveedor.

Aunque el uso de *software* de código abierto no suele llevar aparejados costos de licencia, eso no significa que sea totalmente gratuito. Su instalación, configuración y mantenimiento, y el dominio técnico que para ello requiere, exigen tiempo y dedicación de personal y, por lo tanto, tiene un costo. El costo total de la propiedad de estas plataformas puede no ser obvio para las organizaciones con recursos técnicos limitados y poca experiencia en este tipo de aplicaciones, aunque esa limitación suele también darse —en diversos grados— con los productos comerciales.

Las organizaciones no deben plantearse modelos que se basen exclusivamente en productos amparados por derechos de propiedad intelectual o en *software* de código abierto. Hay productos basados en un modelo híbrido que pretende combinar lo mejor de ambos mundos, es decir, la libertad y la transparencia del enfoque del código abierto y el apoyo estructurado y la agilidad que ofrecen algunos proveedores. Otra posibilidad sería utilizar tanto herramientas patentadas como *software* de código abierto, aunque para funciones y propósitos diferentes dentro de una organización.

J. Inversión en recursos humanos dedicados y especializados

La función o área de seguridad de la información no está presente en todas las organizaciones participantes

110. **Las responsabilidades asociadas a la ciberseguridad no se limitan a la especialización técnica.** La mayoría de las organizaciones participantes han invertido en la contratación de especialistas para cubrir las diferentes dimensiones de la ciberseguridad, a veces bajo la dirección de un oficial principal de seguridad de la información dedicado. Los principales cometidos de la función asociada son, por un lado, la elaboración de controles para las operaciones y, por otro, la orientación de la gestión estratégica, con el fin de alcanzar los objetivos de la ciberseguridad en relación con la protección reflejados en la definición que se menciona en el presente informe. En ese sentido, el alcance de la función trasciende

la esfera digital y no se limita a proporcionar conocimientos técnicos. Implica diversas tareas, entre las que figuran las siguientes: desarrollar y comunicar un marco regulador institucional (definición de políticas y comunicación); ofrecer asesoramiento sobre cómo la identificación y el tratamiento de los riesgos (gestión de riesgos); colaborar con las dependencias institucionales en la realización de evaluaciones de riesgos y análisis del impacto en la actividad (función de coordinación y análisis); investigar infracciones de consideración (capacidad de investigación y análisis), y recomendar y aplicar las mejoras adecuadas en materia de control (conocimientos técnicos y sobre operaciones)[28]. Según esta descripción de tareas se da por supuesto que la función incluye una dimensión de gestión, tanto dentro como fuera del entorno de las TIC, y requiere una estrecha colaboración con un amplio abanico de partes interesadas, en particular las dependencias de las organizaciones. Por lo tanto, la autoridad delegada en el oficial principal de seguridad de la información (y en los expertos en ciberseguridad en general) es de suma importancia para la comunicación y para impulsar la adopción de medidas en toda la organización.

111. **La capacidad interna varía.** De acuerdo con la investigación llevada a cabo por la DCI, al menos 16 organizaciones participantes han desarrollado su capacidad interna con recursos humanos especializados y dedicados, que van desde un oficial de seguridad de la información, a veces solo a tiempo parcial, hasta una unidad dirigida por un oficial principal de seguridad de la información, generalmente de categoría P4 o P5 (anexo V). En cambio, en 10 organizaciones participantes, las tareas relacionadas con la ciberseguridad las desempeñan principalmente los responsables de TIC junto con sus otras funciones. Con frecuencia se recurre a expertos externos debido a la complejidad técnica del tema, que evoluciona constantemente y requiere un grado considerable de especialización que resulta difícil y costoso mantener disponible y actualizado de forma permanente. Por ello, estos conocimientos se complementan a menudo recurriendo temporalmente a consultores y contratistas, entre otros recursos, o bien a servicios de proveedores comerciales o del CICE. Algunos interlocutores señalaron que la escasez mundial de profesionales experimentados en ciberseguridad era uno de los mayores desafíos a los que se enfrentaban las organizaciones del sistema de las Naciones Unidas a la hora de crear, mantener y gestionar sus programas de ciberseguridad. Para ofrecer una alternativa a las entidades que no están en condiciones de establecer inmediatamente una función dedicada, los Inspectores desean destacar que el CICE ofrece un servicio denominado "gobernanza de la seguridad", también conocido en ocasiones como "oficial jefe de seguridad de la información como servicio", al que actualmente están suscritas 6 organizaciones participantes y al que en el pasado han recurrido otras 4. **Los Inspectores opinan que las organizaciones del sistema de las Naciones Unidas tienen que abordar las futuras necesidades de especialización en materia de ciberseguridad mediante una planificación adecuada de los recursos humanos, en particular porque los conocimientos, las aptitudes y las capacidades para hacer frente a los riesgos y problemas de ciberseguridad son específicos y quizá no resulten fáciles de atraer y retener.**

112. **Merece la pena considerar la posibilidad de invertir en capacidad dedicada.** Si bien es cierto que lo ideal es que en las disposiciones institucionales se tengan en cuenta el tamaño de la organización y sus requisitos específicos, atendiendo a la evaluación de riesgos realizada y el entorno cibernético en el que opera la entidad, la realidad es que otros factores pueden ser más decisivos. En concreto, las disparidades en la configuración interna de las organizaciones participantes observadas por los Inspectores pueden ser más bien un indicio de las limitaciones a las que se enfrenta cada una de ellas que una elección deliberada o estratégica. De hecho, en cuatro organizaciones participantes la función de ciberseguridad se consideraba, como mucho, incipiente, lo que indirectamente podría poner en riesgo todo el sistema. **Los Inspectores creen que contar en cada organización con conocimientos especializados en materia de ciberseguridad dedicados contribuye a reforzar la posición no solo de la organización, sino del sistema en su conjunto, por lo que es una inversión que merece la pena.** Al igual que ocurre con otras funciones asociadas a la actividad principal de las organizaciones, en general siempre que se pueda es preferible crear capacidad interna duradera basada en los recursos humanos para proteger la información y los activos cibernéticos a depender de recursos temporales sucesivos, entre otras cosas por los riesgos

[28] Véase SFIA Foundation, *Marco de competencias para la era de la información (SFIA) 7*, 2018.

adicionales que están asociados a su empleo y la limitada capacidad de las organizaciones para asegurar el cumplimiento de las normas por parte del personal afiliado (párr. 100). Además, **la creación de un puesto fijo de oficial principal de seguridad de la información que se encargue de supervisar y gestionar esos recursos especializados puede aportar el enfoque necesario, así como coherencia en el planteamiento y, en opinión de los Inspectores, contribuiría a reforzar la ciberresiliencia de las organizaciones en cuestión.**

113. **No hay consenso sobre la ubicación de la ciberseguridad en el organigrama.** La ubicación de la ciberseguridad en términos de relaciones jerárquicas es una cuestión que se ha debatido dentro y fuera del sistema de las Naciones Unidas, y para la que no existe una respuesta definitiva ni de aplicación universal. Las normas internacionales no proporcionan una orientación autorizada y dejan margen para que cada organización decida en función de sus necesidades y arquitectura cuál es el estatus más adecuado para la ciberseguridad. En la mayoría de las organizaciones del sistema de las Naciones Unidas esta función corresponde al departamento de TIC, lo que generalmente se refleja en una relación jerárquica directa con su jefe o con un puesto equivalente. Esta disposición estructural predominante puede considerarse una herencia del pasado, pero refleja el hecho de que la ciberseguridad tiende a gravitar de forma natural hacia las TIC, habida cuenta de los conocimientos tecnológicos y la especialización necesarios para gestionar los sistemas de información relacionados y otras infraestructuras de protección. Además, el departamento de TIC suele ser el que concibe y ejecuta la respuesta operacional en caso de ciberataque, y la desvinculación de estas dos esferas puede provocar pérdidas de eficiencia.

114. **Gestión de prioridades divergentes desde el punto de vista organizacional entre las funciones de TIC y ciberseguridad.** No obstante lo anterior, situar al funcionario o equipo encargado de la ciberseguridad bajo la autoridad del jefe del departamento de TIC puede crear tensiones por las diferencias entre los principales objetivos de las respectivas funciones, siendo la gestión de riesgos y la seguridad de la información la principal preocupación del oficial principal de seguridad de la información, frente a la eficacia de las operaciones y los costos, así como la rapidez del servicio, que interesan sobre todo al jefe de TIC. El posible conflicto de intereses resulta evidente, pero no es fácil de resolver. Un enfoque con respecto a la ciberseguridad demasiado orientado a las operaciones (como el que se asocia a los profesionales de las TIC) puede multiplicar el impacto negativo en el servicio en una etapa posterior, cuando los riesgos cibernéticos que antes se habían ignorado empiecen a materializarse. Al mismo tiempo, una excesiva aversión al riesgo (como la que se atribuye a los profesionales de la ciberseguridad) puede afectar indebidamente a la agilidad de las operaciones e impedir la ejecución de los mandatos de otras maneras. Gestionar y resolver las tensiones que surgen por las divergencias entre los distintos objetivos de la organización, y en concreto sus repercusiones en lo que respecta a los recursos, forma parte de las tareas cotidianas de todo directivo, y la dirección ejecutiva es la más indicada para encontrar un equilibrio en ese terreno.

115. **Potenciación de la función de la ciberseguridad.** Independientemente de dónde quede situada la ciberseguridad en el organigrama, **los Inspectores subrayan que es importante salvaguardar la oportunidad de que se puedan expresar sin trabas las consideraciones relativas a la ciberseguridad y que sean escuchadas por los responsables de la toma de decisiones.** La función debe situarse allí donde pueda tener acceso de manera independiente a la dirección ejecutiva y contribuir efectivamente a otros marcos institucionales, como la gestión de los riesgos, la gestión de la información y el conocimiento, la seguridad física y la supervisión, como se defiende a lo largo del presente informe. Este acceso se consigue de forma más eficaz cuando existe un sólido mecanismo interno de gobernanza compartida por múltiples partes interesadas en el que participan todos los departamentos pertinentes. La OMPI y la OACI proporcionaron ejemplos elaborados de estos mecanismos de gobernanza que integran múltiples partes interesadas y niveles.

116. **Formación especializada.** Independientemente de quién se encargue de la ciberseguridad en una organización y de si la función recae en una sola persona o en un equipo o se reparte entre varios recursos dedicados a tiempo parcial, es importante que todo el personal de las TIC que tenga responsabilidades relacionadas con la seguridad pueda tener acceso a formación especializada, con objeto de asegurar la actualización continua de conocimientos y competencias. Según se ha indicado, este tipo de formación para el personal

de TIC, como desarrolladores o administradores de sistemas, ya está disponible en la mayoría de las organizaciones y debería promoverse aún más (gráfico VII). Idealmente, un sólido programa de formación en ciberseguridad y, cuando corresponda, un proceso de certificación para funcionarios de TIC seleccionados deberían ser componentes básicos del plan de trabajo de ese departamento, complementado con un presupuesto garantizado. Si no se destinan recursos a la mejora continua de las competencias, el personal de TIC se ve obligado a mantener sus conocimientos profesionales por iniciativa propia o participando en comunidades profesionales. Este enfoque depende demasiado de actitudes profesionales individuales y tiene pocas probabilidades de ser sostenible. Los Inspectores celebran que varias organizaciones hayan manifestado su intención de reforzar este aspecto, pero observan que, incluso en los casos en que el nivel de recursos permite ofrecer ese tipo de formación especializada, en la mayoría de las ocasiones se hace de forma puntual y sin objetivos de formación a largo plazo ni un enfoque sistemático. Especialmente en los casos en que no se han destinado específicamente recursos humanos para gestionar la ciberseguridad de un modo coherente, la disponibilidad de oportunidades de formación adecuadas para el personal al que se pide que se ocupe de aspectos relevantes cobran especial importancia.

Un centro de operaciones de seguridad aporta coherencia a la respuesta operacional en materia de ciberseguridad

117. **Principales funciones de un centro de operaciones de seguridad.** Un centro de operaciones de seguridad es una dependencia orgánica dedicada principalmente a las operaciones cotidianas de ciberseguridad. Aunque inevitablemente existen diferencias entre sus diversas manifestaciones, el mandato más amplio posible encomienda al centro la vigilancia de la seguridad de una entidad mediante la prevención, detección, análisis y respuesta a los incidentes de ciberseguridad. Los expertos en ciberseguridad suelen decir que un centro de operaciones de seguridad está integrado por personas, tecnología y procesos, y constituye el núcleo de las operaciones de recogida, correlación y análisis de flujos de información procedentes de diversas fuentes en tiempo real. La información interna reunida y procesada por este tipo de centros puede incluir datos procedentes de fuentes tales como dispositivos de red, servidores y aplicaciones alojadas, computadoras de escritorio y dispositivos móviles, sistemas de seguridad física y soluciones de seguridad especializadas. Un centro de operaciones de seguridad también recopila y procesa información sobre amenazas procedente de fuentes externas, por lo general consultando una combinación de fuentes abiertas (incluida la información gubernamental de acceso público) e información comercial sobre amenazas, que se correlaciona con los datos recopilados internamente y se analiza en busca de indicios de amenazas emergentes. Dada la complejidad de las tareas y la diversidad de los conocimientos necesarios, la creación y el mantenimiento de un centro de operaciones de seguridad totalmente equipado y funcional puede ser una empresa compleja y costosa. Si es necesario contar con un centro de este tipo y, en caso afirmativo, si debe crearse internamente o contratarse a un proveedor, son cuestiones a las que debe responder cada organización en función de sus necesidades.

118. **Soluciones internas, subcontratadas o híbridas para los centros de operaciones de seguridad: las configuraciones varían de una organización a otra.** Existen opiniones divergentes entre las organizaciones participantes sobre las ventajas e inconvenientes de las soluciones internas frente a las externas, lo que se pone de manifiesto en la diversidad de acuerdos y prácticas que los Inspectores constataron durante su examen. Algunas organizaciones recurren a un centro de operaciones de seguridad virtual o distribuido, en el sentido de que algunas de sus funciones están repartidas entre un conjunto descentralizado de recursos humanos. Varias entidades han tomado la decisión de crear su propio centro interno, mientras que otras utilizan un centro externo en virtud de un contrato con un proveedor comercial o comparten centro con otras entidades a través del servicio conexo del CICE, ya sea como recurso exclusivo o en combinación con una dependencia interna con capacidad básica. En algunos casos, las organizaciones que utilizan este tipo de soluciones híbridas han trazado una línea divisoria entre las funciones estratégicas y de supervisión, por una parte, que siguen siendo gestionadas internamente, y que el control operacional, sobre todo cuando se trata de una vigilancia permanente (24 horas al día, los 7 días de la semana), que se delega en proveedores externos. Algunas organizaciones incluso utilizan más de un centro de operaciones de seguridad, lo que les permite aislar ciertos datos especialmente

sensibles del conjunto de datos confiado a la gestión de equipos externos. Los Inspectores observaron que algunas organizaciones participantes estaban estudiando la posibilidad de crear su propio centro de operaciones de seguridad.

119. **Elementos considerados para las disposiciones relativas al centro de operaciones de seguridad.** Los argumentos a favor de un centro interno incluyen la capacidad de reaccionar más rápidamente ante amenazas y vulnerabilidades y controlar los dispositivos conectados, ciertamente a un costo más elevado. Se dice que este mayor control se consigue gracias a que la visibilidad de los dispositivos y su estado es más directa y se puede corregir la situación de riesgo de cada punto en tiempo real. Además, se considera que un centro interno ofrece un medio eficaz para centralizar las funciones de ciberseguridad, lo que, según un amplio consenso en el sector, conduce a una mayor ciberresiliencia en general. Para muchas organizaciones del sistema de las Naciones Unidas, el costo de la gestión de un centro de operaciones de seguridad interno podría resultar prohibitivo, y los beneficios obtenidos quizá no sean proporcionales al perfil de ciberseguridad de esas organizaciones y los requisitos de protección conexos. Solo un reducido número de entidades de las Naciones Unidas puede permitirse el mantenimiento de un programa completo de ciberseguridad para hacer frente a las amenazas y responder de manera autónoma, recurriendo únicamente a su capacidad interna. Además, aunque una organización llegue a establecer estructuras adecuadas, es posible que no pueda mantener un equipo fijo de guardia, integrado por expertos en ciberseguridad con amplia formación y múltiples aptitudes, capaz de responder a ciberataques complejos, que, por otra parte, suelen ser poco frecuentes e irregulares, lo que implica cierta fluctuación en la especialización necesaria. Además, algunas organizaciones consideran que mantener una capacidad interna suficiente para gestionar todas las tareas operacionales no permite suplir la experiencia de los proveedores externos especializados, que además suelen contar con más recursos para invertir en la investigación y el desarrollo que se consideran indispensables en el dinámico campo de la ciberseguridad. Al mismo tiempo, incluso cuando las entidades opten por la externalización, se ha señalado la necesidad de que exista un nivel suficiente de capacidad interna y representación de algunas de las funciones básicas relacionadas con la ciberseguridad, un equipo que conozca muy bien los flujos de trabajo y procesos internos y que pueda servir también de punto de contacto efectivo con el proveedor externo. En los casos en los que se recurre a centros de operaciones de seguridad externos, la gestión de los proveedores también se convierte en una de las principales preocupaciones y requiere, entre otras cosas, procesos de aprobación exhaustivos, la inclusión de cláusulas de protección jurídica adecuadas en los contratos y evitar depender de los proveedores. Algunos de los pros y contras de la externalización de un centro de operaciones de seguridad también pueden aplicarse a otras decisiones relativas al uso de las capacidades internas frente a las externas para la gestión de la ciberseguridad y se resumen en el recuadro 8.

Recuadro 8
Recurso a proveedores externos para un centro de operaciones de seguridad y otros servicios de ciberseguridad

Pros:

- Permite contar con una serie de competencias y herramientas diversas, actualizadas y altamente especializadas.
- Puede aumentar la eficiencia en relación con los costos.
- Ofrece la posibilidad de aumentar o reducir la escala de las operaciones en función de los cambios en el panorama de las amenazas y de las fluctuaciones de las necesidades de capacidad.
- Percepción de neutralidad e imparcialidad.

Contras:

- Riesgo de dependencia del proveedor (efecto *"lock-in"*).
- Pueden surgir dificultades para la personalización de servicios y soluciones normalizados y que ello conduzca a soluciones subóptimas y rígidas.

- Aumento de la dependencia de personal desconocido o que no ha seguido un proceso de selección y se encuentra bajo el control directo de los administradores.
- Posibilidad de exposición de datos confidenciales en la interacción con terceros.
- Escasa transparencia en torno a la notificación de incidentes.
- Costos.

120. **Un centro de operaciones de seguridad aumenta la coherencia en la respuesta de ciberseguridad.** Cada organización debe evaluar la conveniencia de establecer un centro de operaciones de seguridad basándose en un análisis de costos y beneficios que incluya parámetros tales como la complejidad de la configuración de su infraestructura de TIC, el número y tipo de activos y procesos críticos gestionados, y el volumen global de los flujos de datos y, por tanto, la frecuencia de las amenazas, que pueden sugerir una mayor o menor necesidad de supervisión y protección constantes. Los Inspectores desean destacar que uno de los aspectos importantes de un centro de operaciones de seguridad oficial —independientemente de su tamaño y capacidad— es el enfoque y la coherencia que proporciona a la vigilancia y a las operaciones cotidianas de una organización. Incluso si se trata de un equipo muy pequeño que necesita recurrir a personal de TIC de otros departamentos de la organización o a proveedores externos, puede desempeñar una función crucial de coordinación y sincronización y aumentar la sensibilización en la organización. **Por lo tanto, los Inspectores sugieren que los jefes ejecutivos consideren la opción de crear un centro de operaciones de seguridad o de racionalizar las capacidades existentes para crear un mecanismo equivalente, sobre la base de un examen crítico de sus necesidades institucionales y de las capacidades internas y externas con las que ya cuentan, y que se aseguren de poder fundamentar plenamente su decisión de instituir o no un centro de operaciones de seguridad.**

K. Reflejo e información de las medidas adoptadas en toda la organización para aumentar la ciberresiliencia

121. La medida en que los elementos detallados en el presente capítulo se reflejan en el enfoque adoptado por una organización con respecto a la ciberseguridad influye directamente en su posición y capacidad para identificar, prevenir y detectar ciberamenazas, así como para responder y recuperarse si se produce un incidente. Sabedores de que las disposiciones que se hayan adoptado pueden obedecer a una elección estratégica u operativa o estar dictadas por otras consideraciones, los jefes ejecutivos deberían iniciar un examen global para estudiar el grado de integración de cada uno de estos elementos en las políticas y prácticas de su organización.

122. Se espera que la aplicación de las siguientes recomendaciones mejore la eficacia de la preparación y la respuesta de las organizaciones del sistema de las Naciones Unidas en el ámbito de la ciberseguridad.

Recomendación 1

Los jefes ejecutivos de las organizaciones del sistema de las Naciones Unidas deberían preparar, con carácter prioritario y a más tardar en 2022, un informe completo sobre su marco de ciberseguridad que abarque los factores que contribuyen a aumentar la ciberresiliencia examinados en el presente documento, y presentarlo a sus respectivos órganos legislativos y rectores a la mayor brevedad posible.

123. Las conclusiones de ese examen interno deben ser comunicadas a los órganos legislativos y rectores, considerando los puntos fuertes y débiles identificados y sugiriendo medidas para reforzar aún más la ciberresiliencia. En opinión de los Inspectores, los órganos legislativos y rectores estarían entonces mejor situados para ofrecer una orientación estratégica de alto nivel con referencia a una declaración explícita sobre la voluntad de asumir riesgos en materia de ciberseguridad y para asignar recursos con objeto de alcanzar el nivel

de protección deseado. Como ya se ha dicho, la dirección ejecutiva debería considerar la posibilidad de informar regularmente sobre asuntos de ciberseguridad a los órganos legislativos y rectores. Los Inspectores reconocen que parte de la información presentada en un informe de este tipo puede ser sensible y quizá deba ser tratada con el nivel de confidencialidad apropiado. **Por lo tanto, se aconseja a la dirección ejecutiva que observe la máxima precaución a la hora de seleccionar el canal de información y el formato de esta, a fin de proporcionar suficiente perspectiva al correspondiente órgano legislativo y rector sin poner en peligro las defensas de la organización.**

Recomendación 2

Los órganos legislativos y rectores de las organizaciones del sistema de las Naciones Unidas deberían examinar los informes sobre los factores que contribuyen a aumentar la ciberresiliencia preparados por los jefes ejecutivos y, cuando sea necesario, proporcionar orientación estratégica sobre las nuevas mejoras que deban llevarse a cabo en sus respectivas organizaciones.

IV. La ciberseguridad desde la perspectiva de todo el sistema

A. Ciberseguridad: ¿una prioridad para todo el sistema?

124. **La colaboración a nivel de todo el sistema en la esfera de la ciberseguridad ha sido una prioridad desde hace tiempo.** Los Estados Miembros y los funcionarios de las Naciones Unidas al más alto nivel han declarado desde hace muchos años que el fortalecimiento de la posición de ciberseguridad del sistema de las Naciones Unidas debía ser una prioridad. Por ejemplo, en 2008 la Asamblea General alentó al Secretario General a que, en su calidad de Presidente de la JJE, promoviera una mayor coordinación y colaboración entre las organizaciones de las Naciones Unidas en todas las cuestiones relacionadas con la tecnología de la información y las comunicaciones, la planificación de los recursos institucionales y, en particular, la seguridad, la recuperación en casos de desastre y la continuidad de las operaciones[29]. En 2013, la Comisión Consultiva en Asuntos Administrativos y de Presupuesto, al examinar un informe sobre los progresos realizados en la aplicación de las recomendaciones relativas al fortalecimiento de la seguridad de la información y los sistemas en la Secretaría, alentó al Secretario General a que siguiera tratando de obtener la colaboración de todo el sistema y considerara todas las opciones que permitieran a las organizaciones del sistema de las Naciones Unidas seguir cooperando y compartiendo soluciones en materia de seguridad de la información[30]. Más recientemente, en 2019, el propio Secretario General, en las observaciones formuladas a modo de conclusión tras un debate celebrado por la JJE, destacó la importancia de fortalecer la capacidad propia del sistema de las Naciones Unidas para protegerse de los ciberataques[31]. El supuesto en que se ha basado esta visión es que una mayor colaboración a nivel de todo el sistema, que incluya enfoques conjuntos y soluciones operacionales compartidas, es uno de los factores más importantes a la hora de lograr un mayor nivel de protección para el sistema en su conjunto.

125. **Intentos de adopción de un enfoque estratégico conjunto.** Como ya se ha expuesto, en términos generales las organizaciones del sistema de las Naciones Unidas se enfrentan a las mismas dificultades y amenazas en el entorno cibernético, por lo que cabría pensar que se puede aplicar un enfoque conjunto para darles respuesta. Teniendo en cuenta que la seguridad del sistema en su conjunto depende, al menos en parte, de la seguridad de cada uno de sus miembros, ya que estos están interconectados a varios niveles, existen razones de peso para plantearse dicha posibilidad. Durante la elaboración del presente examen, varias organizaciones participantes abogaron por el establecimiento de una estrategia común para su adopción y ejecución por los distintos órganos —que también presentarían informes al

[29] Resolución 63/262 de la Asamblea General.
[30] A/68/7/Add.11, párr. 6.
[31] CEB/2019/2, párr. 39.

respecto— en tanto que asociados actuando de forma concertada e impulsados por el objetivo común de que el sistema en su conjunto alcanzara un determinado nivel de madurez sobre la base de una serie de criterios mínimos que todos deberían cumplir. En los documentos de 2017 de la Red Digital y Tecnológica aparece un llamamiento al establecimiento de una estrategia de ciberseguridad para todo el sistema con el objetivo de contribuir a crear una base para armonizar las prácticas en materia de ciberseguridad[32]. No obstante, no parece que la iniciativa se materializara o tuviera ningún seguimiento tangible. Otro intento de promover un enfoque armonizado incluía la propuesta de recabar anualmente información de las organizaciones sobre las medidas adoptadas en materia de ciberseguridad con el fin de establecer una referencia interna relativa a la madurez del sistema y evaluar mejor su exposición global al riesgo. Pese a que se llevó a cabo una importante labor preparatoria, que incluyó dos rondas piloto de encuestas realizadas entre aproximadamente 20 organizaciones en el transcurso de 2018 y 2019, la propuesta no logró recabar el apoyo colectivo del personal directivo superior. Los principales argumentos que se adujeron para rechazar esos intentos de establecer análisis comparativos fueron, por un lado, la diversidad de las estructuras y contextos de las organizaciones, que limitaba el valor de toda evaluación colectiva, y, por otro, la escasa preparación de las entidades para comunicar sus evaluaciones internas en materia de ciberseguridad fuera de su organización, por lo que en la práctica se mencionaban los riesgos de ciberseguridad como el principal obstáculo para realizar siquiera una evaluación acumulativa. Las opiniones expresadas durante las entrevistas parecen indicar que la pandemia de COVID-19 podría haber modificado las percepciones y mentalidades en la esfera de la ciberseguridad y que algunas propuestas que antes se consideraban demasiado ambiciosas o poco realistas hoy podrían tener más posibilidades de despertar interés y ser bien acogidas. De hecho, parece que en el contexto de la última reunión interinstitucional entre expertos en ciberseguridad resurgió el debate sobre la idoneidad de aplicar un modelo de madurez de referencia similar al adoptado recientemente por el Foro de Gestión de Riesgos de la JJE.

126. **Responsabilidad colectiva para garantizar un nivel mínimo de defensa.** En efecto, quizá una armonización de todo el sistema basada principalmente en las conclusiones extraídas de una evaluación comparativa de la madurez entre las organizaciones podría ser demasiado ambiciosa e incluso improcedente. Como ha expuesto el centro de estudios Gartner, tratar de comparar las diferentes disposiciones y medidas institucionales en materia de ciberseguridad podría permitir extraer conclusiones sobre la madurez relativa de cada organización, pero no proporcionaría ninguna información fiable sobre el nivel absoluto de protección de ninguna de ellas[33]. Aun así, el hecho de que las organizaciones del sistema de las Naciones Unidas sean interdependientes tanto en términos de reputación como desde el punto de vista operacional hace que tengan la responsabilidad colectiva de elevar el listón al máximo para todos y de ayudarse mutuamente para alcanzarlo. Cabe señalar que las organizaciones que contaban con un marco de ciberseguridad avanzado y una sólida capacidad interna o externa fueron las que más apoyaron este tipo de iniciativas. Es fundamental que el sistema logre el delicado objetivo de encontrar el justo equilibrio entre las respectivas exigencias de las organizaciones participantes, las disposiciones por ellas adoptadas y un enfoque global de todo el sistema para establecer las normas mínimas que deben ser cumplidas por todos en beneficio de todos. **En opinión de los Inspectores, establecer un nivel básico de protección y unos requisitos mínimos de defensa para las organizaciones de las Naciones Unidas, y por consiguiente para el sistema en su conjunto, sigue siendo un objetivo válido que merece la pena tratar de alcanzar.**

127. **Medidas adoptadas para instituir una capacidad compartida a nivel operacional.** La posibilidad de establecer una capacidad federada de todo el sistema para prevenir y detectar las amenazas y ataques cibernéticos y darles respuesta ha sido debatida en numerosas ocasiones a diversos niveles. Hace casi diez años, la Red Digital y Tecnológica elaboró una hoja de ruta para la creación de un equipo de respuesta a incidentes informáticos a nivel de las Naciones Unidas[34], pero la iniciativa no se materializó porque no pudo alcanzarse un acuerdo sobre el modelo de financiación. Más recientemente, el Grupo de Interés Especial

[32] CEB/2017/HLCM/ICT/9, págs. 7 y 8.

[33] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, febrero de 2020.

[34] CEB/2013/5, párrs. 38 y 39.

sobre la Seguridad de la Información reanudó su labor de evaluación de la viabilidad de establecer un centro de operaciones de seguridad compartido entre las entidades de las Naciones Unidas, si bien los debates que surgieron entre sus miembros pusieron de manifiesto la persistencia de numerosas dificultades, como el prorrateo de los costos, la adecuación a las variadas capacidades ya existentes, el acuerdo sobre el alcance esperado y la priorización del apoyo en caso de ataque generalizado, entre otros. Estas iniciativas se han basado en la esperanza de que establecer una capacidad de respuesta a incidentes a nivel de todo el sistema permitiría aumentar notablemente la eficiencia a la vez que ofrecería una mayor protección, en especial en el caso de las organizaciones que no pueden permitirse mantener una capacidad de reserva para responder a un hipotético ataque que, sin embargo, podría producirse en cualquier momento. Todos estos intentos ponen de manifiesto que los objetivos, si bien son claros y cuentan con sólidos apoyos, son más difíciles de llevar a la práctica de lo que cabría pensar. La experiencia al respecto pone de manifiesto que la implementación de dichas iniciativas se vuelve compleja cuando estas alcanzan un determinado nivel de concreción.

128. **Actividades de capacitación y sensibilización, un ámbito que presenta aspectos contradictorios para la agrupación de recursos a nivel de todo el sistema.** Un ejemplo de propuesta prometedora que, al ser examinada con más detalle, resultó presentar aspectos contradictorios fue la esfera de la capacitación y la sensibilización en materia de ciberseguridad. La DCI examinó la cuestión de la colaboración en los programas de formación en el sistema de las Naciones Unidas en un informe reciente[35]. Una de sus conclusiones fue que existía una notable duplicación de esfuerzos en la creación de programas similares por parte de diferentes organizaciones. A primera vista, los recursos de capacitación y sensibilización sobre ciberseguridad parecen una opción natural para la colaboración a nivel de todo el sistema y la agrupación de recursos. Partiendo de la base de que la mayoría de los cursos de formación dirigidos a los usuarios finales puede estandarizarse, ya que una buena proporción de los correspondientes materiales didácticos no tiene que ser específico para cada organización, pues las amenazas a que se enfrentan son las mismas, uno de los primeros proyectos conjuntos llevados a cabo por el Grupo de Interés Especial sobre la Seguridad de la Información consistió en elaborar los componentes básicos de un plan de estudios común sobre ciberseguridad para su posterior adaptación y utilización por sus miembros. Dicho enfoque de establecimiento de un plan de estudios pareció ganar aceptación en varias organizaciones, que optaron por adoptar el módulo de sensibilización en línea sobre la seguridad de la información de la Secretaría de las Naciones Unidas o recurrieron al CICE y su servicio de sensibilización sobre la seguridad de la información para personalizar y adaptar contenidos en esta esfera. No obstante, los Inspectores no observaron un gran consenso entre las organizaciones participantes en cuanto a las ventajas de adoptar un enfoque común a la formación. De hecho, varias de ellas se opusieron con determinación a la adopción de un enfoque estandarizado aduciendo las especificidades de sus respectivos mandatos o las limitaciones que imponía el proceso colectivo de desarrollo, a menudo tedioso, que hacía que los contenidos elaborados quedaran rápidamente obsoletos y no fueran de fácil sustitución. Además, necesariamente dichos contenidos respondían a un enfoque de "mínimo común denominador", por lo que podrían no responder a las expectativas y los requisitos de los usuarios, a menos que luego se realizaran considerables inversiones para adaptarlos y ampliarlos. Teniendo en cuenta estos argumentos, varias organizaciones han diseñado sus propios módulos de capacitación, en ocasiones en colaboración con proveedores externos, lo que supone un costo nada desdeñable. **Los Inspectores siguen convencidos de que a las organizaciones del sistema de las Naciones Unidas les convendría disponer de programas de capacitación armonizados, aunque estos requirieran una adaptación posterior para algunas organizaciones.**

129. **Optimizar los recursos destinados a la ciberseguridad.** Todos los expertos y directivos entrevistados coincidieron en el hecho de que las entidades de las Naciones Unidas, tanto a título individual como colectivo, eran actores pequeños en comparación con las entidades del sector privado, y en que los recursos de que disponían para hacer frente y responder a los ataques externos más sofisticados llevados a cabo por la delincuencia organizada u otros agentes eran, en el mejor de los casos, limitados. Al mismo tiempo, las

[35] JIU/REP/2020/2.

organizaciones participantes suelen asignar recursos a la ciberseguridad de forma aislada y para un fin particular, en ocasiones por efecto de la presión ejercida por un incidente concreto. En el sistema reina la sensación de que se puede ganar en eficiencia adoptando un enfoque conjunto de la ciberseguridad, si bien las respuestas formuladas por las organizaciones participantes en la DCI acerca de las esferas en las que la agrupación de recursos podría ser factible y útil transmitieron visiones divergentes. Un ámbito que recibió respaldo como fuente de posibles ahorros de costos fue el establecimiento de una coordinación más estrecha en torno a la contratación de proveedores de servicios externos, y más concretamente de entidades comerciales y del sector privado. Muchas organizaciones confirmaron que recurrían a dichos proveedores y nombraron con frecuencia a las mismas empresas para servicios idénticos o parecidos, como evaluaciones de riesgos o vulnerabilidades, auditorías en relación con la norma ISO 27001 o soluciones específicas de *software*, lo que significa que cada una de ellas había sometido a las mismas empresas a sus respectivos procedimientos internos de selección y gestión de proveedores y les había pagado independientemente de las demás. Pese a la existencia de un acuerdo de reconocimiento mutuo firmado por 20 organizaciones, apenas un puñado indicaron que habían concertado memorandos de entendimiento o acuerdos similares entre ellas para aprovechar los procesos de adquisición o los contratos de servicios de otras organizaciones en relación con la protección y la respuesta en la esfera de la ciberseguridad. Los Inspectores reconocen que hay factores que limitan la aplicación a gran escala de esas iniciativas conjuntas, pero consideran que estas merecerían más atención para lograr una mayor eficiencia. A través de las entrevistas y el cuestionario, los Inspectores identificaron varios factores que dificultaban las adquisiciones conjuntas y los procesos colaborativos de adquisición en general. Los diferentes procedimientos y normas que el sistema aplica a las adquisiciones constituyen barreras y limitan la posibilidad de llevar a cabo procesos colaborativos de adquisición. Sin embargo, algunos obstáculos no están directamente relacionados con las normas y procedimientos, sino con la cultura de funcionamiento de las organizaciones, que favorece el estricto control organizativo por encima de la cooperación abierta. En este contexto, algunos de los obstáculos son las diferencias en la filosofía de funcionamiento entre los procesos de adquisición muy centralizados y los descentralizados, las diferencias en las modalidades de financiación (como los pagos anticipados) y la escasa armonización de los sistemas de TIC y de los sistemas de cuentas por pagar, como quedó reflejado en un informe de la DCI sobre cuestiones relacionadas con las adquisiciones[36]. En el peor de los casos, si la adquisición conjunta de determinados servicios no es viable, las organizaciones participantes deberían hacer todo lo que esté en su mano para coordinar al máximo sus esfuerzos. De lo contrario, la heterogeneidad en las prácticas de adquisición puede incentivar a los proveedores comerciales a aplicar tarifas diferentes a lo largo del sistema por el mismo servicio, generando con ello una forma de competencia que solo les beneficiaría a ellos y sería perjudicial para los intereses financieros de las organizaciones afectadas.

130. **Falta de medidas auténticamente concertadas a nivel de todo el sistema, más allá de mecanismos de coordinación y soluciones operacionales parciales.** Podría pensarse que la notable relevancia y el impulso adquiridos por la ciberseguridad en los más altos niveles directivos han creado las condiciones óptimas para impulsar avances significativos en el establecimiento de una capacidad a nivel de todo el sistema. Sin embargo, pese a la disponibilidad de varios recursos, mecanismos e iniciativas importantes dentro del sistema, incluida la aparente voluntad política, no hay indicios de que se haya progresado en hacer que esas declaraciones de intenciones se traduzcan en medidas reales. En este momento, ninguna entidad tiene el mandato formal de impulsar el establecimiento de un enfoque armonizado de la ciberseguridad ni de elaborar y aplicar soluciones compartidas para las organizaciones del sistema de las Naciones Unidas. Actualmente, desde el punto de vista institucional, los esfuerzos realizados a nivel de todo el sistema en materia de ciberseguridad se concentran en los mecanismos de coordinación interinstitucional dirigidos por la JJE, que cuentan hasta cierto punto con el apoyo operacional del CICE en calidad de proveedor de determinados servicios compartidos para varias organizaciones del sistema de las Naciones Unidas. En el presente capítulo, los Inspectores examinan las respectivas disposiciones institucionales y operacionales, fijándose también en el aparente grado de desconexión entre

[36] Véase JIU/REP/2013/1.

ellas, y la dinámica interinstitucional imperante en esta materia (anexo VI). Además, tratan de identificar los progresos realizados hasta el momento, las ventajas y limitaciones inherentes a la estructura actual y los ámbitos en los que podría reforzarse la acción colectiva para la elaboración de respuestas globales de todo el sistema de las Naciones Unidas, en la medida en que ello sea práctico y razonable.

B. Mecanismos interinstitucionales que abordan la ciberseguridad

131. **Un largo historial de interés por parte de los mecanismos interinstitucionales.** Bajo los epígrafes "seguridad de la información" o "seguridad de los sistemas de información", la ciberseguridad ha estado presente en el discurso sobre las tecnologías de la información a nivel de todo el sistema desde la época del Comité Administrativo de Coordinación. Ya en 1994 se encargó a un equipo de tareas creado por la entidad predecesora de la Red de Tecnología de la Información y las Comunicaciones (conocida desde 2018 con el nombre de Red Digital y Tecnológica) que examinara un conjunto de "directrices relativas a la seguridad de los sistemas de información para las organizaciones de las Naciones Unidas", publicadas en 1992[37], lo que hace pensar que se habían invertido una atención y un esfuerzo considerables en esta cuestión desde incluso antes. Cabe señalar que dichas directrices representan un intento exhaustivo y sorprendentemente avanzado de delinear las diversas dimensiones de la ciberseguridad y proporcionar orientación al respecto, a nivel tanto de gestión como operacional. La terminología empleada en el documento, algo anticuada, no debe hacernos pasar por alto el hecho de que una parte no desdeñable de sus contenidos y recomendaciones siguen siendo pertinentes 30 años después.

132. **Interés continuado en un enfoque coordinado de la ciberseguridad.** La idea de adoptar una respuesta coordinada a las ciberamenazas seguía apareciendo en los documentos oficiales diez años después, en 2002, cuando los miembros de la JJE reconocieron que, "si bien las necesidades de las organizaciones en materia de seguridad tienen categorías diferentes (ya que algunas disponen de bases de datos extremadamente confidenciales y delicadas), hay cuestiones importantes comunes a todas las organizaciones que deben tratarse con la máxima urgencia"[38]. En 2010, el término "seguridad de la información" parece haber sido sustituido por el de "ciberseguridad", que cobró un gran impulso cuando se volvió a defender la necesidad de definir un "modelo para un enfoque global de todo el sistema" en materia de ciberseguridad y se describieron los efectos de las ciberamenazas en "todos los sectores" como un "posible cibertsunami"[39]. En los años posteriores se formularon declaraciones parecidas a nivel del Comité de Alto Nivel sobre Gestión en relación con el hecho de que se detectaban "notables puntos de coincidencia con respecto a la mejor manera de proteger [a las organizaciones del sistema de las Naciones Unidas] frente a las interrupciones de las actividades y las amenazas a la seguridad"[40], mientras que la Red de Tecnología de la Información y las Comunicaciones declaró que "mejorar la capacidad de los organismos para resistir a las ciberamenazas debe seguir siendo una prioridad"[41].

133. **Documentos emblemáticos a nivel de todo el sistema sobre ciberseguridad y ciberdelincuencia aprobados en 2013 y 2014.** En 2010, la JJE encargó al Comité de Alto Nivel sobre Gestión y al Comité de Alto Nivel sobre Programas que se ocuparan de la cuestión de forma conjunta bajo la dirección de la UIT y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), a las que luego se sumaron la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), el PNUD y la UNESCO. Esta iniciativa transversal culminó con la aprobación en 2013 del marco sobre ciberseguridad y ciberdelincuencia para todo el sistema de las Naciones Unidas[42] y en 2014 del plan de coordinación interna del sistema de las Naciones Unidas sobre ciberseguridad y

[37] Comité Consultivo para la Coordinación de los Sistemas de Información, *Information System Security Guidelines for the United Nations Organizations*, Nueva York, 1992.

[38] CEB/2002/HLCM/10, párr. 8.

[39] CEB/2010/1, párr. 53.

[40] CEB/2013/5, párr. 36.

[41] CEB/2013/2, párr. 58.

[42] *Ibid.*, párr. 85, y anexo III (Marco sobre ciberseguridad y ciberdelincuencia para todo el sistema de las Naciones Unidas).

ciberdelincuencia, basado en el primero[43]. Ambos documentos, si bien se centran principalmente en la dimensión de "proyección exterior" de la labor realizada por las Naciones Unidas (es decir, las actividades programáticas destinadas a apoyar las iniciativas de los Estados Miembros en esta esfera), proporcionan un punto de partida sólido para enmarcar la dimensión "interior" de la ciberseguridad para el sistema (recuadro 9). No obstante, los Inspectores observaron que ninguna organización participante había hecho referencia al marco o al plan durante la preparación del examen. Si bien no parece que el plan como tal se convirtiera en un punto de referencia duradero para el sistema, los Inspectores observaron con satisfacción que los principios y elementos básicos contenidos en él seguían sirviendo de base para el plan de trabajo de los órganos interinstitucionales pertinentes activos en esta esfera.

Recuadro 9
Marco para todo el sistema y plan de coordinación interna en materia de ciberseguridad y ciberdelincuencia

Aprobado por la JJE en su segundo período ordinario de sesiones, celebrado en 2013, el marco sobre ciberseguridad y ciberdelincuencia para todo el sistema de las Naciones Unidas sienta las bases para establecer una coordinación entre las organizaciones del sistema de las Naciones Unidas en respuesta a las preocupaciones de los Estados Miembros relativas a la ciberdelincuencia y la ciberseguridad.

El marco:

- Introduce algunas definiciones comunes de conceptos clave y esboza el alcance de la materia tratada.
- Señala la intersección entre los mandatos de las entidades interesadas en relación con la cuestión.
- Establece los principios básicos para la elaboración de programas y la prestación de asistencia técnica en relación con la ciberdelincuencia y la ciberseguridad.
- Contiene orientaciones para el refuerzo de la cooperación en la prestación de asistencia técnica a los Estados Miembros en este ámbito.

Sobre la base del marco, en 2014 se diseñó el plan de coordinación interna del sistema de las Naciones Unidas sobre ciberseguridad y ciberdelincuencia con el fin de orientar la coordinación interna entre las organizaciones del sistema de las Naciones Unidas en la esfera de la ciberseguridad y la ciberdelincuencia, que se centró en cinco temas que el Secretario General había señalado como susceptibles de ser abordados mediante la acción conjunta de todo el sistema. Para cada uno de esos temas, el plan enunciaba una serie de principios comunes y líneas de actuación que las organizaciones eran invitadas a adoptar. En particular, se animó a los jefes ejecutivos a que elaboraran y pusieran en marcha un curso de capacitación obligatorio por computadora sobre ciberseguridad dirigido al personal, basado en un programa de formación acordado por la Red de Tecnología de la Información y las Comunicaciones, y a que establecieran un equipo interinstitucional de respuesta a incidentes informáticos. Estos mismos puntos fueron los que el Presidente del Comité de Alto Nivel sobre Gestión consideró líneas de actuación pertinentes para el trabajo del Comité (CEB/2014/5, párr. 72).

El siguiente tema tiene particular interés para el presente examen:

> Tema 1: Establecer una preparación interna eficaz para hacer frente a las ciberamenazas en los distintos organismos y en todo el sistema de las Naciones Unidas, que tenga en cuenta los obstáculos en materia de políticas y recursos que puedan impedir que los organismos actúen de forma conjunta para proteger mejor el sistema de las Naciones Unidas, por ejemplo mediante la inclusión de la ciberseguridad en los marcos de evaluación y gestión de riesgos.

[43] Plan de coordinación interna del sistema de las Naciones Unidas sobre ciberseguridad y ciberdelincuencia, noviembre de 2014, documento interno.

134. **El Grupo de Interés Especial sobre la Seguridad de la Información como principal foro de expertos en ciberseguridad del sistema.** En términos globales, se consideró que el mecanismo interinstitucional que se ocupa de la ciberseguridad en el sistema de las Naciones Unidas está bien establecido y por lo general funciona. El Grupo de Interés Especial sobre la Seguridad de la Información, creado en 2011 como principal mecanismo del sistema de las Naciones Unidas para la promoción de la cooperación y la colaboración interinstitucionales a fin de optimizar la seguridad de la información dentro de las organizaciones que lo integran, actúa bajo la autoridad jerárquica de la Red Digital y Tecnológica, de la que recibe instrucciones, y bajo la orientación general del Comité de Alto Nivel sobre Gestión. Según se establece en su mandato, su composición está explícitamente restringida a los oficiales principales de seguridad de la información, o cargo equivalente, de las organizaciones miembros de la JJE. Las organizaciones que no cuentan con dicho puesto suelen estar representadas por un funcionario de TIC. Entre los métodos de trabajo del Grupo de Interés Especial sobre la Seguridad de la Información figuran un simposio anual, que cuenta con la participación de ponentes externos, una reunión ejecutiva para la toma de decisiones formal, que se celebra durante el simposio anual, y grupos de trabajo de duración determinada, en los que las organizaciones se ofrecen para moderar deliberaciones sobre temas de interés. Varias organizaciones no miembros de la JJE, como el CICE, participan en la labor del Grupo de Interés Especial sobre la Seguridad de la Información en calidad de observadoras sin derecho de voto. Ocupa la presidencia del grupo, que tiene carácter rotatorio, uno de sus miembros oficiales. En el momento de redactarse el presente informe la ocupaba la Oficina de Tecnología de la Información y las Comunicaciones de la Secretaría de las Naciones Unidas.

135. **Se confirma la utilidad del principal órgano interinstitucional como foro de diálogo.** El Grupo de Interés Especial sobre la Seguridad de la Información ha adquirido una notable credibilidad profesional como foro oficial en el que los profesionales de la ciberseguridad de las Naciones Unidas se reúnen periódicamente para debatir sobre las dificultades, oportunidades y buenas prácticas para el sistema en su conjunto. Un análisis del contenido de los informes recientes de los simposios celebrados por el Grupo de Interés Especial sobre la Seguridad de la Información confirma que en el seno del Grupo despiertan interés y generan ricos debates una amplia gama de cuestiones operacionales y estratégicas, como la seguridad y la gestión de riesgos en la nube, la gestión de la identidad digital, el análisis comparado de la madurez en materia de ciberseguridad, los programas de sensibilización sobre la seguridad de la información y, más recientemente, la idea de establecer un centro de operaciones de seguridad compartido y la consolidación de los servicios de inteligencia sobre amenazas. De hecho, en las respuestas al cuestionario distribuido por la DCI, aproximadamente dos tercios de las organizaciones participantes afirmaron que consideraban que el Grupo era eficaz en la promoción de la cooperación y la colaboración entre las entidades de las Naciones Unidas y que valoraban las contribuciones sustantivas de sus miembros y las oportunidades de diálogo con expertos externos, incluidos los del sector privado. Muchos miembros elogiaron las iniciativas adoptadas por el Presidente para facilitar el debate profesional y hacer avanzar el plan de trabajo del Grupo. Ya se están abordando algunas debilidades del funcionamiento del Grupo, como la poca frecuencia con que se celebran los simposios del Grupo de Interés Especial sobre la Seguridad de la Información y la falta de interacciones entre períodos de sesiones, que según algunos miembros deberían intensificarse para facilitar un diálogo más continuado e informal. En respuesta a una clara necesidad en este sentido, se creó un canal de mensajería instantánea para que los miembros del Grupo de Interés Especial sobre la Seguridad de la Información pudieran mantener un diálogo informal directo, establecer una comunicación rápida y compartir información cuando fuera necesario. Las medidas destinadas a facilitar la comunicación cotidiana fueron elogiadas por los oficiales principales de seguridad de la información, que también confirmaron haber utilizado activamente esos canales en su trabajo diario.

136. **El mecanismo interinstitucional, pendiente de la ciberseguridad a todos los niveles.** Desde el propio Grupo de Interés Especial sobre la Seguridad de la Información hasta la Red Digital y Tecnológica, pasando por el Comité de Alto Nivel sobre Gestión, quedó claro que la ciberseguridad era objeto de un activo debate y se consideraba crítica. En lo que respecta a la Red Digital y Tecnológica, que reúne a los responsables de los

departamentos de TIC y recibe los informes y recomendaciones del Grupo de Interés Especial sobre la Seguridad de la Información para su aprobación y remisión al Comité de Alto Nivel sobre Gestión, uno de los diez objetivos establecidos en su mandato revisado de 2019 es "la seguridad de la información y la ciberseguridad"[44]. Cabe afirmar que, por regla general, la Red Digital y Tecnológica ha apreciado en la práctica la labor desempeñada por el Grupo de Interés Especial sobre la Seguridad de la Información, ya que en raras ocasiones ha adoptado una posición distinta de este y ha respaldado la mayor parte de sus recomendaciones, a veces introduciendo modificaciones. En cuanto al Comité de Alto Nivel sobre Gestión, que desempeñó un papel importante en la elaboración del marco de 2013 y el plan de coordinación de 2014, la ciberseguridad ha figurado en sus planes estratégicos, incluido el más reciente (2017-2020), como un elemento de la prioridad estratégica atribuida a la gestión de riesgos y el fomento de la resiliencia. En este último plan figura una declaración en la que se indica que el Comité de Alto Nivel sobre Gestión adoptará nuevas medidas a nivel de todo el sistema, entre ellas medidas de mitigación, para promover que las ciberamenazas se sometan a vigilancia y reciban respuesta[45]. Pese a ello, en sus documentos el Comité pone de manifiesto que, si bien es claramente consciente de que la ciberseguridad es motivo de preocupación en términos generales, rara vez le llegan recomendaciones o puntos concretos en relación con este tema. En este contexto, los Inspectores observan que, en su respuesta al cuestionario distribuido por la DCI, solo un tercio de las organizaciones participantes dijeron considerar que el Grupo de Interés Especial sobre la Seguridad de la Información era eficaz a la hora de dar impulso a la adopción de medidas en los niveles superiores del mecanismo de la JJE.

137. **La aplicación de los consejos y orientaciones que formula el Grupo de Interés Especial sobre la Seguridad de la Información depende de la voluntad de sus miembros.** Durante el presente examen, los Inspectores observaron que la coordinación y la colaboración interinstitucionales en el sistema de las Naciones Unidas en materia de ciberseguridad aún no habían dado los frutos esperados. Si bien cada año se lleva a cabo un ingente trabajo conceptual a través del Grupo de Interés Especial sobre la Seguridad de la Información, y pese a que el tema ha captado la atención del personal directivo superior, la materialización de los progresos hacia soluciones compartidas, enfoques comunes o concertados y proyectos conjuntos ha sido lenta. A modo de contexto, cabe recordar que la versión más reciente del mandato del Grupo, revisado en 2018[46], refleja su compromiso de compartir conocimientos, experiencias y soluciones y contempla, en particular, la ejecución de proyectos conjuntos. De hecho, ese mismo año, con motivo de la transición emprendida por la Red de Tecnología de la Información y las Comunicaciones para convertirse en la Red Digital y Tecnológica y de la revisión de los mandatos de cada uno de sus subgrupos, la recién rebautizada Red fue más allá al decidir que, además de promover la colaboración interinstitucional y el intercambio de conocimientos en la esfera de la seguridad de la información, era necesario que el Grupo de Interés Especial sobre la Seguridad de la Información fuera más activo en el diseño y la puesta en práctica de soluciones compartidas y en las actividades de innovación[47]. Pese a ello, esta visión de la Red Digital y Tecnológica de que dicho subgrupo dedique más esfuerzos a la elaboración práctica de soluciones para el sistema no parece respaldado por ninguna capacidad operativa, independientemente de los recursos internos de sus miembros y del nivel individual de compromiso en esta esfera. En la práctica, el Grupo de Interés Especial sobre la Seguridad de la Información no dispone de un mecanismo eficaz para facilitar la implementación y ejecución conjunta de las soluciones propuestas o los acuerdos alcanzados en el contexto interinstitucional. Teniendo en cuenta que no le corresponde a un órgano de coordinación la responsabilidad primordial de ocuparse de la aplicación de sus propias recomendaciones, la ausencia de un "órgano operativo" oficial para el sistema en su conjunto, que reciba las instrucciones del colectivo de oficiales principales de seguridad de la información y sirva al interés común, es, en opinión de los Inspectores, uno de los principales factores que obstaculizan el avance hacia un enfoque global de la ciberseguridad para todo el sistema. En las siguientes secciones del presente informe se examina con más detalle si

[44] CEB/2019/HLCM/DTN/03/R1, pág. 2.
[45] CEB/2016/HLCM/15, pág. 13.
[46] CEB/2018/HLCM/ICT/3/Rev. 1.
[47] CEB/2018/HLCM/ICTN/18, pág. 6.

otros mecanismos u órganos existentes pueden colmar razonablemente dicho déficit en la implementación.

138. **Responsabilidades de los oficiales principales de seguridad de la información a título individual y colectivo.** Se observó que el perfil de los miembros del Grupo de Interés Especial sobre la Seguridad de la Información era heterogéneo y su participación iba del nivel laboral al nivel estratégico, y que algunos oficiales principales de seguridad de la información ocupaban puestos de inicio en la categoría profesional, mientras que otros ocupaban puestos directivos de nivel medio o alto o dirigían departamentos enteros. Más allá de los conocimientos técnicos y de la cultura de discusión abierta que, según sus miembros, caracterizan los debates en el seno del Grupo de Interés Especial sobre la Seguridad de la Información, parece ser que la heterogeneidad de su composición afecta a las dinámicas que se establecen dentro del Grupo y ha repercutido directamente en su capacidad para proporcionar orientaciones autorizadas al sistema. Dado que cada miembro tiene responsabilidades distintas dentro de la estructura de su respectiva organización, lo que limita la capacidad de canalizar el compromiso de la entidad en cuestión en contextos interinstitucionales, las oportunidades que estos tienen para desempeñar un papel transformador, tanto dentro de esa organización como colectivamente mediante la acción concertada en todo el sistema, son restringidas. Como órgano de coordinación, el Grupo de Interés Especial sobre la Seguridad de la Información hace frente a las mismas dificultades en este sentido que cualquier otro mecanismo interinstitucional, al carecer de autoridad decisoria que imponga medidas directamente a nivel del sistema, por lo que sería poco realista esperar que la implementación se materializara en el seno de ese foro. Al mismo tiempo, el Grupo tiene poco poder de influencia en la forma en que los resultados de su trabajo se transmiten al personal directivo superior de cada organización. De los documentos de la Red Digital y Tecnológica se desprende con claridad que esta comprende bien dichas limitaciones, como demuestra la petición que formuló a sus propios miembros (los jefes de los departamentos de TIC) para que facultasen a los oficiales principales de seguridad de la información, entre otros, delegando en ellos más autoridad[48]. Cabe asimismo recordar que el propio Grupo de Interés Especial sobre la Seguridad de la Información actúa bajo la autoridad jerárquica de la Red Digital y Tecnológica, lo que reproduce la estructura que domina en la mayoría de las organizaciones —con sus dificultades asociadas—, en las que el oficial principal de seguridad de la información está supeditado al jefe de su respectivo departamento de TIC. Para contrarrestar las limitaciones que impone la estructura actual, **los Inspectores reiteran su petición de que el puesto de oficial principal de seguridad de la información, cuando exista, vea reforzadas sus responsabilidades internas, entre otras sus responsabilidades de gestión y su independencia del área de TIC, en la medida de lo posible, y de que se cree dicho puesto en caso de que no exista.** En cuanto al refuerzo de las responsabilidades de los oficiales principales de seguridad de la información como colectivo, los Inspectores observaron que, en general, había poco interés en elevar el rango del Grupo de Interés Especial sobre la Seguridad de la Información dentro del mecanismo interinstitucional desvinculándolo de la Red Digital y Tecnológica y otorgándole la condición de Red, lo que le permitiría rendir cuentas directamente al Comité de Alto Nivel sobre Gestión. Por un lado, se adujeron en contra de dicha transición argumentos como la proliferación generalizada de redes, equipos de tareas y foros de coordinación en el seno del mecanismo de la JJE, lo que se consideraba que, en sí mismo, difícilmente contribuiría a avanzar en esta cuestión o a darle una prioridad efectiva. Por otro, la opinión predominante parecía ser que el Grupo de Interés Especial sobre la Seguridad de la Información ya disponía de un canal adecuado y sólido para situar las consideraciones relativas a la ciberseguridad en el primer plano de los debates estratégicos a nivel de todo el sistema a través de la Red Digital y Tecnológica y el Comité de Alto Nivel sobre Gestión. **Los Inspectores reafirmaron que el Grupo de Interés Especial sobre la Seguridad de la Información había mejorado con eficacia el intercambio de información sobre ciberseguridad en el sistema de las Naciones Unidas y debía seguir desempeñando su función sin que se modificara la arquitectura existente. No obstante, señalan la necesidad de concebir un mecanismo que garantice que el Grupo de Interés Especial sobre la Seguridad de la Información, en su**

[48] Véase, por ejemplo, CEB/2017/HLCM/ICT/9, pág. 8.

condición de entidad independiente, pueda proporcionar orientación estratégica en nombre de la JJE y del sistema de las Naciones Unidas.

C. El Centro Internacional de Cálculos Electrónicos de las Naciones Unidas como proveedor de servicios de ciberseguridad

139. **Examen del potencial aún por aprovechar del CICE.** En el contexto de su informe de 2019 sobre la computación en la nube, la DCI ya pidió que se siguieran examinando las condiciones necesarias para aprovechar mejor el potencial del CICE y su amplia gama de servicios de TIC para el sistema de las Naciones Unidas. En ese momento se señaló que la ciberseguridad era uno de los ámbitos en los que se consideraba que ese potencial estaba suficientemente maduro para ser estudiado con más profundidad. Sin embargo, teniendo en cuenta la perspectiva más amplia que ofrece la reforma de las operaciones institucionales de las Naciones Unidas, los Inspectores consideran que sería conveniente llevar a cabo un nuevo examen, con un enfoque más holístico, del CICE y de su funcionamiento general, su modelo institucional, su estructura de gobernanza y su mandato, que lo llevara quizás incluso a superar los límites impuestos por su función establecida como proveedor de servicios de TIC a sus clientes, entre los que actualmente figuran las organizaciones del sistema de las Naciones Unidas. Desde su creación en 1971, que estuvo precedida por un informe detallado de auditoría externa encargado por el Secretario General —en su calidad de Presidente del mecanismo pertinente de coordinación interinstitucional— con el mandato de estudiar las instalaciones y necesidades de procesamiento electrónico de datos de las Naciones Unidas y sus organismos especializados y de la OIEA, y que fue presentado ante la Asamblea General[49], no se ha llevado a cabo ningún análisis dirigido a estudiar la evolución del CICE y examinar con espíritu crítico su capacidad y su potencial inherente para responder a las necesidades más actuales del sistema. Teniendo en cuenta los llamamientos formulados anteriormente por la DCI para que se señalaran posibles impedimentos a este respecto, y sin perjuicio de la aplicación de las recomendaciones formales que figuran en el presente informe, **los Inspectores consideran que en el futuro podría llevarse a cabo un análisis exhaustivo del CICE, en particular con el objeto de determinar las condiciones estructurales, financieras y administrativas que le permitirían materializar plenamente su potencial como asociado estratégico y como recurso para el sistema de las Naciones Unidas en su conjunto.** A los efectos del presente examen, una de las cuestiones que guiaron el análisis que los Inspectores realizaron del CICE, y en particular de su oferta de servicios de ciberseguridad, así como de su configuración y de su visión de su propio posicionamiento en este ámbito específico, fue si ya se daban las condiciones para que se convirtiera en un centro neurálgico de la ciberseguridad para todo el sistema de las Naciones Unidas, y en qué medida.

Mandato y modelo institucional

140. **Evolución del CICE de 1971 a 2021.** En virtud de la resolución 2741 (XXV) de la Asamblea General, el CICE se creó mediante un memorando de acuerdo celebrado en 1971 entre las Naciones Unidas, el PNUD y la OMS. Inicialmente concebido como un dispositivo interinstitucional encargado de prestar "servicios de procesamiento electrónico de datos" a sus tres miembros fundadores y otros usuarios, su catálogo de servicios y su cartera de clientes han evolucionado considerablemente desde la década de 1970. Conocido sobre todo por sus servicios de alojamiento y por la infraestructura compartida de TIC que proporciona en apoyo de los sistemas de gestión de recursos institucionales de muchos de sus clientes, el ámbito de actividad del CICE se ha ampliado a áreas tan diversas como la computación en la nube, la automatización robótica de procesos, la tecnología de cadenas de bloques, el desarrollo de *software*, la consultoría en TIC y la ciberseguridad. Asimismo, su cartera de clientes ha crecido considerablemente. Concebido desde su creación como un servicio al que se irían incorporando nuevos clientes, estos han pasado de las 3 organizaciones del sistema de las Naciones Unidas iniciales a las más de 25 con que contaba en 2003 y a los aproximadamente 70 clientes a los que daba servicio en 2021, entre los que se contaban entidades del sistema de las Naciones Unidas y sus organizaciones afiliadas, así como varias

[49] A/8072.

organizaciones intergubernamentales no afiliadas, organizaciones no gubernamentales internacionales e instituciones financieras internacionales. Su instrumento constitutivo se modificó en 2003 con el fin de dotarlo de una base jurídica más amplia y de normas de actuación más detalladas, para lo que se añadió un nuevo documento de "mandato" en que se concretaron y ampliaron las pocas disposiciones básicas que figuraban en el documento original. En dicho documento, aprobado por separado por cada una de las organizaciones asociadas a través del Comité de Gestión del CICE, se establecieron la estructura de gobernanza, el modelo institucional y las condiciones básicas de participación del CICE. Tal como se refleja en dicho documento, sus dos funciones principales son prestar servicios en el ámbito de las tecnologías de la información, tanto de tipo operacional como de formación, y tratar de ajustar la gama de servicios ofrecidos a las necesidades de sus organizaciones asociadas.

141. **Principios básicos del mandato y del modelo institucional del CICE.** Gracias a su mandato actualizado, el CICE reforzó el propósito original de su creación como proveedor de servicios a las organizaciones del sistema de las Naciones Unidas, vinculando estrechamente su oferta de servicios a la demanda concreta generada por sus clientes. Al mismo tiempo, la reformulación de sus funciones principales le permitió gozar del mayor margen posible a la hora de buscar nuevas líneas de trabajo que trascendieran el restringido ámbito del procesamiento de datos, dotándolo, entre otras cosas, de libertad para ofrecer servicios de ciberseguridad, pese a que en su mandato no figurase ninguna referencia explícita al respecto. Uno de los elementos en los que se insistió y que se desarrolló con más detalle en el nuevo documento fue la noción de infraestructura y servicios compartidos, cuyo objetivo era lograr economías de escala para los clientes del CICE. Este modelo, llamado "modelo de servicios compartidos", permite al Centro reducir los costos de cada servicio en proporción directa al número de clientes que se suscriban a él. En cambio, entre los elementos que han permanecido inalterados a lo largo de sus 50 años de existencia figuran: a) su modelo de recuperación de costos, que en la práctica requiere que todos sus productos sean prefinanciados por los clientes sobre la base de las necesidades establecidas y la aprobación colectiva, sin generar ningún excedente de ingresos ni margen presupuestario para actividades de investigación y desarrollo; b) el carácter voluntario de su catálogo de servicios, gracias al cual las organizaciones pueden decidir, para cada servicio, si hacen o no uso de él mediante el abono de una cuota; y c) su dependencia de una "organización anfitriona" (la OMS), a la que permanece adscrito en términos administrativos y jurídicos, por lo que hace uso de las instalaciones, la capacidad administrativa y el marco normativo que esta le proporciona para poder contratar, reclutar, consignar fondos y funcionar en términos prácticos.

142. **La complejidad de la estructura de gobernanza refleja la función de proveedor de servicios orientado al cliente.** A fin de que su catálogo se adecúe a los clientes a los que presta servicio, el CICE lo elabora en estrecha colaboración con representantes de sus organizaciones asociadas a través del Comité de Gestión del CICE. En este órgano, integrado por 41 miembros, no están representados todos los clientes del CICE, ya que, dentro de lo que se denomina conjuntamente "clientes", se distingue entre organizaciones asociadas y usuarios de los servicios[50]. Solo los primeros son miembros del Comité de Gestión con derecho de voto, por lo que participan en las decisiones sobre las líneas de servicio que el CICE debe desarrollar, mientras que los clientes que no son a la vez organizaciones asociadas (es decir, los meros "usuarios") únicamente pueden suscribirse a los servicios disponibles una vez desarrollados. Además, dado que se aplica un modelo de servicios por suscripción, no todos los miembros del Comité de Gestión tienen por qué ser clientes de los servicios de ciberseguridad, y viceversa (anexo VIII), lo que teóricamente podría conllevar el riesgo de que se viera obstaculizado el desarrollo o la mejora de los servicios para los que algunas organizaciones del sistema de las Naciones Unidas, pero no todas, pueden tener necesidades

[50] En virtud de la modificación de 2003 del memorando de acuerdo fundacional, el término "organización asociada" se refiere a toda organización del sistema de las Naciones Unidas que utilice los servicios del CICE y haya sido aceptada como organización asociada por el Comité de Gestión, mientras que el término "usuario" se refiere a los Gobiernos, organizaciones intergubernamentales que no sean organizaciones asociadas, organizaciones no gubernamentales y otras entidades gubernamentales que hayan sido autorizadas por la Dirección del CICE para utilizar sus servicios.

específicas. Por lo que respecta a los servicios de ciberseguridad en concreto, en 2020 se creó un grupo consultivo informal integrado por los tres principales financiadores de esos servicios —actualmente el PNUD, el ACNUR y la FAO— que se encarga de vigilar la calidad y la pertinencia de la oferta de servicios y de detectar nuevas oportunidades de desarrollo de soluciones compartidas. Dicho grupo cuenta con un canal de comunicación directa con el Jefe de Servicios de Ciberseguridad del CICE, aunque la decisión final sobre el desarrollo de un determinado servicio sigue correspondiendo al Comité de Gestión. En términos generales, se observó que la arquitectura de gobernanza del CICE tenía una notable complejidad, lo que reflejaba la naturaleza de su modelo institucional actual en varios niveles. La cuestión de si esa arquitectura, en su forma actual, podría asumir y desempeñar adecuadamente una función más destacada para el sistema, como se desprende de su mandato, sin necesidad de realizar ajustes importantes no encontró una respuesta fácil. En la sección D de este capítulo se analizan con más detalle algunas de las dificultades que presenta esta cuestión.

143. **Ventajas e inconvenientes del modelo institucional del CICE.** Una vez que se ha desarrollado un determinado servicio, todos los clientes que se suscriben a él abonan una cuota de uso fijada y revisada por el Comité de Gestión con carácter anual y que suele ajustarse a la baja para reflejar las economías de escala conforme disminuye el costo de ese servicio para todos los usuarios gracias a la suscripción de más clientes. En este sentido, el estricto modelo de recuperación de costos que ha regido el funcionamiento del CICE desde su creación presenta la ventaja de que garantiza un alto grado de transparencia en el cálculo de costos de los servicios, obliga a establecer una coordinación continua con los clientes y mantiene controlado el ámbito abarcado por la oferta de servicios al exigir que las necesidades reales y las soluciones que se desarrollan e implementan en respuesta a ellas se ajusten al máximo. Por consiguiente, puede excluirse casi por completo el interés comercial y lucrativo, que es uno de los aspectos que distinguen al Centro de otros proveedores. Al mismo tiempo, no se asigna un presupuesto específico a sufragar las funciones ejecutivas y administrativas básicas[51], lo que significa que esos costos deben repercutirse en las cuotas aplicadas a los servicios ofrecidos. El modelo institucional del CICE, que combina los principios de recuperación de costos y de servicios compartidos, ha demostrado ser tanto un factor facilitador como un obstáculo para llevar a la práctica la visión de esta entidad de convertirse en un centro neurálgico de la ciberseguridad para todo el sistema y ha generado una situación en la que su oferta de servicios depende de que los clientes aporten una financiación inicial para sufragar los costos de desarrollo de un nuevo servicio en respuesta a la demanda, mientras que muchos de ellos solo pueden permitirse adquirir ese mismo servicio una vez que haya sido desarrollado y se haya suscrito a él una masa crítica de clientes. Este funcionamiento puede crear una desventaja sistemática para los organismos con menos poder financiero, cuyas necesidades en materia de ciberseguridad pueden diferir de las de sus homólogos con mayor margen presupuestario para prefinanciar servicios concretos.

Catálogo de servicios de ciberseguridad

144. **El CICE, un actor clave en el panorama de la ciberseguridad de las Naciones Unidas.** En los últimos años, el CICE se ha consolidado como un interesado clave y un recurso en materia de ciberseguridad para el sistema de las Naciones Unidas. Como atestiguan muchos de sus clientes, ha acumulado unos conocimientos especializados y una capacidad considerables en materia de ciberseguridad y ha ampliado progresivamente su oferta hasta incluir 13 servicios especializados en ese ámbito, conocidos comúnmente bajo la marca Common Secure (gráfico IX y anexo VII). Dichos servicios abarcan tanto la gobernanza de la ciberseguridad como los aspectos operativos, y el CICE los ofrece en su calidad de: proveedor de alojamiento de infraestructura que también gestiona los aspectos de seguridad de los datos, los sistemas y las aplicaciones alojados; proveedor específico de servicios de ciberseguridad; asesor en cuestiones estratégicas y de gestión; o proveedor de respuestas prácticas a incidentes, según el tipo de servicios suscritos. La versatilidad de la oferta de servicios del CICE en el ámbito de la ciberseguridad refleja el hecho de que la

[51] Informe de la Dirección del CICE y estados financieros del bienio 2016-2017, publicados en abril de 2018, pág. 46.

demanda de esta línea de servicios ha experimentado un importante crecimiento entre sus clientes. Si bien los productos relacionados con la ciberseguridad representan solo una parte de su catálogo de servicios y apenas el 6,1 % de su volumen total de financiación (a fecha de enero de 2021), su cartera de clientes (actuales y pasados) para dichos productos comprende 45 organizaciones, de las cuales 21 son miembros de la JJE (de un total de 31) y 20 son organizaciones participantes en la DCI (de un total de 28). Pese a que alrededor de un tercio de las organizaciones, y entre ellas, muy particularmente, la Secretaría de las Naciones Unidas, no hacen uso de los servicios del CICE en materia de ciberseguridad, sería difícil dibujar el panorama actual de la ciberseguridad en el sistema de las Naciones Unidas sin tener en cuenta la función desempeñada y las contribuciones aportadas por el CICE.

Gráfico IX
Panorama de los servicios ofrecidos por el CICE en materia de ciberseguridad (2021)

Servicios	*Número de organizaciones participantes en la DCI (clientes pasados y actuales)*
Common Secure Threat Intelligence	17
Servicio común de firma electrónica	14
Respuesta a incidentes	11
Servicios de apoyo a la gobernanza y a los oficiales principales de seguridad de la información	11
Sensibilización sobre la seguridad de la información	10
Gestión de la vulnerabilidad	7
Pruebas de penetración	7
Servicios de simulación de *phishing*	6
Servicio de centro de operaciones de seguridad común	5
Evaluación de la seguridad en la nube	5
Infraestructura de clave pública común	3
Gestión de identidades y accesos	3
Información de seguridad y gestión de eventos Common Secure	1

145. **Common Secure Threat Intelligence, el servicio emblemático del CICE en materia de ciberseguridad.** De los 13 servicios que ofrece el CICE en materia de ciberseguridad, algunos ya han atraído a un número considerable de clientes de dentro y fuera del sistema de las Naciones Unidas, mientras otros todavía no se han forjado una cartera de clientes. Un servicio particularmente popular, que cuenta con 17 suscriptores entre las organizaciones participantes, es el Common Secure Threat Intelligence, que puede considerarse su servicio emblemático en materia de ciberseguridad y que demuestra día a día su utilidad. Este servicio, que ha sido valorado en términos netamente positivos por una clara mayoría de los clientes, responde a una necesidad colectiva formulada tiempo atrás y reiterada en repetidas ocasiones a nivel del sistema. Combina diversas fuentes internas y externas —tanto comerciales como gubernamentales— de información sobre amenazas, que el CICE analiza y filtra para elaborar paquetes de información digeribles y adaptados al entorno de las Naciones Unidas y a sus destinatarios. En un período extraordinario de sesiones celebrado en octubre de 2020 y dedicado a la ciberseguridad, el Comité de Gestión del CICE aprobó una resolución en la que se pedía a todas las organizaciones asociadas y clientes que compartieran con el equipo Common Secure la información de que dispusieran sobre amenazas e incidentes de seguridad, ya fuera de forma anonimizada o no, para que este la analizara y la difundiera a todo el sistema de las Naciones Unidas. Los Inspectores acogen con satisfacción esta decisión, si bien observan que, según la información recibida, aún no se ha aplicado de forma generalizada. La mayor parte de las organizaciones participantes encuestadas por la DCI consideraron que este ámbito era uno de los que más podían prestarse a una cooperación más estrecha a nivel de todo el sistema, y algunas señalaron que, además de compartir la información relativa a las amenazas y, en particular, los indicadores de

peligro, también podía tener utilidad intercambiar información sobre las medidas concretas de respuesta y recuperación adoptadas. Sin embargo, dicho aspecto obtuvo un apoyo desigual entre los expertos entrevistados por los Inspectores, principalmente por reparos relativos a la confidencialidad. No obstante, puede considerarse que el Common Secure Threat Intelligence es el más prometedor de los servicios ofrecidos en materia de ciberseguridad por su potencial para lograr de forma natural la suscripción de todo el sistema y mejorar la protección de forma efectiva, incluso superando lo alcanzado hasta el momento. Ese mismo potencial no puede atribuirse sin más al conjunto de la cartera de servicios de ciberseguridad del CICE.

146. **La evaluación de los servicios ofrecidos por el CICE en materia de ciberseguridad arroja resultados desiguales.** Pese al estrecho control que los clientes del CICE ejercen, en términos estructurales, sobre los servicios que se les ofrecen, las organizaciones participantes evaluaron de forma muy desigual su grado de satisfacción al respecto, que iba de "muy satisfactorio" a "muy insatisfactorio". Este hecho puede atribuirse a varios factores. Por un lado, entre las 20 organizaciones participantes que están o han estado suscritas a al menos uno de los servicios ofrecidos por el CICE en materia de ciberseguridad, hay cierta variación en cuanto al número de servicios solicitados y a cuáles de ellos han sido suscritos y, por lo tanto, evaluados como satisfactorios o insatisfactorios. La variación en la madurez del marco de ciberseguridad de las respectivas organizaciones también puede haber afectado al grado en que cada una de ellas ha sido capaz de absorber y aprovechar plenamente todos los aspectos del servicio ofrecido. Por otro lado, algunos de los servicios que ahora se ofrecen por separado antes estaban agrupados y se ofrecían en forma de paquete, lo que había suscitado algunas críticas debido al hecho de que las entidades se veían obligadas a suscribirse a partes del paquete que no necesitaban para poder disponer de otras que sí necesitaban o atraían su interés. Al parecer, el CICE abandonó esta práctica en 2019 y ahora ofrece a sus clientes total flexibilidad para elegir el nivel y el tipo de servicio que más les convenga. Por otra parte, en una evaluación básica de la satisfacción, la entidad puede estar transmitiendo una idea más general sobre la relación entablada con el CICE u otros aspectos de su experiencia, por lo que dicha evaluación tiene una fiabilidad limitada y carece de los matices necesarios para que puedan extraerse conclusiones definitivas. Teniendo en cuenta estas limitaciones y el hecho de que el objetivo de los Inspectores no era evaluar la eficacia de cada servicio ni del catálogo de servicios del CICE en su conjunto, no fue posible establecer una pauta clara en cuanto al tipo, el tamaño o la madurez de las organizaciones que expresaron más críticas o elogios a su labor. En términos generales, puede afirmarse que hay varias organizaciones, grandes y pequeñas, que han valorado muy positivamente la labor del CICE como proveedor de servicios de ciberseguridad, mientras que un número parecido ha adoptado una postura muy crítica con respecto a esa misma labor. En algunos casos, las críticas pueden reflejar deficiencias que han existido en el pasado, pero han sido subsanadas posteriormente, por lo que no deberían empañar el potencial presente y futuro del CICE como proveedor de servicios de ciberseguridad. No obstante, las reservas expresadas también podrían referirse al presente, seguir siendo pertinentes o incluso ser recurrentes a lo largo del tiempo, por lo que deberían tenerse muy en cuenta. En cualquier caso, la evaluación periódica y detallada del grado de satisfacción de los clientes puede proporcionar información valiosa sobre los aspectos en los que el CICE debería poner más atención con el objetivo de responder a las inquietudes de sus clientes actuales y atraer a otros en el futuro. Además, la evaluación global del CICE en su calidad de proveedor de servicios de ciberseguridad puede contribuir a ofrecer garantías más objetivas de la calidad general y la idoneidad de la línea de servicios que ofrece en esta esfera.

147. **Beneficios percibidos de suscribirse a los servicios del CICE.** Según han comunicado sus propios clientes, entre las razones que los llevan a requerir los servicios del CICE puede mencionarse el conocimiento exhaustivo que este tiene del sistema de las Naciones Unidas y de las necesidades de las organizaciones que lo integran, adquirido gracias a su larga experiencia en el desarrollo de servicios adaptados a ellas, al hecho de que está sujeto a sus mismas normas y estructuras administrativas y a su participación en los foros interinstitucionales pertinentes. Además, el CICE ha señalado varias ventajas comparativas que lo distinguen de los proveedores de servicios comerciales, como: la disminución progresiva del costo de sus servicios a medida que crece su cartera de clientes; el hecho de no tener ánimo de lucro y el consiguiente interés por mantener precios asequibles, también

para las organizaciones con menos recursos económicos que buscan opciones de bajo costo; el objetivo inherente y compartido de lograr que el sistema sea más seguro para todos, también para el propio Centro, que forma parte de él; y la capacidad de observar y adaptarse a sus clientes y de aprender de ellos de primera mano para aplicar las enseñanzas extraídas directamente en beneficio del colectivo. El CICE tiene una visión global del sistema en su conjunto y de todos los elementos que lo constituyen, lo que también lo distingue de los proveedores comerciales, que suelen ver solo partes del conjunto, lo que le permite aportar valor añadido más allá del contexto particular de cada cliente. Otro aspecto que los Inspectores consideraron interesante fue la idea de que, pese a la existencia de mecanismos interinstitucionales y del nivel adicional de gobernanza representativa que aportaba el Comité de Gestión del CICE, no había ninguna entidad que estuviera intrínsecamente motivada para trabajar por el interés colectivo del sistema, y no por el interés particular de cada uno de sus miembros o, en el mejor de los casos, la suma de intereses —a menudo irreconciliable— de todos ellos. En este sentido, el CICE se consideraba a sí mismo un proveedor neutral, apolítico y, dado su modelo de recuperación de costos, desinteresado de soluciones para todo el sistema, impulsado no por las preocupaciones ligadas a la escasez de recursos que podían guiar a los miembros de su Comité de Gestión y hacerlos caer en un posible conflicto de intereses, sino por la búsqueda del bien común.

148. **Deficiencias percibidas del CICE como proveedor de ciberseguridad.** Por el contrario, varias organizaciones hicieron una valoración menos elogiosa del CICE en su función de proveedor de servicios de ciberseguridad y criticaron, en concreto, la relación calidad-precio de sus servicios en comparación con la que podían ofrecer los proveedores comerciales. Algunas dijeron tener la percepción de que las empresas externas podían proporcionar conocimientos expertos y herramientas punteras a un nivel que superaba la capacidad que podían alcanzar el CICE o cualquier otra organización, incluso tras la realización de importantes inversiones. Estas impresiones contrastaban con la opinión de otros clientes, según los cuales el nivel de conocimientos especializados y de preparación en el ámbito cibernético del CICE había dado un auténtico salto en los últimos años, lo que venía corroborado por la realización de importantes inversiones por parte de sus dirigentes en la certificación y el cumplimiento de normas ISO, la contratación de un plantel diversificado de expertos y la creación de un centro de operaciones de seguridad compartido que funcionaba las 24 horas del día, con lo que se había ampliado su capacidad de vigilancia ininterrumpida y mejorado su catálogo de servicios. Sin embargo, los progresos alcanzados no pueden hacer pasar por alto el hecho de que persiste la percepción —quizá acertada— de que existe una brecha, que el CICE difícilmente puede subsanar, en cuanto a los conocimientos especializados y la relación calidad-precio. Además, se señaló que el sector privado ofrecía servicios similares a un precio más competitivo, y algunos encuestados opinaron que, pese a las economías de escala derivadas del modelo de servicios compartidos, el CICE aplicaba tarifas demasiado elevadas a algunos de sus servicios y era poco transparente al respecto, lo que hacía que, para algunos, esos servicios fueran inasequibles u opacos y, para otros, no se vieran suficientemente compensados por los beneficios obtenidos en otros ámbitos. De hecho, el CICE reconoció que competir con el sector privado estaba por encima de sus posibilidades y era incluso contraproducente en algunos aspectos. Teniendo en cuenta su modelo institucional, el costo de sus servicios se reduciría de forma generalizada si lograba tener más clientes, mientras que el costo era precisamente, en muchos casos, el primer obstáculo a que se enfrentaban las organizaciones que deseaban contratar esos mismos servicios. Esta paradoja podría superarse en parte, por ejemplo, inyectando fondos asignados de forma menos estricta en los ámbitos adecuados para permitir al Centro reducir algunas de sus tarifas, posiblemente por debajo de las aplicadas por los proveedores del sector privado, sin verse obligado a tratar de reemplazarlas por completo. Si bien no tiene sentido competir con el sector privado en ámbitos en los que este aporta más valor añadido y es más eficiente, los jefes ejecutivos deberían plantearse si el CICE podría actuar como interfaz entre los proveedores comerciales y sus clientes del sistema de las Naciones Unidas con el fin de reducir las tarifas y lograr economías de escala y, en última instancia, capacidad de negociación. Además, junto con la evaluación independiente de sus servicios de ciberseguridad, ya sugerida en el presente informe, el CICE tal vez desee realizar un análisis crítico de su catálogo de servicios en materia de ciberseguridad con el objeto de distinguir mejor aquellos en los que pueda tener una ventaja comparativa y considerar la posibilidad de dedicar más esfuerzos a esos ámbitos. Por último, los Inspectores observaron que, pese a las

críticas —en ocasiones duras— que el CICE recibía en su función de proveedor de servicios de ciberseguridad, el sistema hacía uso de su oferta.

149. **Oportunidades de mejora en el marco de los límites actuales del mandato del CICE.** Si bien algunas organizaciones han abogado por un fortalecimiento formal de la posición del CICE como proveedor de servicios de ciberseguridad para el sistema de las Naciones Unidas, los Inspectores creen que se puede avanzar en muchos aspectos en el marco de su mandato actual, revisado en 2003, que ya proporciona una base sólida para la aplicación de soluciones que podrían materializarse con un poco más de compromiso de todos los interesados. Aun así, en el caso de que hubiera razones que obligaran a modificar el mandato del CICE, dicha modificación sería competencia colectiva de las organizaciones fundadoras y las entidades que se adhirieron a la enmienda de su instrumento constitutivo en 2003, y no sería necesario que la Asamblea General adoptara medidas hasta que se hubiera llevado a cabo un análisis más profundo del CICE como entidad, de los avances logrados hasta la fecha y de los posibles factores estructurales causantes de que su potencial no haya sido aún aprovechado y que podrían subsanarse gracias a esas medidas. En opinión de los Inspectores, y tal como se expone a continuación, un aspecto fundamental que debería abordarse sin demora ni más condiciones previas es el de analizar a fondo la desconexión existente entre las estructuras y los mecanismos actuales, así como algunas limitaciones del modelo de financiación, a fin de ponerles remedio.

D. Mejora de los vínculos entre la dirección estratégica a nivel de todo el sistema y la capacidad operativa

Poner remedio a la desconexión institucional existente entre el Grupo de Interés Especial sobre la Seguridad de la Información y el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas

150. **Limitaciones formales de la relación entre el Grupo de Interés Especial sobre la Seguridad de la Información y el CICE.** Dado el considerable solapamiento existente entre las organizaciones representadas en los mecanismos de coordinación interinstitucional, por un lado, y el Comité de Gestión del CICE, por el otro (anexo VIII), cabría suponer que el Grupo de Interés Especial sobre la Seguridad de la Información es el órgano que proporciona orientación y dirección estratégicas sobre las soluciones de ciberseguridad compartidas que podrían resultar adecuadas para las organizaciones que integran el sistema de las Naciones Unidas, mientras que el CICE actúa como órgano operativo de ejecución del sistema. Sin embargo, estas dos entidades no cuentan con ningún vínculo formal ni operan conjuntamente en la práctica. Desde el punto de vista formal, el Grupo de Interés Especial sobre la Seguridad de la Información ejerce una mera función de coordinación e intercambio de información y no tiene potestad para dar instrucciones de ningún tipo al CICE, mientras que este ejecuta las decisiones de su propio Comité de Gestión en relación con los servicios que debe desarrollar para sus asociados y clientes, entre los que no figuran todas las organizaciones del sistema de las Naciones Unidas. En la práctica, es posible que la desconexión institucional entre ambos órganos no sea el factor decisivo, pero también es probable que haya contribuido a que se establezca una dinámica que puede estar privando al sistema de ganar en eficiencia debido a que se desaprovechan oportunidades para una colaboración más directa.

151. **Relaciones tensas en la práctica debido a varios factores.** El CICE ha obtenido la condición de observador dentro del Grupo de Interés Especial sobre la Seguridad de la Información y participa en las deliberaciones de este último sin gozar de derecho de voto ni poder presentar temas para debate. Sin embargo, el propio CICE afirmó que en la práctica se le había negado la posibilidad de promocionar su catálogo de servicios y de solicitar opiniones directas sobre sus soluciones en el foro del Grupo de Interés Especial sobre la Seguridad de la Información. Esta postura puede explicarse, en parte, por la propia naturaleza del CICE, que es un dispositivo interinstitucional y no propiamente una entidad cuyo estatus podría conferirle la condición de miembro de la JJE y, por lo tanto, plenos derechos de participación. También se mencionó que existía la percepción tácita de que el CICE no era un asociado para las organizaciones del sistema, sino básicamente un proveedor, lo que dificultaba aún más su plena integración en los mecanismos interinstitucionales existentes. Teniendo en cuenta su funcionamiento orientado al cliente y su función de suministrar

servicios de computación adaptados a sus organizaciones asociadas, difícilmente puede negarse que la percepción de que se trata de un proveedor está hasta cierto punto justificada. Al mismo tiempo, el CICE se presenta abiertamente como una entidad de las Naciones Unidas y Miembro de pleno derecho del sistema de las Naciones Unidas. De hecho, sus dirigentes han manifestado su voluntad de convertirlo en un centro neurálgico de la ciberseguridad para todo el sistema de las Naciones Unidas si se les brinda la oportunidad para ello, y algunas organizaciones han opinado incluso que debería centrar su actividad en la ciberseguridad. Sin embargo, hasta que no se analicen y resuelvan las dificultades ligadas a las dinámicas establecidas entre los mecanismos interinstitucionales del sistema y el CICE en su calidad de proveedor privilegiado de servicios de ciberseguridad con capacidad para asumir la función de órgano operativo del sistema en este ámbito, es probable que esta posibilidad quede relegada al terreno de lo irrealizable.

152. **Estructuras paralelas *de facto*.** Un ejemplo que ilustra el modo en que la dinámica establecida entre el mecanismo interinstitucional y el CICE ha dado lugar a la adopción espontánea de soluciones a las necesidades detectadas, pero al mismo tiempo ha generado duplicidades en la esfera de la ciberseguridad, es el caso de la Conferencia Common Secure, organizada por el CICE. Desde 2019, la Conferencia ha proporcionado a los clientes de los servicios de ciberseguridad del CICE un canal para intercambiar información sobre asuntos de interés común a nivel operacional y para transmitir sus opiniones sobre los servicios prestados, y se ha convertido en un evento periódico reputado en el calendario de la ciberseguridad, que cosecha muchos elogios de los asistentes, muchos de los cuales son organizaciones del sistema de las Naciones Unidas que también están representadas en el Grupo de Interés Especial sobre la Seguridad de la Información. En cierto sentido, puede decirse que la Conferencia Common Secure ha venido a colmar un vacío para el CICE, que trataba de comunicarse directamente con las organizaciones a través del Grupo de Interés Especial sobre la Seguridad de la Información, pero no podía hacerlo con el grado de productividad y concreción que hubiera deseado para lograr el objetivo de mejorar su asociación con el sistema y los aspectos operativos de su oferta de servicios. Algunos pueden llegar a afirmar que la Conferencia se ha convertido *de facto* en el principal foro para gran parte del sistema como consecuencia directa de la incapacidad del mecanismo de coordinación existente del Grupo de Interés Especial sobre la Seguridad de la Información para poner en práctica un debate más orientado a las soluciones. El inconveniente de esta iniciativa, por otro lado proactiva e innovadora, es que la Conferencia puede haber desviado algunos debates que podrían haberse llevado a cabo perfectamente en el marco del Grupo de Interés Especial sobre la Seguridad de la Información a otro foro, en teoría abierto principalmente a los clientes del CICE y no al sistema en su conjunto. La existencia de estas dos estructuras, más paralelas que complementarias y con fines muy similares, una bajo los auspicios de la JJE y la otra bajo los del CICE, conlleva el riesgo de profundizar la desconexión y exacerbar la competencia, lo que se traduciría en ineficacia, duplicaciones y solapamientos. Este es uno de los efectos colaterales perjudiciales de la gestión insatisfactoria de la dinámica establecida entre ambas entidades.

153. **Se necesitan más sinergias.** Estas observaciones deberían guiar la adopción de medidas por ambas entidades para tratar de mejorar la forma en que se relacionan entre sí. Por un lado, el Grupo de Interés Especial sobre la Seguridad de la Información, como colectivo, debería intensificar sus esfuerzos por cumplir su mandato en un sentido más estratégico, identificando los ámbitos que se presten a la adopción de soluciones compartidas, si no para el sistema en su conjunto, sí al menos para grupos de organizaciones cuya mejora de la posición de ciberseguridad mejoraría a su vez la del sistema. De no hacerlo, es probable que el CICE, haciendo uso de la voz autorizada que ostenta en nombre del sistema, se vea empujado a dar un paso adelante para ocupar ese espacio, aunque siempre de forma restringida al círculo de sus clientes. Al mismo tiempo, el hecho de que el CICE aprovechara la oportunidad que supondría que el Grupo de Interés Especial sobre la Seguridad de la Información creara inadvertidamente un vacío sería, en principio, beneficioso para el sistema, dado que podría suponer una innovación, pero algo así no debería ocurrir a espaldas del órgano oficial encargado de la coordinación y la cooperación en materia de ciberseguridad en todo el sistema. Ambas entidades tienen la responsabilidad de buscar formas de mejorar las dinámicas que se establecen entre ellas con espíritu proactivo, adoptando medidas formales o informales. De hecho, hay varios servicios de ciberseguridad del CICE bastante

solicitados que se considera que se han inspirado o han emanado directamente de los diálogos celebrados en el marco del Grupo de Interés Especial sobre la Seguridad de la Información, aun sin haber sido explícitamente encomendados por este último en un sentido formal. El CICE, particularmente si mantiene su propósito de seguir trabajando para convertirse en un centro neurálgico de la ciberseguridad para todo el sistema, y no solo para sus clientes, no puede permitirse permanecer desvinculado de la comunidad de expertos que representa las necesidades colectivas de las organizaciones a las que dicho centro neurálgico serviría. Además, como colectivo, el Grupo de Interés Especial sobre la Seguridad de la Información tiene, en parte, la clave para facilitar una colaboración más constructiva en este sentido. La posibilidad de establecer sinergias y una mayor complementariedad existe, pero hasta ahora no se ha aprovechado en todo su potencial.

154. **Las organizaciones participantes deberían volver a plantearse la posibilidad de utilizar los servicios de ciberseguridad del CICE.** Para solucionar la desconexión existente entre ambas entidades, algunos han propuesto que la utilización de los servicios de ciberseguridad del CICE sea obligatoria para las organizaciones del sistema de las Naciones Unidas. Se ha argumentado que esto, además, aceleraría las posibles ganancias de eficiencia y la reducción de los costos al reforzar el alcance y la difusión de la labor del CICE como proveedor de servicios compartidos. No todo el mundo coincide con esta visión, que, de hecho, puede resultar contraproducente. Por un lado, dicha medida despojaría de autonomía a las organizaciones del sistema de las Naciones Unidas para evaluar la oferta de servicios y decidir cuáles se adaptan mejor a sus necesidades, al instaurar e imponer externamente un monopolio artificial tanto del proveedor como de la oferta de servicios. Por otro, dentro del CICE existen mecanismos de gobernanza que ya permiten el establecimiento de un diálogo fructífero entre su dirección ejecutiva y sus clientes acerca de la configuración de los servicios de ciberseguridad. Los Inspectores consideran que no es prudente ni necesario interferir en estos mecanismos. **Sin embargo, ya en 2019 los Inspectores alentaron a las organizaciones del sistema de las Naciones Unidas y al CICE a encontrar más esferas de cooperación para complementar las capacidades existentes de las organizaciones mediante un mayor número de servicios compartidos**[52]. En particular, los Inspectores creen que puede resultar útil que las organizaciones vuelvan a examinar algunas de las razones que en el pasado les han llevado a darse de baja de los servicios de ciberseguridad ofrecidos por el CICE o a no suscribirse a ellos. Dicha decisión deberá ser matizada y pasar idealmente por la evaluación o reevaluación de cada uno de los servicios de ciberseguridad ofrecidos. De hecho, es posible que algunos de los servicios aún no hayan alcanzado el nivel de madurez necesario o no respondan en grado suficiente a las necesidades de las organizaciones para que todos los miembros del sistema decidan suscribirse a ellos. Corresponde al CICE proseguir los esfuerzos destinados a subsanar cualquier deficiencia en este ámbito. Además, los Inspectores reconocen la individualidad de cada organización. En última instancia, son ellas quienes detentan la responsabilidad de tomar las decisiones pertinentes en función de sus necesidades específicas, en particular teniendo en cuenta la diversidad de sistemas de información, aplicaciones y otras disposiciones técnicas que se hayan establecido internamente o en el marco de arreglos contractuales con proveedores externos.

Contribuciones voluntarias de los donantes para complementar la financiación de soluciones compartidas para el sistema

155. **Las contribuciones voluntarias como medio de apoyo directo.** En opinión de los Inspectores, resulta oportuno considerar la posibilidad de aprovechar las contribuciones voluntarias como mecanismo de financiación complementario con el objeto de destinar recursos más directos a salvaguardar la posición global de ciberseguridad de todo el sistema. Disponer de contribuciones voluntarias específicamente destinadas a la adopción de medidas para el sistema en su conjunto podría eliminar algunos de los impedimentos que dificultan la puesta en práctica de soluciones de ciberseguridad compartidas, puesto que es probable que la escasez de recursos de las organizaciones participantes haya afectado a su disposición a contribuir a un fondo común. Poner a disposición del sistema la posibilidad de recurrir a una fuente de contribuciones de donantes que sea independiente del presupuesto de cada uno de

[52] JIU/REP/2019/5.

sus miembros puede aliviar parte de la presión a la que este se ve sometido, por un lado, por el escaso margen de maniobra de dichos presupuestos, en los que un gran número de prioridades institucionales compiten por unos fondos cada vez más escasos, y, por otro, a causa del modelo de recuperación de costos por el que se rige el CICE. En el caso del CICE, dicha medida le permitiría desarrollar líneas de servicios innovadoras para sus organizaciones asociadas, particularmente las que cuentan con menor capacidad interna o disponen de menos recursos para establecer disposiciones de ciberseguridad en general. En combinación con su modelo de servicios compartidos, un enfoque de este tipo contribuiría a mejorar la relación costo-eficacia, gracias a que las tarifas aplicadas por los servicios se mantendrían bajas, y probablemente atraería a más clientes, con lo que se multiplicarían los efectos positivos. Una de las cuestiones que los Inspectores se plantearon en sus consultas con los interlocutores pertinentes fue si sería mejor situar al mecanismo encargado de recaudar y emplear esas contribuciones voluntarias bajo la autoridad directa del sistema como colectivo, por ejemplo estableciéndolo en forma de fondo fiduciario que estaría administrado por la secretaría de la JJE y recibiría las aportaciones sustantivas del Grupo de Interés Especial sobre la Seguridad de la Información, o bien bajo la del CICE en su condición de proveedor establecido *de facto* de muchas soluciones compartidas para el sistema. Tras examinar varias opciones, los Inspectores llegaron a la conclusión de que lo más conveniente sería que dicho fondo estuviera administrado por la entidad que debería tener una visibilidad operacional continua sobre los gastos al desarrollar los servicios deseados, es decir, el CICE.

156. **Fondo fiduciario de ciberseguridad.** En esencia, desde su modificación en 2003, el mandato del CICE incluye disposiciones que le permiten recaudar contribuciones voluntarias, y de hecho recientemente ya se ha dado el caso de un proyecto concreto que se financió por esta vía. El empleo estratégico de este mecanismo, no suficientemente aprovechado hasta el momento, para el diseño proactivo de servicios destinados a ser compartidos entre todas o varias de las organizaciones del sistema de las Naciones Unidas podría marcar un punto de inflexión. Dar a conocer más ampliamente esta posibilidad y definir mejor las condiciones en las que puede darse brindaría una oportunidad a los Estados Miembros que deseen contribuir directamente a la mejora de la ciberseguridad en el conjunto del sistema en las condiciones aplicables a la respectiva contribución destinada al apoyo específico de soluciones de ciberseguridad compartidas. También facilitaría la aplicación de la recomendación formulada por la DCI en 2019 de que se estableciera un mecanismo de financiación que permitiera al CICE llevar a cabo actividades de investigación y desarrollo sin constreñirse a las limitaciones impuestas por su modelo de recuperación de costos, lo que redundaría en un beneficio adicional para las organizaciones del sistema de las Naciones Unidas que figurasen entre sus clientes. Por consiguiente, los Inspectores recomiendan que, tras celebrar las consultas pertinentes, la Dirección del CICE establezca un fondo fiduciario de ciberseguridad destinado específicamente al diseño y el desarrollo de los servicios de ciberseguridad compartidos que más necesite el sistema. Para distinguir más claramente este mecanismo de otras fuentes de financiación proporcionada al Centro por sus organizaciones asociadas y clientes, lo más prudente sería crear un fondo fiduciario específico, sujeto a condiciones especiales para que su gobernanza no reproduzca sesgos estructurales ya existentes, posibles conflictos de intereses o dinámicas poco útiles dimanantes de las composiciones, distintas pero solapadas, de su Comité de Gestión y de los órganos interinstitucionales pertinentes de todo el sistema.

157. **Puesta en marcha del fondo fiduciario.** Por todo ello, el mandato de dicho mecanismo de financiación sería esencial para su buen funcionamiento. En él deberían establecerse claramente las funciones y responsabilidades de los diferentes interesados, los tipos de servicios que el fondo debería financiar y los procedimientos que deberían seguirse para que los fondos se asignasen con transparencia, entre otras cosas imponiendo la obligación de presentar informes al respecto. Más en concreto, el fondo debería estructurarse de modo que se utilice principalmente con el propósito de obtener resultados tangibles para las organizaciones del sistema. El objetivo principal del fondo podría ser financiar actividades de investigación y desarrollo encaminadas a poner en marcha servicios de ciberseguridad para los que exista un claro interés entre las organizaciones, pero que en un primer momento no cuenten con una masa crítica de usuarios dispuestos a compartir la financiación inicial necesaria. También podría emplearse para ampliar el alcance o la exhaustividad de los servicios ya existentes que cuenten con una clara demanda y requieran

financiación inicial, o cuyo costo convendría reducir para facilitar que otras organizaciones se suscribieran a ellos cuanto antes. Si bien en términos generales el fondo fiduciario estaría sujeto a las normas y reglamentos financieros de la OMS, por los que se rige el funcionamiento del CICE, existe la oportunidad de incorporar a su gobernanza un elemento de consulta con los órganos interinstitucionales competentes, lo que ayudaría a diseñar soluciones compartidas desarrolladas para el sistema en su conjunto, y no solo para los clientes del CICE, con lo que se mejoraría aún más la utilización de los recursos disponibles. Se invita a la Asamblea General, que fue quien puso los fundamentos para la creación del CICE, a que tome nota de la recomendación de establecer el fondo fiduciario de ciberseguridad e invite a los Estados Miembros a que le hagan contribuciones.

158. Se espera que la aplicación de las recomendaciones que figuran a continuación mejore la coordinación y la cooperación entre las organizaciones del sistema de las Naciones Unidas.

Recomendación 3

La Dirección del Centro Internacional de Cálculos Electrónicos debería tratar de establecer, a más tardar a finales de 2022, un fondo fiduciario que recogería las contribuciones de los donantes con el fin de complementar la capacidad del CICE para diseñar, desarrollar y ofrecer servicios y soluciones compartidos que mejoren la posición de ciberseguridad de las organizaciones del sistema de las Naciones Unidas.

Recomendación 4

La Asamblea General de las Naciones Unidas debería, a más tardar en su septuagésimo séptimo período de sesiones, tomar nota de la recomendación dirigida a la Dirección del Centro Internacional de Cálculos Electrónicos de establecer un fondo fiduciario destinado al desarrollo de soluciones compartidas de ciberseguridad e invitar a los Estados Miembros que deseen reforzar la posición de ciberseguridad de las organizaciones del sistema de las Naciones Unidas a que contribuyan a dicho fondo.

E. Oportunidades para una mayor armonización entre la seguridad física y la ciberseguridad

159. **La ciberseguridad no está contemplada en el sistema de gestión de la seguridad de las Naciones Unidas.** En su resolución 59/276, la Asamblea General creó el Departamento de Seguridad con el mandato de establecer a nivel de todo el sistema una política y un marco para la rendición de cuentas, así como normas y procedimientos operacionales para garantizar la seguridad y la protección del personal y los activos de las Naciones Unidas. Tal vez no resulte sorprendente que, en el mandato encomendado al Departamento de Seguridad en 2004, con anterioridad a los importantes avances que se producirían en 2013 y 2014 en todo el sistema en el ámbito de la ciberseguridad, no figurara ninguna referencia explícita a la ciberseguridad ni a la protección de los datos y activos digitales y del entorno cibernético en general[53]. Si bien el Departamento de Seguridad indicó que las orientaciones en materia de seguridad de la información eran aplicables a todo el sistema, el sistema de gestión de la seguridad de las Naciones Unidas y sus documentos de políticas aún no habían establecido los puntos de convergencia entre los ámbitos de la seguridad física y de la ciberseguridad a fin de fijar las responsabilidades de las distintas partes interesadas del sistema en esta esfera. Los Inspectores celebran que en el manual de políticas de seguridad del sistema de gestión de la seguridad de las Naciones Unidas se haya reservado espacio para un epígrafe titulado “Seguridad de la información: sensibilidad, clasificación y tratamiento”, lo que consideran un indicio de que existe cierto reconocimiento de que las consideraciones de ciberseguridad son importantes para la función de seguridad y

[53] El Departamento de Seguridad indicó que las categorías específicas de riesgos de seguridad de las que se ocupaban el Departamento y el sistema de gestión de la seguridad de las Naciones Unidas eran los disturbios civiles, los conflictos armados, el terrorismo, los delitos y los peligros (no deliberados).

protección física. No obstante, el contenido de dicho epígrafe está aún "por desarrollar" y el Departamento de Seguridad ha expresado sus reservas sobre la necesidad de dedicar una sección específica a dicho tema en este momento. Entretanto, según ha confirmado la Oficina de Asuntos Jurídicos y en contra de la interpretación establecida, según la cual las referencias jurídicas a la protección de los bienes y activos en las convenciones pertinentes y los acuerdos con los países anfitriones abarcan los activos y las comunicaciones digitales, no puede afirmarse que hoy en día ni el mandato ni el marco de políticas asociado que rigen la función de seguridad y protección física en el sistema de las Naciones Unidas contemplen la ciberseguridad.

160. **La Red Interinstitucional de Gestión de la Seguridad y el Grupo de Interés Especial sobre la Seguridad de la Información.** En el mandato de la Red Interinstitucional de Gestión de la Seguridad, que presta apoyo al Comité de Alto Nivel sobre Gestión en su examen exhaustivo de las políticas y cuestiones relacionadas con los recursos en relación con el sistema de gestión de la seguridad de las Naciones Unidas y realiza un seguimiento de la aplicación de las políticas, prácticas y procedimientos de gestión de la seguridad por todos los agentes del sistema de las Naciones Unidas, tampoco figura ninguna referencia específica a la ciberseguridad. La investigación llevada a cabo por la DCI confirmó que la Red Interinstitucional de Gestión de la Seguridad ha abordado esta cuestión en contadas ocasiones, y lo ha hecho mayoritariamente desde la perspectiva del uso de las TIC para mejorar los procesos generales de seguridad física, entre otros ámbitos en el de la gestión de la identidad y el acceso (por ejemplo, estudiando la posibilidad de utilizar tarjetas de acceso por identificación biométrica para la entrada tanto a las instalaciones físicas como al espacio digital) o el de los procedimientos de certificación asistidos por TIC para la expedición de autorizaciones de seguridad para viajar. Más recientemente, una recomendación formulada por el Grupo de Interés Especial sobre la Seguridad de la Información relativa al establecimiento de mecanismos de coordinación entre el Grupo y la Red Interinstitucional de Gestión de la Seguridad "en cuestiones de interés mutuo" fue aprobada por la Red Digital y Tecnológica en 2019[54]. Sin embargo, los Inspectores no encontraron indicios de que dicha intención se hubiera materializado más allá del contexto de proyectos concretos. Se invita a los mecanismos interinstitucionales pertinentes a seguir explorando las posibles modalidades prácticas de establecimiento de un canal de comunicación más regular con el fin de intensificar la colaboración. A este respecto, se sugirió a los Inspectores que la participación de las Presidencias de la Red y del Grupo en las reuniones de ambas entidades podría facilitar el intercambio de lecciones aprendidas.

161. **Un modelo de colaboración con las autoridades nacionales en materia de incidentes cibernéticos.** Un ámbito en el que los procedimientos establecidos para la seguridad y la protección físicas pueden inspirar los que se apliquen al ciberespacio es la comunicación con las autoridades nacionales en relación con los ciberataques. En el capítulo II (párrs. 35 a 37) del presente examen, los Inspectores han tratado con cierto detalle el complejo proceso interno que conlleva adoptar la decisión de ponerse en contacto con las autoridades nacionales, sin entrar en el planteamiento de qué ocurre una vez tomada dicha decisión y cómo se establece la comunicación con el interlocutor gubernamental que corresponda. La cuestión dista mucho de ser sencilla, ya que el interlocutor más adecuado a nivel nacional puede variar entre el ministerio competente bajo cuya responsabilidad actúan los equipos nacionales de respuesta (o preparación) ante emergencias informáticas, también llamados equipos de respuesta a incidentes de ciberseguridad (por ejemplo, el correspondiente ministerio del interior, de defensa, de comunicación o de tecnología, en función de las respectivas competencias) y las capacidades paralelas que puedan existir en ese mismo Estado bajo la responsabilidad de la agencia nacional de inteligencia con el mandato de luchar contra los ciberataques con una posible dimensión política. Por consiguiente, es posible que en el país no exista necesariamente un coordinador central que se encargue de recibir formalmente los informes pertinentes de las organizaciones del sistema de las Naciones Unidas, lo que puede complicar la canalización adecuada de la información. A modo de orientación en la gestión de las crisis relacionadas con la seguridad física, en el manual de políticas de seguridad del sistema de gestión de la seguridad de las Naciones Unidas se establece que los funcionarios designados "solicitarán al Gobierno del país

[54] CEB/2019/HLCM/DTN/02 y CEB/2019/HLCM/DTN/07, págs. 4 y 5.

anfitrión que designe coordinadores con autoridad para movilizar y coordinar el apoyo cuando una crisis afecte a las Naciones Unidas en el país"[55]. Podría estudiarse la adopción de un enfoque análogo como modelo para hacer frente a los incidentes cibernéticos, reconociendo al mismo tiempo que los funcionarios designados podrían aprovechar el asesoramiento experto del área de ciberseguridad de su organización en este ámbito.

162. **Falta de un mecanismo para transmitir, recibir y canalizar la información relacionada con la ciberseguridad dentro del sistema.** Análogamente, deberían existir arreglos internos que permitieran recibir la información procedente de los Gobiernos relacionada con la ciberseguridad, pero los Inspectores no lograron distinguirlos durante su examen. Algunos de los entrevistados dieron a entender que existía cierta confusión entre los interlocutores gubernamentales con respecto a la organización con la que debían ponerse en contacto en caso de que en un ciberataque detectado a nivel nacional se observara un vínculo con una o varias organizaciones del sistema de las Naciones Unidas, y con respecto al canal de comunicación que había que utilizar. Se mencionó que dicha información solía estar disponible y era susceptible de ser comunicada, pero que no existía ningún mecanismo que permitiera transmitirla y canalizarla con fiabilidad a los destinatarios adecuados dentro del sistema, principalmente porque las entidades externas no tenían una idea clara de a qué Miembro del sistema de las Naciones Unidas debía llegar la información en cuestión. Según se expuso, esto a su vez había hecho que en el pasado se perdieran ocasiones de proteger y defender los activos de las organizaciones contra los ataques, ya que no se había podido garantizar que la información de ciberseguridad llegara a un destinatario con los conocimientos especializados necesarios para traducirla en medidas concretas. Por consiguiente, los canales diplomáticos de comunicación establecidos no se consideraban suficientemente eficaces, lo que hacía que se dejaran perder posibles ganancias en ciberseguridad para las organizaciones individuales y para el sistema en su conjunto.

163. **Conveniencia e idoneidad de adoptar un enfoque armonizado.** En los párrafos 35 a 37 se han expuesto algunos de los factores que hacen que la práctica actual entre las organizaciones del sistema de las Naciones Unidas en materia de cooperación con las autoridades nacionales no sea homogénea. Algunos se plantean si las incoherencias que se derivan de este hecho pueden generar problemas adicionales, como posibles riesgos para la reputación en la gestión de las relaciones con el país anfitrión, en especial en los casos en que varias organizaciones de las Naciones Unidas con enfoques divergentes en la materia tienen su sede o mantienen una presencia en el mismo país y tratan —o no— las cuestiones relativas a la ciberseguridad con las mismas autoridades. **Los Inspectores solicitan al Comité de Alto Nivel sobre Gestión que se lleve a cabo una reflexión colectiva sobre la conveniencia e idoneidad de aplicar un enfoque armonizado a dicha cooperación y a la elaboración de las correspondientes orientaciones al respecto.** El Grupo de Interés Especial sobre la Seguridad de la Información, la Red Interinstitucional de Gestión de la Seguridad y la Red de Asesores Jurídicos están en buena posición para aportar sus respectivos conocimientos especializados a un examen conjunto de la cuestión y estudiar las posibles ganancias en materia de seguridad, las dificultades asociadas y, en particular, la viabilidad de designar coordinadores institucionales, también a nivel del sistema, que se encarguen de transmitir, recibir y canalizar la información relativa a las amenazas y los riesgos en el ámbito cibernético. Teniendo en cuenta que el CICE participa en la Red Interinstitucional de Gestión de la Seguridad, los Inspectores observaron que el propio CICE había expresado su disposición a desempeñar una función en la consolidación de información relativa a incidentes de ciberseguridad y su comunicación a las autoridades nacionales en nombre de las organizaciones del sistema de las Naciones Unidas si dicha función le era encomendada formalmente. Si bien la comunicación de información y la cooperación con las autoridades nacionales es potestad de cada organización, el hecho de que el CICE tenga acceso a información que le permite detectar conexiones y posibles interdependencias entre ataques lanzados contra distintas organizaciones —datos a los que muy posiblemente ninguna de esas organizaciones tenga acceso por sí sola— es un argumento a favor de que desempeñe un papel más importante en este ámbito, por lo que debería estudiarse dicha posibilidad. Por

[55] *The United Nations Security Management System Security Policy Manual*, secc. D, "Relations with host countries on security issues" (Relaciones con los países anfitriones en materia de seguridad), párr. 14 d), "Crisis management" (Gestión de crisis).

ello, al considerar la posibilidad de adoptar un enfoque armonizado en esta esfera, los mecanismos interinstitucionales competentes deberían también acoger y estudiar las posibles contribuciones de los interesados pertinentes, como el CICE, en particular en lo que se refiere a la capacidad de este último para reunir, correlacionar y analizar las pruebas forenses de los ataques cibernéticos en nombre del sistema.

164. **Hacia una mayor armonización entre la seguridad física y la ciberseguridad.** En términos más generales, y dado que en las directrices relativas a la seguridad de la información elaboradas en 1992 por la entidad predecesora de la Red Digital y Tecnológica ya se mencionaban los vínculos existentes entre la seguridad de los sistemas de información y la seguridad física[56] y que dicha cuestión volvió a plantearse en los debates mantenidos por los órganos competentes en 2013 y 2014[57], los Inspectores consideran que sería oportuno reavivar los esfuerzos dirigidos a establecer una mayor armonización entre las funciones de seguridad física y de ciberseguridad a fin de lograr el mayor grado de protección posible contra las amenazas complejas. En su calidad de autoridad central y entidad normativa de todo el sistema, el Departamento de Seguridad debe desempeñar una función primordial en el reconocimiento de los puntos de convergencia existentes y puede contribuir de forma crucial a operar un cambio fundamental en la cultura institucional. En efecto, en el sistema de las Naciones Unidas las amenazas a la seguridad física ya se consideran una cuestión de extrema gravedad y nadie duda de la necesidad de hacerles frente con rapidez y eficacia. Si bien los Inspectores detectaron una prudente evolución de la mentalidad institucional en lo que respecta a conceder esa misma urgencia a la lucha de las organizaciones contra las ciberamenazas, es necesario invertir más esfuerzos para que el enfoque basado en los riesgos y la respuesta estructurada y centrada en la rendición de cuentas que ya aplica el Departamento de Seguridad se extienda del ámbito puramente físico al ciberespacio. Esto no significa necesariamente que el mandato encomendado al Departamento de Seguridad para todo el sistema deba ser revisado para que contemple la ciberseguridad. Los Inspectores reconocen que hacer frente al reto que plantean modernamente las ciberamenazas exige recursos y conocimientos especializados con los que el Departamento de Seguridad no cuenta en la actualidad, y que no es posible transferir siquiera una parte de la responsabilidad en esa materia sin realizar ajustes importantes. Cualquier movimiento en esa dirección exigiría cambios estructurales que implicarían, entre otras cosas, la adopción de medidas por parte de la Asamblea General y amplias consultas internas con los diversos interesados del sistema de gestión de la seguridad de las Naciones Unidas, así como coordinación entre ellos, por ejemplo en los aspectos relacionados con las necesidades de recursos administrativos y financieros o con la necesidad de mejorar la capacitación del personal de seguridad, como ya se ha mencionado en otros pasajes del presente informe (párr. 68). El examen llevado a cabo pone de manifiesto que el debate a nivel de todo el sistema en torno a esta cuestión todavía no está maduro y requeriría mayores esfuerzos y un examen más detallado que aprovechara los conocimientos especializados de que dispone el sistema y, en particular, al nivel de la Red Interinstitucional de Gestión de la Seguridad y del Grupo de Interés Especial sobre la Seguridad de la Información. Por ello, los Inspectores recomiendan al Secretario General que explore las oportunidades para aprovechar más la convergencia entre la seguridad física y la ciberseguridad en el sistema de las Naciones Unidas y estudie los beneficios y las limitaciones de las posibles formas de hacerlo. El informe que se presente a la Asamblea General sobre esta cuestión debería basarse, en la medida de lo posible, en los resultados de las consultas que se celebren entre los mecanismos de coordinación interinstitucional pertinentes que se ocupan de la ciberseguridad y la Red Interinstitucional de Gestión de la Seguridad, con aportaciones, cuando proceda, del CICE.

165. Se espera que la aplicación de la recomendación que figura a continuación mejore la eficacia de la respuesta del sistema de las Naciones Unidas a las amenazas a la ciberseguridad.

[56] *Information System Security Guidelines for the United Nations Organizations*.

[57] CEB/2013/5, párr. 40; Red Interinstitucional de Gestión de la Seguridad, 19º período de sesiones (2013), documento publicado sin signatura; y Red Interinstitucional de Gestión de la Seguridad, 20º período de sesiones (2014), documento publicado sin signatura.

Recomendación 5

El Secretario General debería presentar a la Asamblea General de las Naciones Unidas, a más tardar en su septuagésimo octavo período de sesiones, un informe en el que se estudien nuevas oportunidades para aprovechar la convergencia entre la seguridad física y la ciberseguridad con el fin de proporcionar una protección más holística al personal y los bienes de las Naciones Unidas y se indiquen las medidas que deban adoptarse para reforzar de forma acorde las estructuras existentes, prestando especial atención a la posible función del Departamento de Seguridad a este respecto.

Anexo I

Líneas de trabajo intergubernamentales sobre ciberseguridad y ciberdelincuencia

Introducción y términos utilizados

Las cuestiones relacionadas con la ciberseguridad han sido debatidas por la comunidad internacional en varios entornos intergubernamentales.

Por un lado, el tema ha sido examinado por diferentes comisiones de la Asamblea General y órganos que le presentan informes o están vinculados a ella de otro modo. Una de las líneas de trabajo se ha centrado en la ciberdelincuencia (denominada "delitos relacionados con computadoras" a principios de la década de 1990), y la otra, en la información y las telecomunicaciones en el contexto de la seguridad internacional (en la que quedan abarcadas la seguridad de las TIC y temas conexos).

Por otro lado, varios de los mandatos de las organizaciones participantes comprenden aspectos de la ciberseguridad sujetos a los procesos intergubernamentales apoyados por esas organizaciones, como la UIT, la Oficina de Asuntos de Desarme, la UNODC, la OMPI, el PNUD, la UNCTAD y el OIEA.

Los términos "ciberdelincuencia" y "ciberseguridad" no son intercambiables, aunque abordan la misma cuestión desde distintos ángulos. Podría decirse que la ciberdelincuencia se centra en la comisión de ciberataques y en la responsabilidad penal a que se enfrentan sus autores por su participación en actividades ilícitas (ya sean ciberhabilitadas o ciberdependientes). Por el contrario, la ciberseguridad se ocupa de la defensa contra esos ataques y, en lugar de centrarse en sus autores, se centra en el objetivo atacado y sus defensas.

En el presente anexo se reseñan las diferentes líneas de trabajo intergubernamentales a nivel de las organizaciones del sistema de las Naciones Unidas, sus orígenes y su labor actual, así como la relación entre ellas, si la hubiere.

Línea de trabajo I: ciberdelincuencia

La ciberdelincuencia, en la agenda mundial desde la década de 1990. El primer registro documentado de la existencia en la comunidad internacional de cierta concienciación sobre la necesidad de prestar una atención específica a la dimensión cibernética de la labor programática, así como de invertir en la capacidad de los Estados nación para defenderse de los ciberataques (contando con la asistencia técnica de las organizaciones pertinentes del sistema de las Naciones Unidas) se remonta a 1990 y surgió en el contexto de la lucha contra la delincuencia transfronteriza. En concreto, en su resolución 45/121, la Asamblea General hizo suyas las recomendaciones del Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y, en particular, la resolución sobre los delitos relacionados con computadoras, en la que se exhortó a los Estados a que intensificaran sus esfuerzos para luchar más eficazmente contra las infracciones relacionadas con computadoras. La labor sobre este tema prosigue bajo el epígrafe "lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos"[1] en la Tercera Comisión de la Asamblea General (Comisión de Asuntos Sociales, Humanitarios y Culturales) y bajo el epígrafe "ciberdelincuencia" en el contexto de la Comisión de Prevención del Delito y Justicia Penal (que es una comisión orgánica del Consejo Económico y Social), y cuenta con el apoyo sustantivo y administrativo de la UNODC.

Labor en curso para aprobar una convención internacional sobre la ciberdelincuencia. Desde 2010 se han realizado esfuerzos por elaborar un "estudio

[1] Resoluciones de la Asamblea General 73/187, 74/247 y 75/539, y resoluciones anteriores 55/63 y 56/121.

exhaustivo del problema de la ciberdelincuencia" en el contexto de un grupo intergubernamental de expertos de composición abierta (denominado "grupo intergubernamental de expertos sobre la ciberdelincuencia") establecido con ese fin bajo los auspicios de la Comisión de Prevención del Delito y Justicia Penal[2]. La ingente labor resultante de esos esfuerzos ha cobrado impulso y madurado hasta dar lugar a una nueva iniciativa encaminada a elaborar un instrumento jurídicamente vinculante sobre la ciberdelincuencia. El proceso de redacción y negociación de dicho instrumento está supervisado por un comité especial encargado de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos (denominado "el comité especial"), que fue creado por la Asamblea General en 2019 e inició sus trabajos en 2020[3]. El resultado final de ese proceso se remitirá principalmente a los Estados nación en su condición de partes en la convención resultante. Este instrumento proporcionará un marco jurídico destinado en primer lugar a regular el tratamiento de los infractores individuales (ciberdelincuentes) a nivel nacional, por lo que tiene poca relación directa con el enfoque que las organizaciones del sistema de las Naciones Unidas apliquen a la ciberseguridad. Por consiguiente, los esfuerzos en este ámbito tienen un interés limitado para el presente examen.

Línea de trabajo II: la información y las telecomunicaciones en el contexto de la seguridad internacional

En una segunda línea de trabajo intergubernamental, desde 1998 "el examen de las amenazas reales y potenciales en la esfera de la seguridad de la información" empezó a figurar en las resoluciones de la Asamblea General en el marco del nuevo —y en lo sucesivo recurrente— tema del programa titulado "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional"[4]. Se han ocupado del tema dos órganos intergubernamentales que funcionan en el marco de la Primera Comisión de la Asamblea General (Comisión de Desarme y de Seguridad Internacional): a) el Grupo de Expertos Gubernamentales, órgano integrado por un número limitado de expertos nombrados por el Secretario General y que actúan a título personal[5], que es el sexto grupo de este tipo desde la creación del primero en 2004[6]; y b) el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (abierto a todos los Estados Miembros de las Naciones Unidas y creado en 2018)[7]. Los principales objetivos de los dos Grupos son examinar "las amenazas reales y potenciales en el ámbito de la seguridad de la información, y las posibles medidas de cooperación para conjurarlas"[8] y seguir elaborando "las reglas, normas y principios de comportamiento responsable de los Estados [enunciados en la resolución], así como las modalidades de aplicación correspondientes"[9]. Tanto el Grupo de Trabajo de Composición Abierta como el sexto Grupo de Expertos Gubernamentales concluyeron su labor y aprobaron informes de consenso en marzo y mayo de 2021, respectivamente[10]. Se espera que el nuevo Grupo de Trabajo de Composición Abierta sobre la seguridad y la utilización de las tecnologías de la información y las comunicaciones para el período 2021-2025, de reciente creación, examine la labor de su predecesor (que abarcó el período 2019-2020) y celebre su primera reunión en 2021[11]. La labor desempeñada por estos órganos cuenta con el apoyo sustantivo y administrativo de la Oficina de Asuntos de Desarme de las Naciones Unidas.

[2] Resolución 65/230 de la Asamblea General.
[3] Resolución 74/247 de la Asamblea General.
[4] Véase la resolución 53/70 de la Asamblea General y sucesivas, siendo la más reciente de ellas la resolución 75/240.
[5] Véase la resolución 58/32 de la Asamblea General.
[6] Véase la resolución 73/226 de la Asamblea General.
[7] Véase la resolución 73/27 de la Asamblea General.
[8] Véase la resolución 58/32 de la Asamblea General, párr. 4.
[9] Véase la resolución 73/27 de la Asamblea General.
[10] Véase A/75/816.
[11] Véase la resolución 75/240 de la Asamblea General.

Mandatos de las organizaciones del sistema de las Naciones Unidas en materia de ciberseguridad

En los mandatos de cooperación sustantiva y técnica de varias organizaciones del sistema de las Naciones Unidas figuran aspectos relacionados con la ciberseguridad. Un ejemplo de ello es la UIT, que, entre otras cosas, acoge el foro anual de la Cumbre Mundial sobre la Sociedad de la Información —la principal vía para impulsar la cuestión de las TIC para el desarrollo— y es el único organismo facilitador de la línea de acción C5 de la Cumbre, es decir, el "fomento de la confianza y la seguridad en la utilización de las TIC". En esta función, la UIT colabora con los principales interesados para ayudar a los países, entre otras cosas, a adoptar estrategias nacionales de ciberseguridad, establecer capacidades nacionales de respuesta a incidentes, fijar normas internacionales de seguridad, proteger a los niños en el entorno cibernético y fomentar la capacidad. Parte de la labor llevada a cabo en el contexto de la Cumbre Mundial sobre la Sociedad de la Información ha sido reseñada en las resoluciones de la Asamblea General tituladas "creación de una cultura mundial de seguridad cibernética", elaboradas en la Segunda Comisión de la Asamblea General (Comisión de Asuntos Económicos y Financieros)[12]. Otras organizaciones con mandatos que incluyen un componente de ciberseguridad son la UNODC, la OMPI, el PNUD, la UNCTAD, la Oficina de Asuntos de Desarme y el OIEA, así como muchas otras en grados diversos.

En el marco de la JJE debía elaborarse un compendio de los mandatos y las principales actividades de las organizaciones del sistema de las Naciones Unidas en materia de ciberseguridad y ciberdelincuencia con el objeto de reseñar todas las formas en que esas organizaciones habían participado, dentro de sus respectivos mandatos y esferas prioritarias, en la prestación de asistencia técnica y apoyo a la formulación de políticas en este ámbito a lo largo de los años. No obstante, dicho compendio no ha pasado de ser un documento interno cuya conclusión y actualización se ha revelado excesivamente ardua. Por su volumen, puede observarse en él la diversidad y fragmentación que caracterizan la labor programática de las organizaciones del sistema de las Naciones Unidas en esta esfera. En este contexto, el Comité de Alto Nivel sobre Programas ha señalado en repetidas ocasiones la necesidad de que el sistema adopte un enfoque coordinado y coherente, que tenga en cuenta el carácter complementario de los respectivos mandatos de cada organización, así como cierto grado de superposición entre ellos[13].

[12] Véanse las resoluciones de la Asamblea General 57/239 y 64/211.

[13] Véase, por ejemplo, CEB/2010/HLCP XX/CRP.7, párr. 3; CEB/2010/6, párrs. 38 a 43; CEB/2011/HLCP-XXII/CRP.6; y CEB/2014/6, párrs. 42 a 49.

Anexo II

Algunos elementos de un enfoque de la ciberseguridad basado en los riesgos

Además de incorporar formalmente la ciberseguridad al registro o matriz de riesgos institucionales de una organización, los Inspectores desean señalar tres aspectos del enfoque de la ciberseguridad basado en los riesgos que pueden acelerar la obtención de beneficios conexos: a) un enfoque individualizado, sistemático y adaptativo de las evaluaciones de riesgos; b) una declaración estratégica de alto nivel sobre el apetito de riesgo y la tolerancia al riesgo; c) oportunidades adecuadas para que los especialistas en ciberseguridad aporten sus conocimientos al proceso de gestión de riesgos; y d) el empleo de pruebas de penetración como herramienta de gestión de riesgos.

- **Evaluaciones de riesgos individualizadas.** Las evaluaciones de riesgos de ciberseguridad deben adaptarse al contexto en el que una organización desarrolla sus actividades, teniendo debidamente en cuenta criterios como su mandato, su capacidad financiera y de recursos humanos, su modelo institucional, el tipo de información que posee o custodia y sus particularidades organizativas, y en particular la forma en que los incidentes de ciberseguridad afectarían a la ejecución de las tareas que tiene encomendadas, también en entornos descentralizados o en distintos lugares de destino sobre el terreno. Algunas organizaciones participantes se remiten a las normas del sector en apoyo de su proceso de evaluación de riesgos, lo que puede considerarse una buena práctica, siempre que dichas normas se seleccionen en función de su adecuación al contexto de la organización en cuestión (párrs. 59 a 64). Además de la adaptación de las evaluaciones de riesgos, cabe destacar el aspecto de la periodicidad, que no solo facilita la aplicación de un enfoque sistemático, sino que también garantiza la adaptabilidad del marco e idealmente la capacidad de respuesta *ad hoc* a un panorama de amenazas en constante evolución que puede no seguir el mismo ritmo que los ciclos ordinarios de examen.

- **Declaración relativa al apetito de riesgo y la tolerancia al riesgo.** Un componente clave de un enfoque más estratégico de la gestión de los riesgos de ciberseguridad es la articulación de una declaración relativa al apetito de riesgo y la tolerancia al riesgo, a poder ser con la participación de los órganos legislativos y rectores y de la dirección ejecutiva de la organización (párrs. 53 y 54). Dicha declaración debería formularse sobre la base de una evaluación de los riesgos de ciberseguridad exhaustiva y periódica, que abarque todas las categorías de ciberamenazas, no solo las malintencionadas y no solo las externas a la organización (párrs. 25 a 29), y reúna información tanto del departamento de TIC sobre el estado de los sistemas de información institucionales y las vulnerabilidades conocidas como de las dependencias institucionales, en consonancia con el espíritu dimanante de un enfoque que abarque a toda la organización. La determinación del apetito de riesgo adecuado adquiere una importancia primordial cuando se basa en un conjunto cuidadosamente seleccionado y diseñado de parámetros significativos de ciberseguridad. Se trata de un proceso específico de cada organización que impulsará otras decisiones de gestión, como el establecimiento de una capacidad de ciberseguridad institucional interna (por oposición a subcontratada); los recursos que se le asignan; los instrumentos y la orientación de políticas que se incluyen en el marco regulador; y las decisiones relativas a la inversión y a la respuesta a incidentes en caso de notificación a una instancia superior. En organizaciones como la OMPI o el OIEA, que manejan información particularmente sensible, el apetito de riesgo puede ser bajo por defecto. El hecho de haber sufrido incidentes de ciberseguridad importantes también puede reducir el apetito de riesgo de una organización, pero ello puede llevar a una inversión excesiva en ciberdefensas, lo que a su vez puede generar una falsa sensación de seguridad.

- **Incorporación de los conocimientos especializados en ciberseguridad a los procesos de gestión de riesgos.** Puede parecer una obviedad que es necesario ofrecer oportunidades adecuadas para que los conocimientos especializados en ciberseguridad se integren en los procesos de gestión de riesgos institucionales, pero en muchas organizaciones eso está lejos de ser una realidad. El formato y la periodicidad de las aportaciones en cuestión no son decisivos, pero es esencial que los profesionales de la ciberseguridad cuenten con una forma de acceso fiable —que no encuentre trabas y no sea *ad hoc*— a las fuerzas que impulsan la gestión de riesgos dentro de una organización, por lo que ello debería instituirse de manera sistemática a fin de que las consideraciones fundamentales de ciberseguridad se reflejen en las fases de diseño, ejecución y seguimiento del marco de gestión de riesgos de la organización. En algunas organizaciones, el oficial principal de seguridad de la información, de existir dicho cargo, participa en el comité de gestión de riesgos institucionales o es miembro oficial de este. Los comentarios recibidos sobre esta disposición fueron positivos, por lo que quizá sería beneficioso establecerla como práctica en todas las organizaciones.
- **Las pruebas de penetración como herramienta de gestión de riesgos.** Las pruebas de penetración *(pen testing)* consisten en realizar una simulación autorizada de un ataque real contra las redes, sistemas y recursos humanos de una organización con las herramientas y técnicas empleadas habitualmente por los atacantes con el fin de detectar vulnerabilidades en las protecciones de esa organización, evaluar la eficacia de las medidas de mitigación previstas y poner a prueba los procedimientos de respuesta y recuperación. En general son llevadas a cabo por contratistas externos con sujeción a normas diseñadas para permitir una evaluación adaptada y eficaz que a la vez reduzca al mínimo la posibilidad de dañar gravemente los activos y procesos de las organizaciones. Varias organizaciones participantes recurren a esta herramienta, en algunos casos contratando a lo largo de cierto período a contratistas distintos —por ejemplo, alternándolos—, a poder ser con perfiles diversos, para que ataquen a la organización (“equipo rojo”) y pongan a prueba la preparación de la defensa (“equipo azul”). Una organización ha adoptado la estrategia de establecer un equipo conjunto (“equipo morado”) integrado por el contratista externo, que simula el ataque, y los miembros de su centro de operaciones de seguridad, que se defiende de este, lo que permite que los equipos se comuniquen en tiempo real acerca de los resultados y de las posibles medidas de mitigación. Tanto si se recurre a uno como a varios contratistas, las pruebas de penetración son onerosas y exigen una sólida preparación y una cuidadosa selección de evaluadores expertos que se hagan pasar por los atacantes y sean fiables, ya que permitirles el acceso, aunque sea temporal, a sistemas e información sensibles entraña riesgos reales. Aun así, son una herramienta sofisticada y eficaz de gestión de riesgos, que puede utilizarse en apoyo de la planificación de la continuidad de las operaciones y constituye un método fiable para obtener una visión rápida de la posición de ciberseguridad de la organización desde diversos ángulos y, dependiendo del alcance que se defina para cada ejercicio, detectar deficiencias en sus defensas generales o vulnerabilidades específicas en ámbitos concretos.

Anexo III

Principales normas del sector sobre ciberseguridad mencionadas por las organizaciones participantes en la Dependencia Común de Inspección

ISO 27001 (International Organization for Standardization, 2005)[1]

Utilizada principalmente con fines de auditoría y cumplimiento, la ISO 27001 se centra sobre todo en los hitos que deben alcanzarse en relación con los aspectos técnicos de las defensas de ciberseguridad y proporciona orientación al respecto. Sigue un conjunto general de 14 controles destinados a integrar la ciberseguridad en los objetivos institucionales y las prácticas de gestión de riesgos de la organización. Dichos controles se agrupan principalmente en las esferas de las políticas en materia de seguridad de la información, la gestión de activos, el control de acceso, la seguridad de las operaciones y las comunicaciones, la gestión de incidentes y el cumplimiento. Debido a sus características, este marco parece adecuarse mejor al examen y la auditoría de las medidas de ciberseguridad en organizaciones grandes y con abundancia de recursos.

Marco del Instituto Nacional de Normas y Tecnología de los Estados Unidos, 1901[2]

Al definir los objetivos y prioridades de una organización y establecer las medidas adecuadas, el Instituto Nacional de Normas y Tecnología de los Estados Unidos proporciona una orientación flexible y adaptable para entender los riesgos de ciberseguridad. Además de sus orientaciones internas, el marco, actualizado por última vez en 2015, también incluye referencias a otras normas, orientaciones y prácticas, como los Center for Internet Security Controls, las normas internacionales de la International Organization for Standardization, los Objetivos de Control para la Tecnología de la Información y Tecnologías Conexas y otros. El plan de acción del Instituto Nacional de Normas y Tecnología señala cinco funciones básicas (identificar, proteger, detectar, responder y recuperar) y clasifica los flujos de información y decisión en diferentes niveles dentro de la organización. Debido a su fuerte enfoque holístico, esta norma parece adecuarse especialmente a la definición de las estrategias y políticas de ciberseguridad de la organización.

Objetivos de Control para la Tecnología de la Información y Tecnologías Conexas (Asociación de Auditoría y Control de los Sistemas de Información (ISACA), 1996)[3]

Los Objetivos de Control para la Tecnología de la Información y Tecnologías Conexas constituyen un marco de gobernanza y gestión de la tecnología de la información basado en las mejores prácticas, que ayuda a las organizaciones a alcanzar sus objetivos en los ámbitos del cumplimiento y la gestión de riesgos y a ajustar su estrategia de tecnología de la información a sus objetivos. Dicho marco aplica un enfoque basado en el concepto de niveles de capacidad y se centra en la adaptación de los servicios a las necesidades de la organización. En esta norma internacional, los aspectos relativos a la seguridad de la información se consideran enmarcados en la gestión de riesgos y la continuidad y disponibilidad de las operaciones. Además de a sus materiales internos, en los Objetivos de Control para la Tecnología de la Información y Tecnologías Conexas se hace referencia a otras normas y guías, como el marco del Instituto Nacional de Normas y Tecnología de los

[1] Puede consultarse en: www.iso.org/home.html.
[2] Puede consultarse en: www.nist.gov.
[3] Puede consultarse en: www.isaca.org/credentialing/cobit/cobit-foundation.

Estados Unidos, la norma ISO 27001 y los Center for Internet Security Controls. Los objetivos de armonización más pertinentes de entre los que figuran en los Objetivos abarcan la gestión de riesgos de la tecnología de la información, la seguridad de la información, el cumplimiento y la continuidad y disponibilidad de las operaciones. Por lo que respecta a la orientación en materia de ciberseguridad, esta norma parece ser particularmente adecuada para las organizaciones que ya hacen uso de los Objetivos de Control para la Tecnología de la Información y Tecnologías Conexas para su marco de gobernanza y gestión de la TIC. Además, este marco puede ampliarse combinándolo con otras normas a las que se remite (los Center for Internet Security Controls, el marco del Instituto Nacional de Normas y Tecnología y la ISO 27001).

Biblioteca de Infraestructura de Tecnología de la Información (Organismo Central de Computación y Telecomunicaciones del Reino Unido de Gran Bretaña e Irlanda del Norte, década de 1980)[4]

La Biblioteca de Infraestructura de Tecnología de la Información es un conjunto de directrices en materia de gestión de servicios de TIC y comprende varias publicaciones que proporcionan orientación pertinente sobre la prestación de servicios de TIC y sobre los procesos y recursos que necesitan las organizaciones. Elaborada por el Organismo Central de Computación y Telecomunicaciones del Reino Unido en la década de 1980, esta norma consta de cinco volúmenes, en cada uno de los cuales se trata una de las fases del ciclo de gestión de servicios de TIC. Entre los principales temas abarcados figuran la definición del valor de los servicios, el desarrollo empresarial, los activos de los servicios, el análisis del mercado y los tipos de proveedores de servicios. Desde 2005, las prácticas de la Biblioteca de Infraestructura de Tecnología de la Información contribuyeron a la norma ISO 20000 y se ajustaron con ella.

Center for Internet Security Controls, 2008[5]

También conocida como Critical Cybersecurity Controls, esta norma ofrece un conjunto de recomendaciones basadas en las mejores prácticas del sector. Si bien tiene una orientación básicamente técnica, incluye también algunos controles que se ocupan de aspectos organizativos más amplios de la ciberseguridad, como los programas de sensibilización y la respuesta a incidentes. Este marco parece ser bastante práctico y muy útil en lo que respecta a los grupos de aplicación, ya que se centra en las medidas que pueden aplicarse en función del tamaño, las habilidades, los recursos disponibles y la sensibilidad de los datos de cada organización. Entre sus principales controles figuran el inventario y los activos, la gestión de la vulnerabilidad, la configuración segura, las protecciones del correo electrónico y el navegador, la recuperación y protección de datos, la respuesta a incidentes y las pruebas de penetración. Este enfoque se ha demostrado particularmente adecuado para la aplicación de estrategias de defensa de la ciberseguridad en organizaciones pequeñas y medianas que ya cuenten con marcos de riesgo que integren aspectos de ciberseguridad.

[4] Puede consultarse en: www.axelos.com/best-practice-solutions/itil.
[5] Puede consultarse en: www.cisecurity.org/controls/.

Anexo IV

Marcos reguladores de las organizaciones del sistema de las Naciones Unidas en materia de ciberseguridad

a) Niveles de un marco regulador de ciberseguridad

Nivel estratégico	A menudo, un único documento en el que se recogen declaraciones de alto nivel en las que se expresan aspiraciones	Define la visión, los objetivos y los principios fundamentales de la organización, expone las funciones y responsabilidades básicas de tipo organizativo y de gobernanza, y puede abordar la ciberseguridad en términos de decisión institucional e incluir una declaración relativa a la tolerancia al riesgo o el apetito de riesgo de la organización	Se aplica a la organización a nivel de entidad y tiene como principal destinatario al personal directivo superior para que se encargue de llevarlo a la práctica
Nivel de políticas	Un conjunto de documentos independientes que contienen un lenguaje prescriptivo y traducible en medidas concretas, generalmente publicados como disposiciones administrativas oficiales	Expone los principios organizativos que sustentan el sistema de gestión de la seguridad de la información con reglamentos y normas internos vinculantes, con inclusión de declaraciones de intenciones y medidas conexas organizadas por temas (por ejemplo, clasificación de la información, gestión de riesgos, continuidad de las operaciones y recuperación en casos de desastre o usos aceptables de los datos y activos de la TIC) y asignación de funciones y responsabilidades específicas	Se aplica a todo el personal y contempla la posibilidad de imponer sanciones disciplinarias en caso de incumplimiento
Nivel de procedimiento	Un conjunto de directrices o procedimientos operativos estándar destinados a apoyar las políticas de alto nivel mediante la descripción de procesos para establecer prácticas sistemáticas	Proporciona orientación detallada sobre los pasos concretos a seguir o los comportamientos a evitar (respetar las convenciones de uso de las contraseñas, ejecutar antivirus y actualizar el *software* con regularidad, analizar los lápices de memoria USB recibidos como obsequio antes de su utilización, y otros)	Puede aplicarse a todo el personal o estar orientado a funciones específicas (por ejemplo, al personal de TIC, los gestores de archivos y registros o los especialistas en adquisiciones)
Nivel técnico	Un conjunto de protocolos técnicos destinados a lograr una ejecución correcta y uniforme	Ofrece una orientación detallada y paso a paso cuya aplicación y puesta en práctica requiere un nivel importante de conocimientos técnicos en la materia. Pueden tratarse temas como la configuración de bases de datos, la seguridad de las redes o la seguridad en la nube	Dirigido principalmente a expertos técnicos

Fuente: Elaborado por la DCI.

b) Estrategias de tecnología de la información y las comunicaciones y documentos de política de ciberseguridad específicos en las organizaciones participantes

Organización participante	*Estrategia institucional de tecnología de la información y las comunicaciones con un componente de ciberseguridad*	*Documentos de política de ciberseguridad específicos*
Secretaría de las Naciones Unidas	Sí: Tecnología de la información y las comunicaciones en las Naciones Unidas (A/69/517) y resolución 69/262 de la Asamblea General	Sí: Directiva de política de seguridad de la información para la Secretaría de las Naciones Unidas (2013)
ONUSIDA	No: La Estrategia de TIC (2017-2020) no contempla la ciberseguridad	No: ONUSIDA está elaborando un plan de ciberseguridad a nivel mundial que incluirá una política de ciberseguridad
UNCTAD	Sigue la estrategia de tecnología de la información y las comunicaciones de la Secretaría de las Naciones Unidas	Sí: Sigue la estrategia de ciberseguridad de la Secretaría de las Naciones Unidas
PNUD	Sí: Estrategia de tecnología de la información (2020-2023)	Sí: Política de seguridad de la información (2016)
PNUMA	Sigue la estrategia de tecnología de la información y las comunicaciones de la Secretaría de las Naciones Unidas	Sí: Sigue la estrategia de ciberseguridad de la Secretaría de las Naciones Unidas
UNFPA	Sí: Estrategia de tecnología de la información y las comunicaciones (2018-2021)	Sí: Política de seguridad de la tecnología de la información y las comunicaciones
ONU-Hábitat	Sigue la estrategia de tecnología de la información y las comunicaciones de la Secretaría de las Naciones Unidas	Sí: Sigue la estrategia de ciberseguridad de la Secretaría de las Naciones Unidas
ACNUR	Sí: Estrategia de tecnología de la información (2020-2022) (proyecto final en proceso de examen)	Actualmente en proceso de elaboración
UNICEF	Sí: Estrategia de tecnología de la información y las comunicaciones	Sí: Plan estratégico de seguridad de la información de UNICEF (2018-2022)
UNODC/ONUV	Sigue la Estrategia de tecnología de la información y las comunicaciones de la Secretaría de las Naciones Unidas	Sí: Sigue la estrategia de ciberseguridad de la Secretaría de las Naciones Unidas
UNOPS	Una estrategia de TIC quinquenal (en proceso de elaboración)	Sí: Seguridad de la información
UNRWA	Sí: Estrategia del Departamento de Gestión de la Información (2019-2020)	Existe una política de seguridad de la información independiente (pendiente de aprobación definitiva)
ONU-Mujeres	Sí: Estrategia de tecnología de la información y las comunicaciones (2018-2021)	Sí: Política de seguridad de la información
PMA	Sí: Estrategia institucional de tecnología de la información (2016-2020)	Sí: Política institucional de seguridad de la información y de la tecnología de la información (2015)
FAO	Sí: Estrategia digital de tecnología de la información y las comunicaciones (2017)	Sí: Política de seguridad de la información

Organización participante	*Estrategia institucional de tecnología de la información y las comunicaciones con un componente de ciberseguridad*	*Documentos de política de ciberseguridad específicos*
OIEA	Sí: Plan Estratégico de Tecnología Institucional (2015-2020)	Sí: Normas sobre seguridad de la información
OACI	Sí: Estrategia digital de tecnología de la información y las comunicaciones (2017) (en proceso de examen)	Sí: Política de seguridad de la información (2007, Rev. 2)
OIT	Sí: Estrategia de tecnología de la información (2018-2021)	Sí: Declaraciones de política de seguridad de la información electrónica (2010)
OMI	Sí: Plan estratégico de tecnología de la información y la comunicación (2019-2023)	Sí: Gestión de riesgos para la seguridad de la información (2015)
UIT	No: La UIT aplica un enfoque más holístico, con la introducción de un sistema de gestión de la resiliencia institucional en cuyo marco se prevé la realización de un análisis detallado del impacto en las operaciones con el fin de trazar los riesgos estratégicos y las estrategias contra el impacto en las operaciones, así como la gestión de crisis, la continuidad de las operaciones y la recuperación en casos de desastre relacionados con la TIC	No
UNESCO	Sí: Estrategia de gestión del conocimiento y tecnología de la información y las comunicaciones (2018-2021)	Sí: Incluidos en el marco de gestión de los riesgos institucionales y en el manual administrativo (política de seguridad de la información y de la tecnología de la información)
ONUDI	Sí: Estrategia institucional de tecnología de la información y las comunicaciones (2019-2021)	No
OMT	No: La estrategia de tecnología de la información y las comunicaciones no contempla la ciberseguridad	No: En proceso de elaboración
UPU	No: La estrategia de TIC de la UPU estará disponible en diciembre de 2021	No
OMS	Sí: Estrategia de gestión y tecnología de la información (2019)	Sí: Estrategia de ciberseguridad
OMPI	Sí: Estrategia de tecnología de la información y las comunicaciones (nueva estrategia en proceso de elaboración)	Sí: Políticas y normas de seguridad de la información y Estrategia de seguridad de la información de próxima generación (2021-2024)
OMM	Sí: Estrategia de tecnología de la información y las comunicaciones (2020-2023)	No

Anexo V

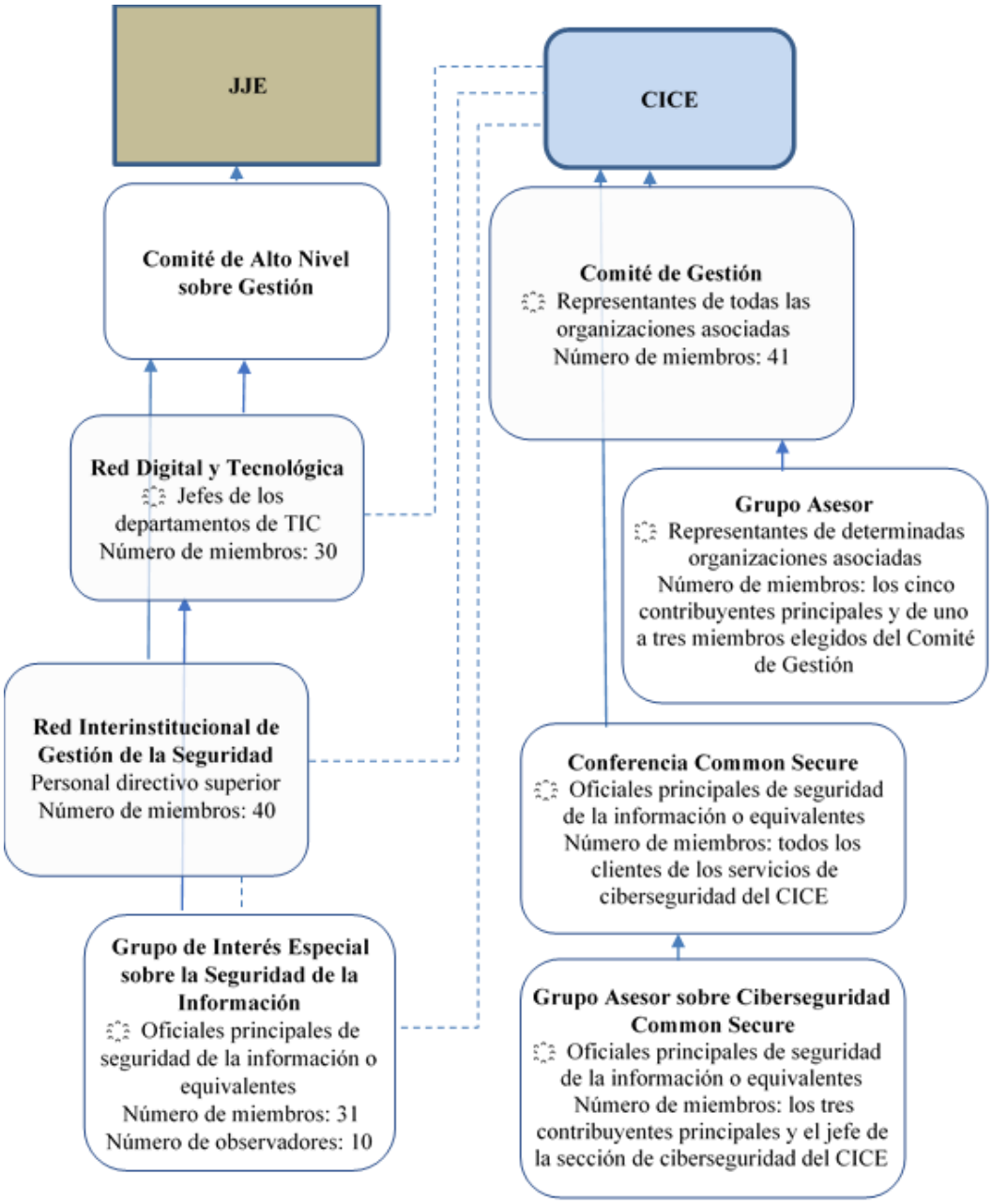
Disposiciones de ciberseguridad y relaciones jerárquicas en las organizaciones participantes en la Dependencia Común de Inspección a fecha de enero de 2021

Organización participante	*Se ocupa de las cuestiones relacionadas con la ciberseguridad una capacidad interna específica o especializada*	*Se ocupa de la ciberseguridad el departamento de TIC de la organización (entre sus otras funciones de TIC)*	*Ha utilizado el "oficial principal de seguridad de la información como servicio" o servicio de gobernanza de la seguridad prestado por el CICE*	*Bajo la autoridad jerárquica del jefe de TIC (o equivalente)*
Secretaría de las Naciones Unidas	√		X	√
ONUSIDA		√	X	√
UNCTAD		√	√ (Cliente actual)	√
PNUD	√		X	√
PNUMA		√	X	√
UNFPA	√ (Oficial principal de seguridad de la información en proceso de contratación)	√ (Hasta que se complete el proceso de contratación)	√ (Cliente actual)	√
ACNUR	√		X	√
UNICEF	√		√ (Cliente actual)	√
UNODC/ONUV		√	X	√
UNOPS	√		X	El oficial principal de seguridad de la información depende jerárquicamente del Oficial Jefe de Finanzas y del Director de Administración
UNRWA	√		X	√
ONU-Mujeres		√	√ (Cliente en el pasado)	√
PMA	√		√ (Cliente en el pasado)	√
FAO	√		√ (Cliente actual)	√
OIEA	√		X	√

Organización participante	*Se ocupa de las cuestiones relacionadas con la ciberseguridad una capacidad interna específica o especializada*	*Se ocupa de la ciberseguridad el departamento de TIC de la organización (entre sus otras funciones de TIC)*	*Ha utilizado el "oficial principal de seguridad de la información como servicio" o servicio de gobernanza de la seguridad prestado por el CICE*	*Bajo la autoridad jerárquica del jefe de TIC (o equivalente)*
OACI	√		√ (Cliente en el pasado)	El oficial principal de seguridad de la información está bajo la autoridad jerárquica directa del Jefe de Administración
OIT	√		**X**	√
OMI		√	**X**	√
UIT	√		**X**	√
UNESCO	√		√ (Cliente actual)	√
ONUDI		√	**X**	√
OMT		√	**X**	√
UPU		√	**X**	√
OMS	√		√ (Cliente en el pasado)	√
OMPI	√		**X**	El Jefe de la División de Seguridad y Aseguramiento de la Información, que desempeña la función de oficial jefe de seguridad encargado tanto de la seguridad física como de la seguridad de la información, depende jerárquicamente del Subdirector General de Administración, Finanzas y Gestión
OMM		√	√ (Cliente actual)	√

Anexo VI

Disposiciones institucionales y operacionales entre las organizaciones en materia de ciberseguridad



Fuente: Elaborado por la DCI.

Anexo VII

Visión general de los servicios de ciberseguridad ofrecidos por el CICE suscritos por las organizaciones participantes en la Dependencia Común de Inspección a fecha de enero de 2021

Servicio de ciberseguridad	*Breve descripción*	*Número de organizaciones participantes en la Dependencia Común de Inspección suscritas actualmente*	*Número de organizaciones participantes en la Dependencia Común de Inspección suscritas en el pasado o proyectos completados*
Common Secure Threat Intelligence	Recopilación pronta y continua de información procedente de: los miembros del organismo; empresas comerciales de seguridad; proveedores de servicios; organismos gubernamentales federales, estatales y locales; fuerzas del orden y otros recursos de confianza. Permite a las entidades suscritas intercambiar toda la información pertinente y traducible en medidas sobre amenazas a la seguridad física y la ciberseguridad y sobre incidentes.	17	
Servicio común de firma electrónica	Ofrece la posibilidad de proporcionar firmas digitales.	14	
Sensibilización sobre la seguridad de la información	Ofrece servicios de asesoramiento estratégico destinados a ayudar a la organización a establecer una estrategia moderna y eficaz de sensibilización sobre la seguridad de la información, un laboratorio de aprendizaje en la nube líder en el sector o apoyo en la esfera de las comunicaciones, que puede incluir entregables con mensajes, boletines, pósteres y apoyo al portal.	7	3
Gestión de la vulnerabilidad	Combinación de procesos y tecnologías que permiten detectar y subsanar de forma continua las vulnerabilidades y fallos de configuración. Esto se logra realizando análisis de vulnerabilidad de las computadoras centrales y las aplicaciones, comprobaciones de la configuración de seguridad y un seguimiento del rastro dejado en Internet, entre otros.	6	1

Servicio de ciberseguridad	*Breve descripción*	*Número de organizaciones participantes en la Dependencia Común de Inspección suscritas actualmente*	*Número de organizaciones participantes en la Dependencia Común de Inspección suscritas en el pasado o proyectos completados*
Servicios de apoyo a la gobernanza y a los oficiales principales de seguridad de la información	Servicio de sistema de gestión de la seguridad de la información que tiene por objetivo proteger los activos de la organización y mitigar el riesgo de exposición a los efectos negativos sobre la reputación, la pérdida de información importante y los actos malintencionados, así como los riesgos para la propiedad intelectual, los datos sensibles y la reputación.	6	5
Servicios de simulación de *phishing*	Evalúa la eficacia de los programas de sensibilización sobre la seguridad de la información llevados a cabo por las organizaciones. Esta herramienta incluye el diseño y ejecución de campañas de simulación de *phishing* y la elaboración de informes de seguimiento.	6	
Servicio de centro de operaciones de seguridad Common Secure	Proporciona conocimientos especializados para vigilar, analizar y responder a los eventos de ciberseguridad a fin de que las entidades suscriptoras puedan responder de forma oportuna a los incidentes de seguridad mediante una combinación de procesos y soluciones tecnológicos.	4	1
Respuesta a incidentes	Proporciona procedimientos de gestión de incidentes basados en las normas del sector para analizar los datos relativos a los incidentes y establecer las respuestas adecuadas a cualquier incidente de seguridad de la organización en tiempo real.	4	7
Evaluación de la seguridad en la nube	Evaluación, migración, implementación y apoyo operacional integral, así como gestión de costos para varias soluciones en la nube.	4	1
Pruebas de penetración	Permiten identificar los puntos débiles de los controles de seguridad de la información y determinar el grado en que los adversarios pueden penetrar en la red o los sistemas que se ponen a prueba.	3	4
Infraestructura de clave pública común	Se facilita y gestiona el cifrado de clave pública y privada y las firmas digitales con el fin de crear un entorno seguro para las transacciones electrónicas y las transferencias de datos.	3	

Servicio de ciberseguridad	*Breve descripción*	*Número de organizaciones participantes en la Dependencia Común de Inspección suscritas actualmente*	*Número de organizaciones participantes en la Dependencia Común de Inspección suscritas en el pasado o proyectos completados*
Gestión de identidades y accesos	Se recopila, analiza y presenta información sobre las aplicaciones de gestión de identidades y accesos.	2	1
Información de seguridad y gestión de eventos Common Secure	Proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el *hardware* de la red.	1	

Fuente: Catálogo de servicios del CICE (julio de 2021) y respuestas de las organizaciones participantes a los cuestionarios de la DCI.

Anexo VIII

Comparación de la participación de las entidades activas en la esfera de la ciberseguridad a fecha de enero de 2021

Organizaciones participantes	*Red Digital y Tecnológica (33er período de sesiones, 2019)*	*Grupo de Interés Especial sobre la Seguridad de la Información (octavo Simposio, 2019)*	*CICE Comité de Gestión (en 2020)*	*Clientes de los servicios del CICE (pasados y actuales)*
Secretaría de las Naciones Unidas	√	√	√	X
ONUSIDA	√	X	√	X
UNCTAD	√	X	√	√
PNUD	√	√	√	√
PNUMA	√	X	√	X
UNFPA	√	√	√	√
ONU-Hábitat	√	X	X[1]	X
ACNUR	√	√	√	√
UNICEF	√	√	√	√
UNODC/ONUV	X	X	X[2]	√
UNOPS	√	X	√	√
UNRWA	√	X	√	√
ONU-Mujeres	√	√	√	√
PMA	√	√	√	√
FAO	√	X	√	√
OIEA	√	√	√	√
OACI	√	X	√	√
OIT	√	√	√	√
OMI	√	X	√	√
UIT	√	√	√	√
UNESCO	√	X	√	√
ONUDI	√	√	√	√
OMT	X	√	X	√
UPU	X	√	√	X
OMS	X	√	√	√

[1] El CICE comunicó que ONU-Hábitat estaba representado en el Comité de Gestión a través de la Secretaría de las Naciones Unidas.

[2] El CICE comunicó que la UNODC/Oficina de las Naciones Unidas en Viena estaba representada en el Comité de Gestión a través de la Secretaría de las Naciones Unidas.

Organizaciones participantes	*Red Digital y Tecnológica (33er período de sesiones, 2019)*	*Grupo de Interés Especial sobre la Seguridad de la Información (octavo Simposio, 2019)*	*CICE Comité de Gestión (en 2020)*	*Clientes de los servicios del CICE (pasados y actuales)*
OMPI	√	√	√	√
OMM	√	√	√	√

Anexo IX

Glosario de términos relacionados con la ciberseguridad

Ataque de denegación de servicio distribuida	Ataque en el que se utilizan múltiples sistemas infectados para atacar a un único objetivo. El sistema atacado es inundado por una avalancha de mensajes que lo obliga a desconectarse y a denegar el servicio a los usuarios legítimos. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Cifrado	Función matemática que protege la información haciéndola ilegible para todos los que no posean la clave para descifrarla. *Fuente:* National Cyber Security Centre (Reino Unido) www.ncsc.gov.uk/information/ncsc-glossary
Cortafuego	Barrera de seguridad interpuesta entre dos redes que controla la cantidad y el tipo de tráfico que puede circular entre ellas. Esto protege a los recursos locales del sistema, de modo que no se pueda acceder a ellos desde el exterior. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Dispositivo de usuario final	Cualquier dispositivo conectado a una red, como una computadora de escritorio, un portátil, un teléfono inteligente, una tableta, una impresora u otro *hardware* especializado, como los terminales de punto de venta o los terminales para compras en autoservicio, que actúa como terminal de usuario en una red distribuida. *Fuente:* glosario de Barracuda Networks Inc. www.barracuda.com/glossary/endpoint-device
Exposición de datos	Divulgación involuntaria o intencionada de información, de modo que se vean afectadas su confidencialidad, integridad o disponibilidad. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Ingeniería social	Manipulación ejercida sobre una persona para que realice determinadas acciones o divulgue información de utilidad para el atacante. *Fuente:* National Cyber Security Centre (Reino Unido) www.ncsc.gov.uk/information/ncsc-glossary
Internet de los objetos	Red de dispositivos de uso cotidiano con conexión a Internet que pueden conectarse entre sí e intercambiar información. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Pastoreo de bots *(bot herding)*, red de bots *(botnet)*	Una red de bots es un gran número de computadoras infectadas y controladas remotamente que se utilizan para crear y enviar *spam* o virus, o para inundar una red con mensajes a modo de ataque de denegación de servicio. *Fuente:* glosario de términos de seguridad del ESCAL Institute of Advanced Technologies www.sans.org/security-resources/glossary-of-terms/

Phishing	Intento por parte de un tercero de solicitar información confidencial a una persona, grupo u organización imitando o suplantando *(spoofing)* una determinada marca, por lo general muy conocida, normalmente con el objetivo de obtener un beneficio económico. Los autores tratan de engañar a los usuarios para que les revelen datos personales, como la numeración de su tarjeta de crédito, sus credenciales de acceso a plataformas bancarias en línea u otra información sensible, que luego pueden utilizar para cometer actos fraudulentos. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Phishing* personalizado *(spear phishing)	Utilización de correos electrónicos de suplantación de identidad *(spoofing)* con el objeto de persuadir a personas de una organización para que revelen sus nombres de usuario o contraseñas. A diferencia del *phishing*, en el que hay un envío masivo de correos, el *spear phishing* se realiza a pequeña escala y se dirige a un objetivo muy concreto. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Programa malintencionado *(malware)*	Software malintencionado diseñado para infiltrarse en un sistema informático o dañarlo sin el consentimiento del propietario. Entre las formas más comunes figuran los virus informáticos, los gusanos, los troyanos, los programas espía y el *adware*. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Programa secuestrador *(ransomware)*	Tipo de *malware* que deniega el acceso a un sistema o a datos a un usuario hasta que pague cierta suma de dinero. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Red privada virtual	Red privada de comunicaciones generalmente utilizada por una empresa, o varias empresas u organizaciones distintas, para comunicarse a través de una red más amplia. Las comunicaciones de una red privada virtual suelen estar cifradas o codificadas para protegerlas del tráfico de otros usuarios de la red pública que sirve de canal a la red privada virtual. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Suplantación de identidad *(spoofing)*	Suplantación del remitente de una transmisión para entrar ilegalmente en un sistema seguro. *Fuente:* Committee on National Security Systems (Estados Unidos) https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
TI en la sombra *(shadow IT)*	El uso de *hardware* o *software* por un departamento o individuo sin el conocimiento de los responsables de la tecnología de la información o de la seguridad de la organización. *Fuente:* Cisco. www.cisco.com/c/en/us/products/security/what-is-shadow-it.html

Vulnerabilidad	Fallo o debilidad en el diseño o el despliegue de un sistema informático o de su entorno que podría ser aprovechado para afectar negativamente a los activos o las operaciones de una organización. *Fuente:* Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary

Anexo X

Sinopsis de las medidas que han de adoptar las organizaciones participantes en relación con las recomendaciones de la Dependencia Común de Inspección

			Naciones Unidas, sus fondos y programas																*Organismos especializados y OIEA*											
		Efecto previsto	*CICE*	*Naciones Unidas*	*ONUSIDA*	*UNCTAD*	*ITC*	*PNUD*	*PNUMA*	*UNFPA*	*ONU-Hábitat*	*ACNUR*	*UNICEF*	*UNODC*	*UNOPS*	*UNRWA*	*ONU-Mujeres*	*PMA*	*FAO*	*OIEA*	*OACI*	*OIT*	*OMI*	*UIT*	*UNESCO*	*ONUDI*	*OMT*	*UPU*	*OMS*	*OMPI*	*OMM*
Informe	**Adopción de medidas**		☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	Para información		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Recomendación 1		**f**		**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**
Recomendación 2		**f**		**L**	**L**			**L**	**L**	**L**			**L**		**L**		**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
Recomendación 3		**c**	**E**																											
Recomendación 4		**c**		**L**																										
Recomendación 5		**f**		**E**																										

Leyenda: **L:** Recomendación para la adopción de decisiones por el órgano legislativo.
E: Recomendación para la adopción de medidas por el jefe ejecutivo.
☐**:** La recomendación no requiere la adopción de medidas por esta organización.

Efecto deseado: **a:** aumento de la transparencia y la rendición de cuentas; **b:** divulgación de buenas/mejores prácticas; **c:** mejora de la coordinación y la cooperación; **d:** fortalecimiento de la coherencia y la armonización; **e:** mejora del control y el cumplimiento; **f:** mayor eficacia; **g:** ahorro notable; **h:** más eficiencia; **i:** otros.