Organización Internacional del Trabajo

▶ GB.346/PFA/3

Consejo de Administración

346.ª reunión, Ginebra, octubre-noviembre de 2022

Sección de Programa, Presupuesto y Administración

PFA

Segmento de Programa, Presupuesto y Administración

Fecha: 16 de septiembre de 2022
Original: inglés

Tercer punto del orden del día

Examen del marco de ciberseguridad de la OIT

Finalidad del documento

En este documento se informa acerca de los resultados de una evaluación del grado de madurez en ciberresiliencia y la armonización de las prácticas de la OIT con los pilares señalados en el informe de la Dependencia Común de Inspección, *La ciberseguridad en las organizaciones del sistema de las Naciones Unidas* (véase el proyecto de decisión que figura en el párrafo 13).

Objetivo estratégico pertinente: Ninguno.

Resultado más pertinente: Resultado funcional C: Servicios de apoyo eficientes y utilización eficaz de los recursos de la OIT.

Repercusiones en materia de políticas: Ninguna.

Repercusiones jurídicas: Ninguna.

Repercusiones financieras: Ninguna.

Seguimiento requerido: Ninguno.

Unidad autora: Departamento de Gestión de la Información y de las Tecnologías (INFOTEC).

Documentos conexos: Programa y Presupuesto para el bienio 2022-2023.

▶ Introducción

1. En 2021, la Dependencia Común de Inspección (DCI) presentó un informe en el que se señalaban los retos comunes en materia de ciberseguridad que se plantean en el sistema de las Naciones Unidas [1]. Según el informe, para gozar de una posición sólida en materia de ciberseguridad, las organizaciones deben aplicar un enfoque multifacético, a escala de toda la organización, que incluya varios ámbitos y competencias organizativas, como las tecnologías de la información y las comunicaciones, la gestión de los riesgos, la seguridad e integridad físicas y la gestión de la información y del conocimiento, en un contexto más amplio. En el informe se señalan además diez factores, o pilares, que contribuyen a mejorar la ciberresiliencia de las organizaciones del sistema de las Naciones Unidas; es decir, su capacidad para identificar, prevenir y detectar ciberamenazas, así como para responder y recuperarse si se produce un incidente (gráfico 1).

▶ Gráfico 1. Pilares de la ciberresiliencia establecidos por la DCI

Colaboración con los órganos legislativos y rectores	Incorporación de la ciberseguridad en la gestión de los riesgos de la organización	Aprovechamiento de la convergencia entre la seguridad física y la ciberseguridad	Configuración de marcos reguladores para el cumplimiento y la rendición de cuentas	Aprovechamiento de las aportaciones de los mecanismos de supervisión
Fomento de una cultura de ciberseguridad desde la dirección	Aplicación de un enfoque que abarque a toda la organización	Establecimiento de una primera línea de defensa basada en el personal	Optimización de la asignación de recursos financieros para la ciberseguridad	Inversión en recursos humanos dedicados y especializados

2. Una de las recomendaciones principales que la DCI formula en su informe a los jefes ejecutivos de las organizaciones del sistema de las Naciones Unidas es que deberían examinar sus marcos de ciberseguridad y presentar un informe sobre sus conclusiones a sus respectivos órganos rectores. Con arreglo a las mejores prácticas establecidas, la OIT encargó a una organización independiente, el Centro Internacional de Cálculos Electrónicos, que efectuara el examen y comunicara sus conclusiones. En este documento se presentan las conclusiones y recomendaciones fundamentales del examen, que consistió en una evaluación del nivel de madurez en materia de ciberresiliencia.

[1] Naciones Unidas, *La ciberseguridad en las organizaciones del sistema de las Naciones Unidas*, Informe de la Dependencia Común de Inspección, JIU/REP/2021/3, 2021.

▶ Conclusiones y recomendaciones

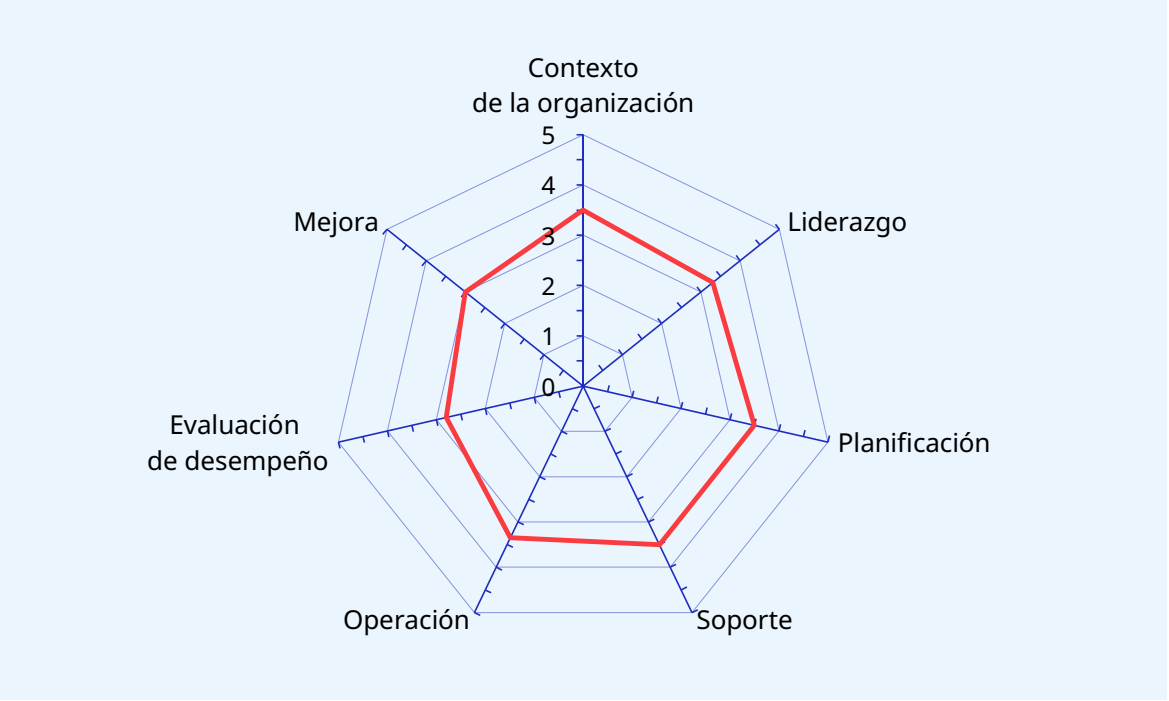
Perfil del nivel de madurez de la ciberseguridad de la Oficina

3. La Oficina cuenta con una Unidad de Servicios de Aseguramiento y Seguridad de la Información específica cuyo equipo se ha ido ampliando desde el nombramiento en 2007 de un funcionario responsable de la seguridad de la tecnología de la información. Dicha unidad ha establecido un sistema de gestión de la seguridad de la información que ha recibido, de una entidad independiente, la acreditación de conformidad con la norma ISO 27001 sobre seguridad de la información. En todo el mundo se reconoce que dicha acreditación indica conformidad con las mejores prácticas en materia de seguridad de la información.

4. Para evaluar el nivel de madurez de la ciberresiliencia, el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas se basó tanto en la norma ISO 27001 como en los pilares establecidos por la DCI. Los resultados se vincularon con el modelo de madurez de las capacidades. La evaluación arrojó unos resultados generales de madurez de la ciberseguridad de 3,58 sobre 5, lo que sitúa a los procesos de ciberseguridad de la OIT en la mitad superior del tercer nivel de madurez del modelo, calificado de «proceso definido».

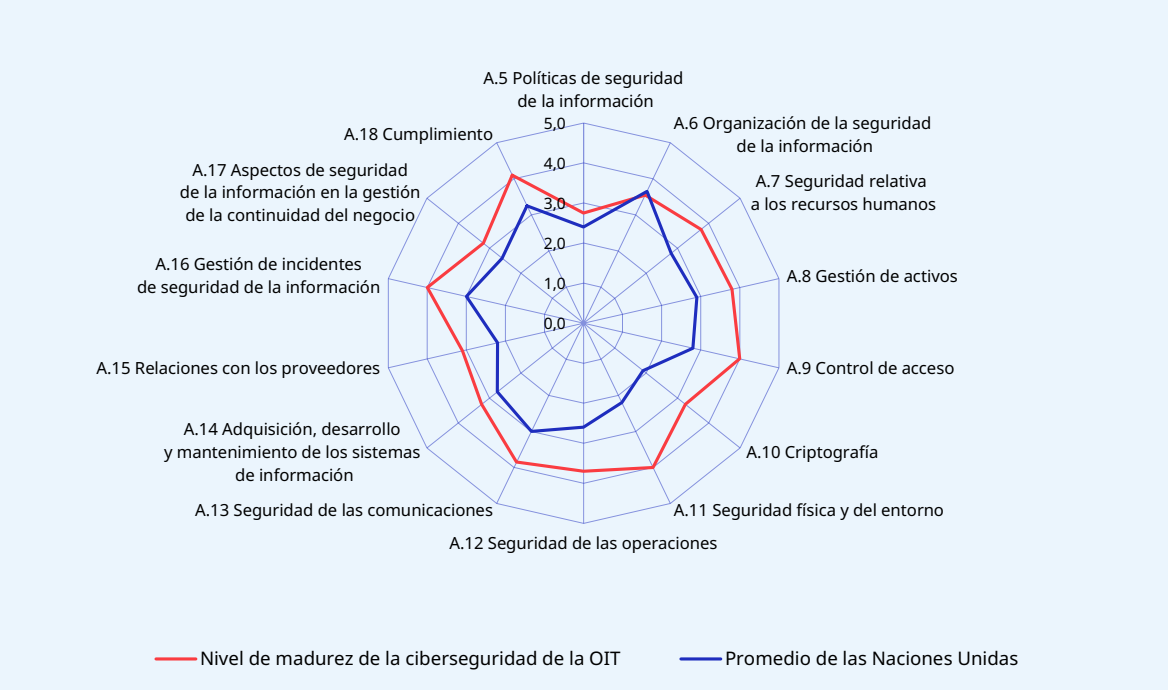
5. El gráfico 2 muestra la madurez de los elementos fundamentales de los procesos de la tecnología de la información de la OIT conforme a los ámbitos establecidos en la versión de 2013 de la norma ISO 27001 (el color del trazado del gráfico no es indicativo del nivel de madurez).

▶ Gráfico 2. Niveles de madurez de la ciberseguridad de la OIT en función de los ámbitos establecidos en la norma ISO 27001



6. En el gráfico 3 se muestran las conclusiones de la OIT en función de los ámbitos de control de la ciberseguridad establecidos en el anexo A de la versión de 2013 de la norma ISO 27001. En el gráfico aparece superpuesta una línea que representa la clasificación media de otras organizaciones del sistema de las Naciones Unidas en que se ha efectuado ese mismo examen, la cual muestra que la OIT supera la media en muchos ámbitos.

▶ Gráfico 3. Niveles de madurez de la ciberseguridad de la OIT en función de los ámbitos de control de la ciberseguridad establecidos en el anexo A de la norma ISO 27001



7. En la evaluación del nivel de madurez de la ciberresiliencia se constató que ya se han aplicado varios de los controles de ciberseguridad de la norma ISO 27001, los cuales se ajustan a las recomendaciones que la DCI formula en su informe. En la evaluación se señalaron asimismo posibilidades de seguir mejorando los controles de ciberseguridad.

8. En el gráfico 4 se muestra el nivel actual de madurez de cada control de ciberseguridad de la OIT. Los controles de ciberseguridad que recibieron la calificación de «conforme» están en sintonía con la norma ISO 27001 sobre mejores prácticas del sector. Aquellos que recibieron la calificación de «parcialmente conforme» están en sintonía, en cierta medida, con la norma ISO 27001, pero existe en ellos un factor por el que, en un proceso de certificación ISO 27001, podrían recibir la calificación de no conformidad leve. Para obtener y mantener la certificación, debería establecerse un plan de mitigación. Los controles de ciberseguridad que reciben la calificación de «no conformes» constituyen una desviación clara de la norma ISO 27001 por la que, en un proceso de certificación ISO 27001, recibirían la calificación de no conformidad grave, y, por ello, exigirían la adopción de medidas prioritarias. Ninguno de los controles de ciberseguridad de la OIT recibió la calificación de «no conforme».

9. En el anexo I de este documento se examina la conformidad de estos controles con los diez pilares de la ciberresiliencia establecidos por la DCI.

▶ Gráfico 4. Conformidad de la OIT con los controles de ciberseguridad establecidos en el anexo A de la norma ISO 27001

Políticas de seguridad de la información	Organización de la seguridad de la información	Seguridad relativa a los recursos humanos	Gestión de activos	Control de acceso	Criptografía	Seguridad física y del entorno	Seguridad de las operaciones	Seguridad de las comunicaciones	Adquisición, desarrollo y mantenimiento de sistemas de información	Relaciones con los proveedores	Gestión de incidentes en seguridad de la información	Gestión de la continuidad del negocio	Cumplimiento
A5.1 Directrices de gestión de la seguridad de la información	A6.1 Organización interna	A7. Antes del empleo	A8.1 Gestión de activos	A9.1 Requisitos de negocio para el control de acceso	A10.1 Controles criptográficos	A11.1 Áreas seguras	A12.1 Procedimientos y responsabilidades operacionales	A13.1 Gestión de la seguridad de las redes	A14.1 Requisitos de seguridad en los sistemas de información	A15.1 Seguridad de la información en las relaciones con proveedores	A16.1 Gestión de los incidentes de seguridad de la información	A17.1 Continuidad de la seguridad de la información	A18.1 Cumplimiento de los requisitos legales y contractuales
	A6.2 Dispositivos móviles y teletrabajo	A7.2 Durante el empleo	A8.2 Clasificación de la información	A9.2 Gestión de acceso de usuario		A11.2 Seguridad de los equipos	A12.2 Protección contra los programas maliciosos (*malware*)	A13.2 Intercambio de información	A14.2 Seguridad en los procesos de desarrollo y soporte	A15.2 Gestión de la prestación de servicios de los proveedores		A17.2 Redundancias	A18.2 Revisiones de la seguridad de la información
		A7.3 Finalización del empleo o cambio en el puesto de trabajo	A8.3 Manipulación de los soportes	A9.3 Responsabilidades del usuario			A12.3 Copias de seguridad		A14.3 Datos de prueba				
				A9.4 Control de acceso a sistemas y aplicaciones			A12.4 Registro y supervisión						
							A12.5 Control del *software* de funcionamiento						
							A12.6 Gestión de la vulnerabilidad						
							A12.7 Auditoría de sistemas de información						

Controles conformes | Controles parcialmente conformes | Controles no conformes | Controles que no se aplican

10. Aunque la evaluación arrojó resultados relativamente positivos, también suministró una lista de recomendaciones que la Oficina podría seguir para seguir mejorando su ciberresiliencia (anexo II). En la medida en que para aplicar dichas recomendaciones sería necesario desviar recursos de la Oficina que se han asignado a otras actividades, se propone centrar la atención en las recomendaciones que presentan más probabilidad de producir los mejores resultados.

11. La Oficina propone que se actualice su plan actual sobre comunicaciones de ciberseguridad a fin de incorporar las recomendaciones que facilitarán la ejecución de una hoja de ruta coherente para mejorar la ciberresiliencia.

12. Cada una de las recomendaciones se examinará más a fondo de manera que puedan valorarse en función del trabajo que requieran y sus posibles efectos. Ulteriormente se presentarán propuestas y costos para establecer prioridades y formular orientaciones al Comité de Gobernanza de la Tecnología de la Información, integrado por altos representantes de las tres carteras de la Oficina. A partir de las decisiones que la Oficina adopte con arreglo a dichas orientaciones, se propone incluir informes de situación en los documentos en que se ofrece información actualizada sobre la Estrategia de Tecnología de la Información de la OIT que se presentan anualmente al Consejo de Administración.

▶ Proyecto de decisión

13. **El Consejo de Administración toma nota de la información contenida en el documento GB.346/PFA/3 y pide a la Oficina que tenga en cuenta sus orientaciones en el seguimiento de las recomendaciones del examen.**

▶ Anexo I

Conformidad con los pilares de ciberresiliencia establecidos por la DCI

Pilar 1. Colaboración con los órganos legislativos y rectores

Orientaciones de la DCI

- Los órganos legislativos y rectores deberían proporcionar orientación estratégica de alto nivel, entre otras formas, mediante la formulación de una declaración explícita de apetito de riesgo.
- Las organizaciones deberían elaborar un marco de presentación de informes que sirva para compilar y difundir parámetros de ciberseguridad entre los órganos legislativos y rectores y para prever protocolos de notificación a niveles jerárquicos superiores que deban aplicarse en caso de un ataque.

Conclusiones

En su informe, la DCI señala diversos ejemplos en las organizaciones del sistema de las Naciones Unidas en que las mejoras introducidas en los marcos de ciberseguridad se basaban en las recomendaciones de supervisión. También se mencionó la colaboración con los órganos legislativos en el seno de la Oficina.

- El puesto de funcionario responsable de la seguridad de la tecnología de la información se creó inicialmente por recomendación del Consejo de Administración.
- Al Consejo de Administración se le mantiene informado de los riesgos de ciberseguridad por diversas vías:
  - o informes sobre auditorías de seguridad de la información a cargo de la Oficina de Auditoría Interna y Control;
  - o informes a cargo del Comité Consultivo de Supervisión Independiente (basados en sesiones informativas ofrecidas por el funcionario principal de seguridad de la información), e
  - o informes específicos de incidentes de ciberseguridad presentados al Comité de Gobernanza de la Tecnología de la Información mediante informes a cargo del Director de los Sistemas de Información, que también se presentan al Consejo de Administración, según proceda.

La Unidad de Servicios de Aseguramiento y Seguridad de la Información ha definido también un conjunto de indicadores de riesgo no exhaustivo. En el documento sobre el marco de gestión de los riesgos de la Oficina se hace una referencia genérica al apetito de riesgo. En la sección relativa al registro estratégico de riesgos de la OIT del Programa y Presupuesto para el bienio 2022-2023 se hace una referencia específica al riesgo de ciberataque contra los sistemas de la OIT (suceso de riesgo 8). Sin embargo, cabe señalar que los parámetros de tolerancia a los riesgos de ciberseguridad definidos para orientar a los equipos operacionales podrían ser más claros.

Recomendaciones

- El Comité de Gobernanza de la Tecnología de la Información debería precisar los niveles aceptables de riesgo para la ciberseguridad basándose en información suministrada por el Consejo de Administración.
- Debería informarse anualmente al Comité de Gobernanza de la Tecnología de la Información sobre problemas habituales de seguridad de la información, tendencias, riesgos y oportunidades a partir del análisis de las tendencias del sector, informes de auditoría, registros de riesgos, evaluaciones de los riesgos para la seguridad de la información, investigaciones y datos de incidentes.

Pilar 2. Incorporación de la ciberseguridad en la gestión de los riesgos de la organización

Orientaciones de la DCI

- Mayor hincapié en la elaboración de medidas de mitigación de riesgos que sean coherentes y eficaces, así como en una sólida planificación de la continuidad de las operaciones.
- Los expertos en ciberseguridad deberían participar plenamente en el diseño, la implementación y el seguimiento de los procesos internos de gestión de riesgos.

Conclusiones

En su informe, la DCI afirma que la incorporación formal de la ciberseguridad en el marco de la gestión institucional de los riesgos contribuye a priorizar esa cuestión entre otras diversas prioridades institucionales. La Oficina ha establecido un sistema de gestión institucional de los riesgos del que se encarga el funcionario principal de gestión de riesgos, que depende de la Oficina del Tesorero y Contralor de Finanzas. El sistema incorpora un registro estratégico de riesgos que comprende el riesgo de perturbación a raíz de un ataque cibernético. Los riesgos para la seguridad de la información también se observan en el nivel operacional; así, el Departamento de Gestión de la Información y de las Tecnologías (INFOTEC) y la Unidad de Servicios de Aseguramiento y Seguridad de la Información también participan en la labor de registro de riesgos. En los registros de riesgos de las oficinas de país también se deja a menudo constancia de ese tipo de riesgos. La gestión institucional de los riesgos presenta, no obstante, algunas limitaciones.

- Cabe suministrar más aclaraciones en el marco del sistema de gestión institucional de los riesgos acerca de los riesgos relacionados con la seguridad de la información.
- La coherencia de las actividades de gestión de los riesgos entre la sede y algunos proyectos financiados con fondos de cooperación para el desarrollo es limitada. Las responsabilidades relativas a la gestión de los riesgos han sido delegadas en cierta medida, y no hay coherencia con respecto a la gestión de los riesgos para la seguridad de la información en los diferentes proyectos de cooperación para el desarrollo.

Recomendación

- Debería fomentarse la integración de la gestión de los riesgos para la seguridad de la información en el sistema de gestión institucional de los riesgos y deberían aplicarse las prácticas de gestión de los riesgos a la gestión de la seguridad de la información para facilitar la priorización de recursos y conseguir así el mayor impacto posible.

  Esta recomendación se repite en el pilar 9.

Pilar 3. Aprovechamiento de la convergencia entre la seguridad física y la ciberseguridad

Orientaciones de la DCI

- Integrar los marcos de gestión de la seguridad física y la ciberseguridad en la arquitectura institucional.
- Ampliar la capacidad en ciberseguridad dentro de la función de seguridad física.

Conclusiones

En su informe, la DCI hace referencia a las líneas difusas entre la seguridad física y la ciberseguridad, ya que los sistemas de tecnologías de la información y de las comunicaciones se utilizan cada vez más para respaldar la seguridad física, y, a veces, los incidentes de seguridad se producen como consecuencia de infracciones en ambas esferas. Pese a las líneas difusas entre ambas, en la Oficina los ámbitos físico y cibernético se siguen tratando generalmente como ámbitos independientes.

- La gestión de la seguridad física corre a cargo del Departamento de Servicios Internos y Administración (INTSERV) de conformidad con las políticas del sistema de gestión de la seguridad de las Naciones Unidas.
- La gestión de la ciberseguridad corre a cargo de la Unidad de Servicios de Aseguramiento y Seguridad de la Información, de conformidad con la norma ISO 27001.

Cada equipo ha aplicado diversos controles a sus respectivos ámbitos e INTSERV colabora con INFOTEC para apoyar los controles de identidad y acceso. Se ha observado una deficiencia, derivada de la convergencia de ámbitos y un grado relativamente bajo de experiencia en ciberseguridad en el seno del equipo de INTSERV, a saber, que en lo que respecta a la red de dispositivos en el ámbito de internet de las cosas [1] que da apoyo a la seguridad física no se ha evaluado la conformidad con las normas de ciberseguridad.

Recomendación

- Debería efectuarse una evaluación de los riesgos y una prueba de seguridad de la red de internet de las cosas.

[1] La red operacional integrada por sensores y dispositivos que automatizan y gestionan algunas de las operaciones diarias del funcionamiento de los bienes e instalaciones de la OIT.

Pilar 4. Configuración de marcos reguladores para el cumplimiento y la rendición de cuentas

Orientaciones de la DCI

- 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.
- Reforzar la responsabilidad individual en incidentes causados por una ciberhigiene deficiente. Elaborar un sistema más matizado para afrontar los casos de infracción de ciberseguridad de manera proporcional con la gravedad de la infracción, a fin de animar a los usuarios a que asuman su responsabilidad por ejercer prácticas arriesgadas.

Conclusiones

En su informe, la DCI señala que en los documentos de orientación procedimental, técnica, de política, y estratégica deberían incluirse referencias a la ciberseguridad, práctica que se observó en la OIT durante la evaluación del nivel de madurez en ciberresiliencia.

- La Unidad de Servicios de Aseguramiento y Seguridad de la Información menciona la norma ISO 27001 como parte del sistema de gestión de la seguridad de la información que se ha aplicado.
- La serie de documentos sobre el sistema de gestión de la seguridad de la información abarca diversos ámbitos de control técnico. Sin embargo, algunos de los documentos podrían revisarse con mayor frecuencia y algunas de las partes interesadas entrevistadas parecen tener dificultades para entenderlos. Hay algunas discordancias en lo que respecta a la estimación por parte del personal del valor de los datos y la gravedad de las infracciones cibernéticas, lo que ha dado lugar a una falta de coherencia en la aplicación de los controles y los procesos de ciberseguridad en la Organización. Además, se ha señalado que las recomendaciones relativas a la evaluación de la seguridad de la información no se aplican siempre con el mismo rigor que en el caso de las recomendaciones de auditoría.
- En la OIT se aplican los procedimientos disciplinarios habituales que se utilizan en los departamentos de recursos humanos de las organizaciones del sistema de las Naciones Unidas para sancionar a los miembros del personal que incumplen las políticas y las normas; no obstante, durante la pandemia, las actividades de concienciación en materia de seguridad han sido irregulares. Será necesario volver a instaurar estas actividades con regularidad para fomentar la concienciación de las responsabilidades individuales.
- Los encargados de algunos sistemas, incluidos los de proyectos de cooperación para el desarrollo, han optado por no dar cumplimiento a las políticas y normas de seguridad de la información establecidas por la Unidad de Servicios de Aseguramiento y Seguridad de la Información.
- La OIT dispone de algunos mecanismos para gestionar y tramitar denuncias de faltas graves y un marco de protección para los funcionarios que denuncian irregularidades, pero generalmente dichos mecanismos no se ocupan de las denuncias presentadas en el contexto de la ciberseguridad. Existe también una función de control y de respuesta en caso de incidente, pero se centra principalmente en incidentes de seguridad en el ámbito de la tecnología.

Recomendaciones

- Debería elaborarse un programa que abarque a toda la Organización para fomentar una cultura de seguridad de la información de la OIT, el cual debería constar de:
  - medidas que el personal directivo superior pueda adoptar que sirvan de pauta de las buenas prácticas en materia de ciberseguridad;
  - comunicaciones específicas formuladas en un lenguaje no técnico y atractivo para que todos los públicos puedan comprender las consecuencias de una conducta cibernética arriesgada;
  - formación en sensibilización sobre la seguridad de la información adaptada a diferentes funciones, y
  - controles de rendición de cuentas que establezcan responsabilidades individuales precisas para mantener unos buenos niveles de ciberhigiene.

  Las conclusiones que figuran en los pilares 6, 7 y 8 también dieron lugar a esta recomendación.

- Deberían elaborarse guías y listas sobre riesgos para la seguridad a fin de ayudar a los directivos de los proyectos de cooperación para el desarrollo a proteger sus datos y sistemas teniendo en cuenta el apetito de riesgo acordado. Deberían incorporarse controles de seguridad (y establecerse parámetros mínimos de seguridad) en los marcos de adquisición, desarrollo y mantenimiento de los sistemas.

  Las conclusiones que figuran en el pilar 7 también dieron lugar a esta recomendación.

Pilar 5. Aprovechamiento de las aportaciones de los mecanismos de supervisión

Orientaciones de la DCI

- Elaborar procedimientos que aseguren que los conocimientos y la experiencia de los expertos en ciberseguridad de una organización puedan orientar la labor de la función de supervisión y contribuir a ella sistemáticamente.

Conclusiones

En el informe de la DCI se ofrecen varios ejemplos de casos en que las mejoras introducidas en la ciberseguridad se basan en las recomendaciones de supervisión, lo que pone de relieve el valor de tales recomendaciones. La Oficina mantiene las funciones de supervisión, incluidas las que se describen más adelante.

- La supervisión operacional se efectúa mediante el seguimiento de los indicadores clave de riesgos, la investigación de incidentes, la presentación de informes y el marco de gestión de riesgos de la Unidad de Servicios de Aseguramiento y Seguridad de la Información.

- La supervisión estratégica se lleva a cabo mediante exámenes de la gestión a cargo del Comité de Gobernanza de la Tecnología de la Información, exámenes a cargo del Director de los Sistemas de Información del plan de trabajo de la Unidad de Servicios de Aseguramiento y Seguridad de la Información y los exámenes del Consejo de Administración de los informes de estrategia y auditoría, de evaluación y de supervisión de la tecnología de la información. Si bien la Unidad de Servicios de Aseguramiento y Seguridad de la Información contribuye con frecuencia en estas funciones de supervisión estratégica, no

existen procedimientos operativos documentados para garantizar una colaboración coherente y eficaz con dicha unidad durante la ejecución de esos exámenes.

- Las auditorías independientes corren a cargo de:
  - auditores externos: se ha contratado a un auditor independiente para facilitar la certificación ISO 27001 del sistema de gestión de la seguridad de la información; sin embargo, la seguridad de la información de los sistemas de tecnologías de la información y las comunicaciones que no gestiona la Unidad de Servicios de Aseguramiento y Seguridad de la Información no entra en el ámbito de la auditoría, y
  - auditores internos: la Oficina de Auditoría Interna y Control efectúa dos o tres auditorías de seguridad de la información al año. Los ámbitos de auditoría se determinan utilizando un enfoque basado en el riesgo. Además, tanto la Oficina de Auditoría Interna y Control como los consultores externos llevan a cabo auditorías de pruebas de penetración. La última de dichas auditorías se efectuó en 2019 y está previsto llevar a cabo otra en 2022.

Recomendación

- Deberían elaborarse y supervisarse nuevos indicadores clave de desempeño para medir la eficacia de los controles de ciberseguridad y la gestión de las actividades destinadas a corregir las fallas.

Pilar 6. Fomento de una cultura de ciberseguridad desde la dirección

Orientaciones de la DCI

- Asegurar que la dirección sea consciente de los riesgos y las implicaciones asociados a la inacción y una ciberhigiene deficiente.
- Fomentar una cultura en que los incidentes ocurridos se consideren como un punto de partida para abordar un problema común y proteger mejor la organización, y no como un fracaso.

Conclusiones

En su informe, la DCI señala que la sensibilización y la rendición de cuentas de la dirección ejecutiva constituyen un punto de partida, y que el propio personal directivo debe fomentar el reconocimiento de los errores y las vulnerabilidades.

El equipo directivo de la Oficina está informado de los riesgos y problemas de ciberseguridad mediante diversas vías de comunicación (como se ha señalado anteriormente en relación con el pilar 5). El compromiso del personal directivo ha quedado demostrado desde una perspectiva estratégica mediante la creación de la Unidad de Servicios de Aseguramiento y Seguridad de la Información; la prestación de apoyo para la certificación del sistema de gestión de la seguridad de la información, y el apoyo de políticas, normas y procedimientos de ciberseguridad.

Pese a la constitución de la Unidad de Servicios de Aseguramiento y Seguridad de la Información y de equipos de apoyo (por ejemplo, en los ámbitos de la gestión institucional de los riesgos, la continuidad de las operaciones, la gobernanza de la tecnología de la información y la auditoría y supervisión internas), todavía se detectan en la Oficina limitaciones que repercuten en su situación en materia de ciberseguridad.

Por otra parte, si bien el personal directivo apoya también medios no monetarios para incidir en la cultura y las conductas en materia de ciberseguridad mediante campañas de simulación de suplantación de la identidad y participa activamente en iniciativas de ciberseguridad (por ejemplo, en auditorías externas), siempre es posible seguir introduciendo mejoras mediante la participación visible en otros programas de concienciación.

Recomendaciones

- Debería llevarse a cabo un examen integral de los recursos y las responsabilidades en materia de seguridad de la información en toda la Organización, a fin de mejorar el cumplimiento de los actuales controles de seguridad y garantizar una mayor coherencia entre la seguridad de la información y la gestión de los riesgos.

  Las conclusiones que figuran en el pilar 9 también dieron lugar a esta recomendación.

- Debería elaborarse un programa que abarque a toda la Organización para fomentar una cultura de seguridad de la información en la OIT, como se señala en la recomendación que figura en el pilar 4.

Pilar 7. Aplicación de un enfoque que abarque a toda la organización

Orientaciones de la DCI

- Descentralizar y delegar responsabilidades en el personal directivo intermedio.
- Definir las responsabilidades en materia de ciberseguridad de todas las funciones e impartir formación en ciberseguridad específica de cada función y llevar a cabo actividades de sensibilización.

Conclusiones

En su informe, la DCI reitera que hay cada vez mayor conciencia de que la ciberseguridad no es un asunto que incumba únicamente a la tecnología de la información, lo cual ha quedado ampliamente reconocido con la asignación de responsabilidades sobre seguridad de la información más allá de la Unidad de Servicios de Aseguramiento y Seguridad de la Información y de INFOTEC; sin embargo, todavía existen algunas limitaciones con respecto a la descentralización de responsabilidades en la Oficina.

- En los procedimientos de trabajo de los equipos no se tienen en cuenta las consideraciones de ciberseguridad. Por ejemplo:
  - la incorporación de controles de ciberseguridad en los procedimientos de gestión de programas y proyectos es limitada, es decir que los controles de seguridad no se adoptan de manera coherente en los diferentes proyectos y equipos, y
  - los procesos de ciberseguridad no se aplican de manera coherente en las oficinas de país.
- Se imparte una formación mínima en ciberseguridad por funciones a todo el personal.

Recomendaciones

- Debería elaborarse un programa que abarque a toda la Organización para fomentar una cultura de seguridad de la información en la OIT, como se señala en la recomendación que se formula en el pilar 4.
- Deberían elaborarse guías y listas sobre riesgos para la seguridad a fin de ayudar a los directivos de proyectos de cooperación para el desarrollo, como se señala en la recomendación que se formula en el pilar 4.

Pilar 8. Establecimiento de una primera línea de defensa basada en el personal

Orientaciones de la DCI

- Establecer una alfabetización digital básica de todos los miembros del personal y capacitar a los usuarios para que desempeñen un papel activo en la mejora de la ciberresiliencia.
- Elaborar un programa de formación y sensibilización con objetivos claros para cada categoría de interesados en función de los riesgos que puedan presentar para la organización.

Conclusiones

Cada vez hay más conciencia de la importancia que reviste el «factor humano» en la ciberseguridad, y en todo el mundo se reconoce que los usuarios finales individuales son, con creciente frecuencia, el blanco de ataques. La Oficina entiende que es necesario que los usuarios mantengan una vigilancia suficiente como primera línea defensiva; por ello, actualmente es obligatorio para todo el personal cursar la formación inicial que incorpora la sensibilización en seguridad de la información. Otras actividades específicas relativas a comunicaciones y sensibilización (por ejemplo, campañas de simulación de suplantación de la identidad, conforme al pilar 6, y la difusión de avisos sobre amenazas cibernéticas) contribuyen a mejorar la atención de los usuarios.

Hay, no obstante, limitaciones que pueden afectar a los niveles de vigilancia.

- Se ha registrado un alto índice de miembros del personal que han completado la formación inicial, pero ese dato no aporta las garantías suficientes de que se esté produciendo realmente un cambio de conducta.
- No se imparte regularmente formación de sensibilización ni formación basada en las distintas funciones a todo el personal (conforme a los pilares 4 y 7).

Recomendación

- Debería elaborarse un programa que abarque a toda la Organización para fomentar una cultura de seguridad de la información en la OIT, como se señala en la recomendación que se formula en el pilar 4.

Pilar 9. Optimización de la asignación de recursos financieros para la ciberseguridad

Orientaciones de la DCI

- Determinar a qué esferas deberían asignarse recursos de ciberseguridad para conseguir el impacto más decisivo.
- Vincular las inversiones en ciberseguridad con las necesidades institucionales y con prácticas sólidas de gestión de riesgos para evitar tanto el exceso de inversión como la falta de recursos en esferas fundamentales para la continuidad de las operaciones.

Conclusiones

En su informe, la DCI reconoce que, pese al aumento de los recursos asignados a la ciberseguridad, la insuficiencia de recursos que se ha puesto de manifiesto sigue impidiendo que se abarquen todos los aspectos de la ciberresiliencia. Las conversaciones con el personal directivo superior de la OIT indican que si no se dispone de los recursos adecuados, no será posible avanzar en las diferentes actividades que contribuyen a las deficiencias de ciberseguridad en varias esferas, como la gestión de activos y de la vulnerabilidad, la gestión de proyectos de cooperación para el desarrollo, la gestión de datos y el control de algunos aspectos de la gestión de la seguridad de la información.

Recomendaciones

- Debería llevarse a cabo un examen integral de los recursos y las responsabilidades en materia de seguridad de la información en toda la Organización, como se señala en la recomendación que se formula en el pilar 4.
- Debería fomentarse la integración de la gestión de los riesgos para la seguridad de la información en el sistema de gestión institucional de los riesgos y deberían aplicarse las prácticas de gestión de los riesgos a la gestión de la seguridad de la información para facilitar la priorización de recursos y conseguir así el mayor impacto posible (recomendación que se formula en el pilar 2).

Pilar 10. Inversión en recursos humanos dedicados y especializados

Orientaciones de la DCI

- Mantener la capacidad interna de expertos en ciberseguridad [2].

Conclusiones

Muchas organizaciones del Sistema de las Naciones Unidas, entre ellas la OIT, han establecido una capacidad interna de recursos humanos especializados en ciberseguridad.

- La Oficina ha nombrado, a tiempo completo, a un funcionario principal de seguridad de la información que dirige el equipo de la Unidad de Servicios de Aseguramiento y Seguridad de la Información, integrado por expertos en ciberseguridad. Las responsabilidades del equipo han ido evolucionando con el tiempo y actualmente conciernen tanto a los servicios de operaciones de seguridad como a la gobernanza de seguridad.

[2] Deben evitarse los conflictos de intereses en los casos en que el equipo que presta servicios de supervisión deba ser distinto e independiente del equipo responsable de los servicios de ciberseguridad.

- La Unidad de Servicios de Aseguramiento y Seguridad de la Información también contrata a expertos en ciberseguridad externos para que presten servicios adicionales de seguridad de la información, como servicios de información sobre amenazas y control de la seguridad y servicios de respuesta a incidentes y pruebas de penetración [3].

En su informe, la DCI subraya 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 adopción de decisiones, con independencia de la posición que ocupe la ciberseguridad en el organigrama, ya sea en el departamento de las tecnologías de la información y de las comunicaciones o en una estructura independiente de él.

No se imponen restricciones al Director de los Sistemas de Información ni a la Unidad de Servicios de Aseguramiento y Seguridad de la Información en lo que respecta a que comuniquen sus opiniones sobre ciberseguridad a los responsables de la adopción de decisiones, si bien puede existir un margen para mejorar la forma en que las consideraciones en materia de ciberseguridad pueden contribuir a otros marcos institucionales, como la gestión institucional de los riesgos, la gestión de la información y el conocimiento, la seguridad y protección física y la supervisión.

[3] Una empresa externa se ocupa de la gestión del Centro de Operaciones de la Red y del Centro de Operaciones de Seguridad de la Oficina.

▶ Anexo II

Hoja de ruta para la mejora de la ciberresiliencia

Pilar de la DCI	Recomendación
1	El Comité de Gobernanza de Tecnología de la Información debería precisar los niveles aceptables de riesgo para la ciberseguridad basándose en los datos suministrados por el Consejo de Administración.
1	Debería informarse anualmente al Comité de Gobernanza de Tecnología de la Información sobre cuestiones comunes, tendencias, riesgos y oportunidades relativos a la seguridad de la información a partir de análisis de tendencias en el sector, informes de auditoría, registros de riesgos, evaluaciones de los riesgos para la seguridad de la información, investigaciones y datos de incidentes.
2, 9	Debería fomentarse la integración de la gestión de los riesgos para la seguridad de la información en el sistema de gestión institucional de los riesgos y deberían aplicarse las prácticas de gestión de los riesgos a la gestión de la seguridad de la información para facilitar la priorización de los recursos a fin de conseguir el mayor impacto posible.
3	Debería efectuarse una evaluación de los riesgos y una prueba de seguridad de la red de internet de las cosas.
4, 6, 7, 8	Debería elaborarse un programa que abarque a toda la Organización para fomentar una cultura de seguridad de la información en la OIT.
4, 7	Deberían elaborarse guías y listas sobre riesgos para la seguridad a fin de ayudar a los directivos de proyectos de cooperación para el desarrollo a proteger sus datos y sistemas.
5	Deberían elaborarse y supervisarse indicadores clave de desempeño para medir la eficacia de los controles de ciberseguridad y la gestión de las actividades encaminadas a corregir las fallas.
6, 9	Debería llevarse a cabo un examen integral de los recursos y las responsabilidades en materia de seguridad de la información en toda la Organización.