Organización Mundial de la Salud

CONSEJO EJECUTIVO **EB148/30**
148.ª reunión **11 de enero de 2021**
Punto 18.1 del orden del día provisional

Actualización sobre gestión y tecnologías de la información

Informe del Director General

1. En la 31.ª reunión del Comité de Programa, Presupuesto y Administración del Consejo Ejecutivo celebrada en enero de 2020, la Secretaría informó sobre sus iniciativas en materia de ciberseguridad.[1] Además, en el informe más reciente del Auditor Interno,[2] examinado en la 32.ª reunión del Comité, se destacaron elementos clave de la auditoría de la Hoja de Ruta sobre Ciberseguridad. El presente informe responde a la solicitud del Comité a la Secretaría para que facilite información sobre la gestión de la ciberseguridad.

AVANCES ANTES DE LA PANDEMIA

2. La ciberseguridad es una de las principales esferas de obtención de resultados en la estrategia de gestión y tecnologías de la información (TI). Su objetivo es proteger los activos digitales de la Secretaría, reforzar la seguridad de los datos y garantizar la capacidad de prestar servicios con un nivel aceptable de riesgo.

3. Entre las iniciativas emprendidas para fomentar la ciberseguridad figura la formación obligatoria destinada a sensibilizar a toda la Organización sobre esta materia; ejercicios mensuales sobre *phishing*; la celebración de un evento anual para tomar conciencia sobre la ciberseguridad; la creación de un repositorio central de registros de sistema que sirva de prueba en posibles investigaciones ulteriores; la uniformización de la gestión del cortafuegos; el despliegue de una solución antivirus global; la implementación de un servicio de filtrado del tráfico en la red de internet, y la implementación de un sistema de inteligencia para amenazas con el que poder tomar medidas preventivas para evitar incidentes futuros y predecibles.

4. La Secretaría también ha establecido un equipo de ciberseguridad especial e independiente. Además, ha iniciado la creación de un centro adecuado e integrado de operaciones de seguridad para trabajar en la identificación, prevención y detección de los ciberataques, y la protección y respuesta ante ellos.

5. El área de gobernanza se fortaleció mediante la publicación de la estrategia de ciberseguridad aprobada y de la Hoja de Ruta sobre Ciberseguridad y mediante políticas, normas, criterios y procedimientos operativos estándar generales; la creación del Consejo de Ciberseguridad, y la revisión de los estatutos del comité directivo mundial de tecnología de la información para abordar la necesidad de una responsabilidad integral en materia de ciberseguridad.

---

[1] Documento EB146/40.

[2] Documento A73/28.

RESPUESTA A LOS ATAQUES RELACIONADOS CON LA COVID-19

6. Desde la declaración de la pandemia de COVID-19, la Secretaría ha observado un aumento de los ciberataques con objetivos determinados. Entre ellos: *spear phishing*, suplantación de la identidad, *phishing*, *vishing* (*phising* a través de la voz) y ataques a infraestructuras y aplicaciones de TI. Entre marzo y mayo de 2020 se registraron más de 130 000 dominios relacionados con la COVID-19, de los cuales un 70%, según diversos investigadores, eran falsos y se utilizaron para realizar múltiples ciberataques.

7. Los ciberataques siguen aumentando significativamente en volumen y complejidad. Se ha visto que la solución inicial de inteligencia contra las amenazas es insuficiente. El 7 de mayo de 2020 se puso en marcha una nueva solución gracias a la cual se detectan nuevas amenazas de grupos que llevan a cabo amenazas persistentes avanzadas. Eso ha permitido a la Secretaría actuar con mayor rapidez y corregir la infraestructura, los sistemas y las herramientas de TI existentes.

8. A pesar de ello, según los análisis de las tendencias realizados por empresas especializadas en ciberseguridad, está previsto que continúen los ataques. Deben reforzarse continuamente las medidas para identificar, detectar y prevenir esos ciberataques, para protegerse y responder ante ellos y para recuperarse posteriormente. En consecuencia, la Secretaría ha acelerado la aplicación del programa de ciberseguridad. **Se han tomado medidas clave,** incluidas las que se exponen a continuación.

a) **Financiamiento.** En el informe del Auditor Interno de octubre de 2020 se afirmaba que los US$ 1,3 millones recibidos eran inadecuados para aplicar la Hoja de Ruta sobre Ciberseguridad.[1] El comité directivo mundial de tecnología de la información ha proporcionado US$ 4,7 millones adicionales para poder asignar un total de US$ 6 millones al programa.

b) **Equipo de ciberseguridad.** El equipo ha pasado de 6 a 11 miembros, con recursos en Ginebra y Budapest. Se ha establecido un «equipo rojo» para llevar a cabo acciones ofensivas con las que verificar la seguridad de los sistemas de TI y, por ejemplo, detectar vulnerabilidades en el sistema y evaluar riesgos.

c) **Establecimiento de un centro de operaciones de seguridad gestionado e integrado.** En junio de 2020 se creó un centro de operaciones de seguridad, en el que las operaciones de esa índole se integran con un servicio de información de seguridad y gestión de eventos. El centro proporciona visibilidad sobre todos los incidentes de seguridad y permite a la Secretaría centrarse en aquellos cuya gestión se ha trasladado desde un nivel inferior. Entre agosto y noviembre de 2020, se detectaron 14 500 millones de eventos de seguridad. Gracias a la puesta en marcha del centro de operaciones de seguridad, la Secretaría pudo filtrar, procesar y analizar esos incidentes de seguridad y centrar sus esfuerzos en 243 de ellos, cuya gestión se ha trasladado desde un nivel inferior.

d) **Mejora en la aplicación de la autenticación de usuario.** La Secretaría está aumentando los métodos de autenticación tradicionales (como la autenticación por nombre de usuario y contraseña) mediante servicios de autenticación de múltiples factores (por ejemplo, *soft tokens*) con los que se comprueba la identidad del usuario. Se ha completado la aplicación de la autenticación de múltiples factores, que abarca ahora todos los servicios de la Secretaría disponibles a través de internet.

e) **Seguimiento continuo de los activos de TI de la Organización.** La Secretaría ha implementado una solución de detección y respuesta para puntos finales con la que solventar la necesidad de un seguimiento continuo de las amenazas contra las activos de TI de la Organización, y de respuesta ante ellas, mediante el uso de herramientas para detectar, contener (si es necesario)

[1] Documento A73/28.

e investigar actividades sospechosas. Esta solución proporciona visibilidad sobre todo el entorno de trabajo y genera la capacidad de detectar amenazas y protegerse y responder ante ellas, de manera oportuna. Hasta la fecha, se ha instalado en el 88% de todos los ordenadores y servidores de la Organización, y se está trabajando para completar la aplicación en todos ellos durante el segundo trimestre de 2021.

f) **Sistema para evitar la suplantación de correo electrónico de la Organización en mensajes al público.** Cada mes se envía un promedio de 2,3 millones de mensajes de correo electrónico bajo la dirección <@who.int>. En abril de 2020, alrededor del 80% de esos mensajes eran suplantaciones. En mayo de 2020, la Secretaría puso en servicio una solución de autenticación de mensajes, informes y conformidad basada en dominios (DMARC) para minimizar esas prácticas y permitir que solo fuentes autorizadas pudieran enviar mensajes en nombre de la Organización. Desde entonces, el 96% de los mensajes de correo electrónico han sido auténticos y el 4% restante suplantaciones que han podido ser eliminadas y nunca han llegado a los buzones de las organizaciones en las que se utiliza DMARC.

g) **Eliminación de aplicaciones antiguas.** Los sistemas antiguos desarrollados con tecnología obsoleta son vulnerables a ataques ultramodernos. Se están aplicando parches de seguridad, pero en algunos casos el diseño y la arquitectura del sistema obsoleto hacen que estos no basten para defenderse de ataques malintencionados. Así, la Secretaría ha sustituido un número importante de aplicaciones que ya no pueden corregirse ni mejorarse con parches.

9. Para gestionar de manera eficaz el programa de ciberseguridad se requiere una comunicación y una coordinación constantes. En particular:

a) internamente, la coordinación a nivel mundial se realiza a través del grupo de ciberseguridad, que está compuesto por el equipo de ciberseguridad y representantes de todas las regiones. Este grupo coordina las actividades de la OMS relacionadas con la ciberseguridad, incluida la aplicación de procedimientos, normas y soluciones en ese ámbito;

b) se ha establecido un canal de comunicación directa con múltiples equipos informáticos de respuesta de emergencia, organizaciones gubernamentales y empresas privadas con el fin de recibir y compartir información sobre amenazas procesables. Cada día se comparten indicadores de compromisos.

10. Además, los sistemas y aplicaciones institucionales (incluidos el Sistema Mundial de Gestión, el correo electrónico, los sitios web, las plataformas colaborativas y las plataformas de desarrollo) se supervisan constantemente. Además se aplican parches de seguridad sin demora para reducir o eliminar los riesgos de ciberseguridad.

SOSTENIMIENTO DE LAS MEDIDAS DE CIBERSEGURIDAD

11. Los ataques e infracciones en materia de ciberseguridad, cuando tienen éxito, son costosos. Algunos de los posibles costos son: daños al valor y la reputación de la Secretaría; pérdidas financieras directas (medidas correctivas, tiempo invertido, costos jurídicos, costos en materia de relaciones públicas y costos de notificación); repercusiones en la disponibilidad del sistema; pérdida de datos críticos, y pérdida de integridad en los datos.

12. A pesar de todos los esfuerzos mencionados que ha realizado la Secretaría, todavía hay problemas que deben tratarse y una serie de esferas en las que debe mejorarse. Las siguientes ocho nuevas soluciones de trabajo son esenciales para proteger a la Secretaría contra los actores que realizan amenazas persistentes avanzadas y se incluyen en el ámbito de aplicación del programa de ciberseguridad.

a) **Mejora de la protección de correo electrónico, con enlaces y archivos adjuntos seguros.** Más del 90% de los ciberataques comienzan mediante *phishing* de correo electrónico con enlaces y archivos adjuntos. Las funciones de seguridad de correo electrónico integradas proporcionarán protección ya que permitirán comprobar automáticamente y de forma mejorada si los archivos adjuntos al correo electrónico presentan contenido malintencionado y verificar el tiempo de clic en los mensajes de correo electrónico.

b) **Acceso más seguro a internet.** Al utilizar un proxy de nube general se protegerán los dispositivos de punto final que acceden a internet, tanto dentro como fuera de las oficinas de la Organización. Gracias a eso se controlará el acceso a internet de los dispositivos de punto final mediante la verificación del sitio web, el filtrado y la protección contra programas maliciosos.

c) **Análisis de vulnerabilidades en aplicaciones.** Proporcionará una evaluación de seguridad coherente y mejorada de las aplicaciones móviles y basadas en web durante las fases de desarrollo, prueba y operación. El objetivo es detectar vulnerabilidades en el sistema, la red y las aplicaciones.

d) **Cortafuegos de aplicaciones web.** Se trata de una nueva generación de protección y acceso para aplicaciones web. Un cortafuegos de aplicaciones web actúa como escudo y pasarela entre la internet y la aplicación, e impide que se produzcan ataques contra esta última. El acceso externo se rastrea, filtra y supervisa.

e) **Control de seguimiento de vulnerabilidades**. Sirve para crear un sistema en línea automático de verificación y presentación de informes que se integrará con los procesos de gestión de incidentes, cambios y parches. Facilitará la corrección de vulnerabilidades relacionadas con sistemas y aplicaciones sin parches.

f) **Gestión de accesos con privilegios.** Esta solución no solo proporciona a la Organización visibilidad sobre las posibles amenazas que plantean diversos tipos de acceso con privilegios, sino que también, mediante la puesta en servicio de herramientas adecuadas, protege contra el abuso de cuentas muy privilegiadas (como las de los administradores del sistema).

g) **Gestión de la separación de funciones.** Sirve para que haya una clara separación de funciones y cometidos para acceder a los sistemas. No deberían producirse casos en los que un individuo pueda crear y aprobar transacciones para cometer delitos cibernéticos (robo o fraude en beneficio propio).

h) **Tecnología de engaño**. Sirve para crear trampas o señuelos diseñados para engañar a los agentes generadores de amenazas y hacerles creer que han conseguido entrar en la Organización (por ejemplo, cuando intentan robar credenciales o información confidencial). Esto mejorará la capacidad de la Secretaría para detectar comportamientos de personas ajenas a la Organización que tratan de infiltrarse en ella y para utilizar esos conocimientos con miras a reforzar la seguridad de sus sistemas.

13. Es fundamental seguir aplicando este tipo de medidas. La inclusión de estas soluciones de trabajo en las labores de ciberseguridad de la Secretaría reforzará aún más las modalidades de identificación, detección, prevención, protección y respuesta que conducen a la aplicación de la Hoja de Ruta sobre Ciberseguridad.

FINANCIACIÓN SOSTENIBLE

14. En la decisión WHA70(16) (2017) se autorizó al Director General a asignar, al final de cada bienio, al menos US$ 15 millones, en función de la disponibilidad, para las necesidades de inversión en tecnología de la información dentro del Fondo para Infraestructura.[1] El actual programa de ciberseguridad está financiado con cargo a ese Fondo.

15. La Secretaría entiende que la ciberseguridad es una prioridad absoluta. Es importante proteger todos los avances realizados hasta la fecha y seguir con la labor que se está realizando para proteger a la Organización. Se han realizado unos primeros cálculos para poder completar el programa de ciberseguridad. Con todo, en los próximos años se necesitará invertir de forma importante para mantener las operaciones de ciberseguridad más allá de la finalización del programa.

16. El Comité Consultivo de Expertos Independientes en materia de Supervisión ha recomendado que se lleve a cabo un examen general de los gastos en tecnologías de la información de la Organización como parte del ciclo general de planificación.[2] En el examen deberían tenerse en cuenta tanto los costos del funcionamiento de la Secretaría como todas las iniciativas de cambio en tecnología de la información, incluida la ciberseguridad. La Secretaría está llevando a cabo ese examen en el contexto más amplio de la preparación del proyecto de presupuesto por programas 2022-2023.

17. La Secretaría proporcionará a los Estados Miembros, por conducto del Comité de Programa, Presupuesto y Administración en su 34.ª reunión, la relación de iniciativas (es decir, operaciones frente a cambios), incluido un examen general actualizado de los gastos futuros en materia de tecnologías de la información.

INTERVENCIÓN DEL CONSEJO EJECUTIVO

18. Se invita al Consejo a tomar nota del informe.

= = =

[1] Véase el documento WHA70/2017/REC/1.

[2] Véase el documento EBPBAC30/2.