Organización de las Naciones Unidas para el Desarrollo Industrial

Distr. general
20 de septiembre de 2024
Español
Original: inglés

**Junta de Desarrollo Industrial**
**52º período de sesiones**
Viena, 25 a 27 de noviembre de 2024
Tema 4 f) del programa provisional
**Gestión general de riesgos**

# Información actualizada sobre la gestión general de riesgos

## Informe del Director General

En su conclusión 2016/8, el Comité de Programa y de Presupuesto "invitó al Director General a que en los siguientes períodos de sesiones de la Junta de Desarrollo Industrial y del Comité de Programa y de Presupuesto informara acerca de la estrategia general de gestión de riesgos de la ONUDI y sugiriera medidas amplias para hacer frente a las consecuencias financieras y administrativas de que Estados Miembros abandonaran la Organización, entre otras cosas, con miras a revertir la tendencia a la retirada".

El presente documento ofrece información actualizada con respecto al informe presentado en el 40º período de sesiones del Comité (IDB.52/9-PBC.40/9), destacándose la creación de una nueva Dependencia de Gestión de Riesgos y Cumplimiento, dependiente de la Dirección de Servicios y Operaciones Institucionales, que incluye funciones adicionales relacionadas con la ciberseguridad.

# I. Introducción

1. Con la promulgación de la estructura ajustada de su Secretaría para 2024 (DGB/2024/03), la ONUDI estableció la Dependencia de Gestión de Riesgos y Cumplimiento. La nueva dependencia presta apoyo al Director Gerente de la Dirección de Servicios y Operaciones Institucionales, en su calidad de coordinador designado de la gestión de los riesgos institucionales de la ONUDI, para seguir desarrollando, coordinando y ejecutando los marcos de gestión de los riesgos institucionales y de seguridad de la información de la ONUDI. También apoya activamente al personal directivo superior para fomentar una cultura robusta en lo que respecta a los riesgos. Además de las funciones de gestión de riesgos y cumplimiento, el mandato de la Dependencia está relacionado con la gobernanza de la ciberseguridad.

2. En este documento se destacan las medidas adoptadas por la ONUDI para gestionar y reducir la amenaza de riesgos en lo que respecta a la de ciberseguridad.

# II. Marco y mejoras de la ciberseguridad

3. En respuesta a la recomendación de la Dependencia Común de Inspección (DCI) contenida en su informe titulado “La ciberseguridad en las organizaciones del sistema de las Naciones Unidas” (JIU/REP/2021/3), la ONUDI presenta una sinopsis de las medidas aplicadas en relación con su marco de ciberseguridad. En la sinopsis, contenida en el documento de sesión IDB.52/CRP.14, se describen los elementos críticos y las medidas adoptadas para proteger a la Organización de las ciberamenazas y garantizar la ejecución de prácticas de seguridad robustas.

4. La ONUDI ha hecho progresos sustanciales en el fortalecimiento de su marco de ciberseguridad, que ha ajustado a las recomendaciones del Auditor Externo, la DCI y las mejores prácticas del sector. La Organización ha establecido una sólida base de ciberseguridad mediante la definición del marco de gobernanza y el establecimiento del sistema de gestión de la seguridad de la información (que se ajusta a la norma ISO 27001) a través de la Política de Seguridad de la Información de la ONUDI (DGB/2023/01), así como de la Instrucción Administrativa sobre el Proceso de Gestión de Riesgos para la Seguridad de la Información (AI/2024/01), que describe el proceso para garantizar que los riesgos para la seguridad de la información se detecten, evalúen, gestionen y mitiguen de manera eficaz, oportuna y estructurada.

5. A medida que la ONUDI avanza, es crucial mantener un enfoque proactivo de la ciberseguridad. Esto incluye reevaluar continuamente los riesgos, mejorar las capacidades técnicas y fomentar una cultura de concienciación sobre la ciberseguridad en toda la Organización. Gracias a esos esfuerzos, la ONUDI no solo estará preparada para hacer frente a las cambiantes ciberamenazas y salvaguardar sus activos de información, sino también para apoyar su misión más amplia con resiliencia y confianza.

6. En el informe del Auditor Externo sobre las cuentas de la ONUDI correspondientes al ejercicio económico comprendido entre el 1º de enero y el 31 de diciembre de 2023 (IDB.52/4-PBC.40/4), presentado en el 40º período de sesiones del Comité de Programa y de Presupuesto, el Auditor Externo validó los progresos de la ONUDI en materia de ciberseguridad al dar por cumplidas las cinco recomendaciones, centradas en el establecimiento de una función dedicada a la ciberseguridad, el desarrollo del Sistema de Gestión de la Seguridad de la Información y la ejecución de un proceso de gestión de la vulnerabilidad. También se abordaron y corrigieron vulnerabilidades técnicas críticas identificadas por el Auditor Externo, y una prueba de penetración de la seguridad dirigida en 2023 por la ONUDI con el apoyo de empresas externas especializadas reveló problemas adicionales que se incluyeron en el plan de trabajo de los Servicios de Digitalización, Innovación y Optimización de la Cooperación Técnica. En una evaluación de riesgos para la seguridad de la información realizada en 2023 también se identificaron activos y riesgos clave, lo que dio lugar a un exhaustivo plan de tratamiento de riesgos para la seguridad de la información correspondiente a 2023-2024, que incluye 35 actividades, de las cuales 15 se concluyeron y las restantes están en curso. En el anexo de este documento se presenta un panorama general de alto nivel de esas actividades. Los resultados confirman la eficacia de la función de ciberseguridad de la ONUDI en la detección y gestión proactivas de los riesgos, así como en la mejora de la seguridad y la resiliencia de la Organización.

7. El presente documento se complementa con el documento de sesión IDB.52/CRP.14, en el que se describen los procesos que contribuyen a mejorar la ciberresiliencia de la Organización.

# III. Medidas que se solicitan a la Junta

8. La Junta tal vez desee tomar nota de la información que figura en el presente documento.

# Anexo

## Estado de las actividades del plan de tratamiento de riesgos para la seguridad de la información 2023-2024

**Actividades concluidas**

1. Pruebas de penetración: Se contrató a un contratista externo para realizar pruebas de penetración exhaustivas en las que simulara ser un atacante con acceso interno. Esto llevó a perfeccionar los controles y a incluir nuevas actividades en el plan de tratamiento de riesgos.

2. Establecimiento de la autenticación moderna en Exchange Online: Se estableció la autenticación moderna en Exchange Online con el fin de mejorar la seguridad del correo electrónico.

3. Desmantelamiento del sistema de intercambio de archivos xFiles: Se desmanteló con éxito el antiguo sistema de intercambio de archivos de la ONUDI y se introdujo una solución de intercambio moderna basada en Microsoft 365 (OneDrive), lo que redujo la superficie de ataque.

4. Mejora de la autenticación para Microsoft Teams: Se estableció la autenticación multifactor para Teams a fin de mitigar los riesgos de robo de credenciales.

5. Mejora de las políticas de contraseñas: Se desarrollaron y aplicaron nuevos procedimientos que abarcan políticas de contraseñas exhaustivas, aprovisionamiento y supervisión del cumplimiento.

6. Mejora de la autenticación, la experiencia de los usuarios y la seguridad: Se llevó a cabo la transición al inicio de sesión único (SSO) basado en Microsoft 365 Azure AD, mejorando así la supervisión, la resiliencia y la disponibilidad.

7. Establecimiento de la autenticación multifactor para los sistemas de nube: Se habilitó la autenticación multifactor para todos los servicios que utilizan autenticación en nube para reforzar la seguridad.

8. Herramienta y proceso de gestión de vulnerabilidades: Se introdujo una herramienta de gestión de vulnerabilidades que cubre recursos críticos como los sistemas de cara al público, los servidores críticos y las estaciones de trabajo de los administradores. También se elaboraron un proceso y un procedimiento adicionales, conforme a las recomendaciones del Auditor Externo y las mejores prácticas.

9. Mejora de la supervisión del cumplimiento: Se mejoró la supervisión del cumplimiento de los controles clave de ciberseguridad, en consonancia con la base de referencia de las Naciones Unidas y las mejores prácticas de Microsoft.

10. Mejora de la seguridad de los sistemas de Microsoft 365: Se estableció Seamless SSO para determinados sistemas de Microsoft 365, lo que mejoró la experiencia de los usuarios y la seguridad.

11. Formación interna específica para administradores de tecnologías de la información (TI): Se impartió formación cruzada interna para administradores de TI y se ofrecieron cursos especializados para usuarios privilegiados.

12. Revisión del almacenamiento de archivos de las oficinas sobre el terreno: Se realizó una revisión de los permisos y se evaluó la posibilidad de migrar a Teams los archivos compartidos en las oficinas sobre el terreno para mejorar la seguridad.

13. Mejora de los procesos y políticas de seguridad: Se mejoraron los procesos y políticas relacionados con los derechos de acceso, la segregación de funciones y las configuraciones seguras, reduciendo así las desviaciones de las prácticas estándar.

14. Optimización de los procesos de seguridad de la información: Se adoptaron y adaptaron las mejores prácticas actuales en materia de seguridad de la información para optimizar la postura de seguridad de la Organización.

15. Revisión de la seguridad de Teams: Se revisaron la configuración de seguridad y los permisos de Teams.

**Actividades en curso**

16. Revisión de las cuentas para garantizar que solo se conceda acceso a quien estrictamente lo necesite y según el principio del menor privilegio: Se siguen revisando las cuentas de usuarios privilegiados y las cuentas de servicio, los derechos de acceso al intercambio de archivos y la aplicación de medidas como la solución de la contraseña de administrador local.

17. Introducción de la protección de credenciales: Se está introduciendo la función de seguridad Credential Guard tanto en los servidores como en los terminales para mejorar la seguridad y reducir el riesgo de que las credenciales se vean comprometidas.

18. Aplicación de las políticas más recientes de contraseñas en toda la ONUDI: Actualización de las políticas de contraseñas y de acceso privilegiado sobre la base de los procedimientos actualizados de la política de contraseñas.

19. Mejoras en la gestión de parches: Se están realizando esfuerzos para perfeccionar la gestión de parches y los procesos de corrección.

20. Mejora de la seguridad de SAP: Se están aplicando medidas para abordar las constataciones de las auditorías y mejorar la higiene de la seguridad en el sistema SAP.

21. Mejoras en el cortafuegos: Se están realizando mejoras que incluyen la instauración de la confianza cero y una revisión completa de la arquitectura, la gestión y las políticas de seguridad del cortafuegos.

22. Sustitución de la herramienta de gestión de contraseñas para los administradores de TI: Se está en proceso de sustituir la anticuada herramienta de gestión de contraseñas para los administradores de TI.

23. Evaluación de la madurez de la confianza cero: Se está llevando a cabo una evaluación exhaustiva de la madurez de la confianza cero para orientar futuras mejoras.

24. Desmantelamiento/reemplazo de los sistemas heredados: Se ha emprendido el desmantelamiento y reemplazo de los sistemas heredados a fin de reducir la superficie de ataque.

25. Mejora de la respuesta a los incidentes de seguridad: Se están reforzando los procesos y herramientas de respuesta a incidentes con recursos internos y externos.

26. Supervisión de los controles clave de SAP: En consonancia con las recomendaciones del Auditor Externo, se está procediendo a supervisar el cumplimiento de los controles clave en SAP y los procesos de apoyo.

27. Segregación de las funciones de TI para el sistema de planificación de los recursos institucionales: La mejora de la segregación de las funciones de TI para SAP está en curso en la medida en que los recursos lo permiten y en consonancia con las recomendaciones del Auditor Externo.

28. Cuentas personalizadas para administradores: Se está avanzando en la creación de cuentas personalizadas y separadas para administradores de TI en diversos sistemas.

29. Prueba piloto de autenticación sin contraseña: Se están evaluando y probando métodos innovadores de autenticación sin contraseña para mejorar la seguridad y al mismo tiempo simplificar el acceso.

30. Análisis de los proveedores de Internet en las oficinas sobre el terreno: Se están analizando la calidad y el ancho de banda de los servicios de Internet en las oficinas sobre el terreno.

31. Mejora de la cooperación con los asociados externos: Se están estudiando posibilidades de colaborar con asociados externos para cubrir necesidades de conocimientos especializados y seguridad.

32. Elaboración de una hoja de ruta de la confianza cero: Se está elaborando una hoja de ruta de la confianza cero que se ajusta a las prioridades institucionales y los perfiles de riesgos.

33. Autenticación multifactor para todos los servicios de acceso público: Se está estableciendo la autenticación multifactor para todos los accesos externos y privilegiados.

34. Mejora de la gestión y detección de activos: Se están realizando esfuerzos por mejorar las herramientas de gestión y detección de activos, incluida la ampliación del inventario de servidores y el perfeccionamiento del despliegue de parches.

35. Consideración del emplazamiento de recuperación en casos de desastre: Se está planificando el establecimiento de un emplazamiento secundario para la recuperación en casos de desastre y el albergamiento de copias de seguridad de datos para garantizar la continuidad de las operaciones.