Naciones Unidas A/77/88/Add.1

Asamblea General

Distr. general
7 de junio de 2022
Español
Original: inglés

**Septuagésimo séptimo período de sesiones**
Tema 145 de la lista preliminar*
**Dependencia Común de Inspección**

# Examen de la ciberseguridad en las organizaciones del sistema de las Naciones Unidas

## Nota del Secretario General

El Secretario General tiene el honor de transmitir a los miembros de la Asamblea General sus observaciones y las de la Junta de los Jefes Ejecutivos del Sistema de las Naciones Unidas para la Coordinación sobre el informe de la Dependencia Común de Inspección titulado “La ciberseguridad en las organizaciones del sistema de las Naciones Unidas” (véase A/77/88).

* A/77/50.

22-08682 (S) 160622 220622

# I. Introducción

1. En el informe de la Dependencia Común de Inspección titulado “La ciberseguridad en las organizaciones del sistema de las Naciones Unidas” (véase A/77/88), la Dependencia presenta su examen de la ciberseguridad en las organizaciones del sistema de las Naciones Unidas, cuyos principales objetivos 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).

# II. Observaciones generales

2. Las organizaciones acogen con beneplácito el informe y sus conclusiones, que tienen el potencial de mejorar la posición de ciberseguridad del sistema de las Naciones Unidas. Además, valoran el hecho de que el examen promueva: a) un enfoque basado en el riesgo institucional que va más allá del enfoque tradicional, centrado en la tecnología de la información y la comunicación; b) el punto de vista y los procesos internos de las entidades; y c) un fuerte apoyo a un nivel básico común y compartido de medidas y protección de la seguridad en todo el sistema de las Naciones Unidas, con el fin de reducir la brecha de madurez entre las entidades y mejorar la ciberresiliencia en todo el sistema de las Naciones Unidas.

3. Las organizaciones apoyan las recomendaciones formuladas en el examen.

# III. Observaciones sobre recomendaciones específicas

**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.**

4. Las organizaciones apoyan esta recomendación.

5. En algunas entidades, los mecanismos de información periódica existentes en materia de gobernanza sobre ciberseguridad podrían satisfacer ya las necesidades subyacentes a la recomendación, por ejemplo, mediante la presentación de informes a los órganos rectores, los comités de auditoría y supervisión, las juntas internas de tecnología de la información a nivel institucional y las juntas consultivas de expertos externos en tecnología.

6. A la hora de elaborar los informes recomendados, las entidades subrayan la importancia de garantizar que estos documentos públicos no proporcionen ningún detalle que pueda reconocer información específica sobre la detección de ataques y las capacidades de detección de las respectivas organizaciones o que proporcione

información que un posible adversario pueda aprovechar para aumentar la probabilidad de éxito de ataques específicos.

**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.**

7. Las organizaciones señalan que esta recomendación está dirigida a los órganos legislativos y rectores.

8. La orientación estratégica prevista debe tener en cuenta que se necesitarán recursos adicionales para reforzar las medidas locales de seguridad y facilitar la colaboración con el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas (CICE).

**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.**

9. Las organizaciones señalan que esta recomendación está dirigida a la Dirección del CICE.

10. Las entidades de menor tamaño que carezcan de recursos y competencias en materia de ciberseguridad podrían beneficiarse de los servicios compartidos adicionales y específicos que desarrollaría el CICE. Las entidades que trabajan a través de alianzas público-privadas en la ejecución de programas digitales de desarrollo y humanitarios están deseosas de seguir recibiendo el apoyo directo de los Estados Miembros para la ejecución de sus programas digitales, incluidos los aspectos relacionados con su ciberseguridad, y en ese sentido algunas entidades interpretan que el alcance de esta recomendación abarca la posición de ciberseguridad interna de sus oficinas en todo el mundo y la posición y los riesgos de ciberseguridad relacionados con el trabajo externo con asociados público-privados.

11. Si se aplica esta recomendación, algunas organizaciones miembros del CICE señalan que prevén desempeñar un papel en los debates sobre la gobernanza, la financiación y la aplicación del fondo fiduciario y el acceso a él, incluso mediante la participación en el contexto de la Red Digital y Tecnológica, antes de que se finalice cualquier propuesta.

**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.**

12. Las entidades señalan que esta recomendación se dirige a la Asamblea General y reiteran los comentarios formulados en respuesta a la recomendación 3.

**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.**

13. Las organizaciones señalan que esta recomendación está dirigida al Secretario General.

14. La Secretaría de las Naciones Unidas ya ha iniciado ese proceso. Además de la colaboración informal y *ad ho*c entre la Oficina de Tecnología de la Información y las Comunicaciones y el Departamento de Seguridad, este último es miembro de la recientemente creada red híbrida de respuesta a ciberataques. Además, en el marco del plan de inversiones de capital destinadas a las operaciones de tecnología de la información y las comunicaciones, se considerarán las inversiones necesarias para reforzar las estructuras, el personal, los activos y los servicios existentes, con miras a aprovechar la convergencia entre la seguridad física y la ciberseguridad.

15. En cuanto a la convergencia de las funciones de seguridad física y de ciberseguridad, algunas organizaciones ven un posible conflicto en la redacción del párrafo 164 del informe. Aunque los Inspectores reconocen que la dependencia de seguridad física no debe absorber las funciones de ciberseguridad, proceden a recomendar la convergencia, lo que podría crear una situación en los distintos organismos que podría dar lugar precisamente al resultado que los Inspectores no recomiendan. Dichas organizaciones sugieren que se haga hincapié en que las funciones de ciberseguridad no deben ser absorbidas por las dependencias de seguridad física.

16. Aunque existe una colaboración permanente entre el Departamento y la Oficina en materia de ciberseguridad, cabe señalar que la Oficina tendrá el papel director y que la función y los recursos del Departamento se limitarán a garantizar la seguridad física del personal y los locales de las Naciones Unidas, dado que la ciberseguridad no es de su competencia. Esta alianza se activa cuando se trata de ciberataques híbridos[1] contra las Naciones Unidas, en cuyo caso el Departamento y la Oficina colaboran en la realización de evaluaciones de los riesgos para la seguridad y en la elaboración y aplicación de recomendaciones relativas a medidas preventivas y de mitigación.

[1] En este contexto, el ciberataque híbrido puede describirse como el uso de la tecnología digital o de un ataque físico contra la infraestructura de tecnología de la información para causar un daño deliberado a los programas y actividades de las Naciones Unidas que da lugar a una importante vulnerabilidad de la seguridad física en las instalaciones de las Naciones Unidas o a un mayor riesgo de que los miembros del personal sufran algún daño.