Organización Panamericana de la Salud
Organización Mundial de la Salud
OFICINA REGIONAL PARA LAS Américas

12.ª SESIÓN DEL SUBCOMITÉ DE PROGRAMA, PRESUPUESTO Y ADMINISTRACIÓN DEL COMITÉ EJECUTIVO

Washington, D.C., EUA, del 21 al 23 de marzo del 2018

Punto 5.4 del orden del día provisional

SPBA12/INF/4
17 de enero del 2018
Original: inglés

CIBERSEGURIDAD EN LA OPS

Introducción

1. En vista de que las amenazas cibernéticas siguen afectando a las organizaciones internacionales, la Oficina Sanitaria Panamericana (la Oficina u OSP) continúa comprometida con el fortalecimiento de las medidas de ciberseguridad necesarias para proteger los datos y mantener un entorno digital seguro.

2. En el presente documento se informa acerca de las iniciativas de la Oficina para evaluar y fortalecer la ciberseguridad. Se resumen las actividades en curso y se presenta la hoja de ruta que se ha elaborado para seguir fortaleciendo la postura de ciberseguridad de la Oficina.

Antecedentes

3. La Oficina utiliza ampliamente la tecnología de la información para llevar adelante sus funciones. Dado que se depende de la tecnología cada vez más, resulta imperativo tener permanentemente un alto grado de confianza en la seguridad de los datos de la Oficina.

4. En el 2016, el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas (CICE) prestó a la Oficina asesoramiento estratégico sobre la ciberseguridad. Se evaluaron las medidas de ciberseguridad vigentes en relación con las mejores prácticas de la industria, recogidas por la Organización Internacional de Normalización (ISO por su sigla en inglés) en la norma ISO 27001, y se definió una hoja de ruta sobre la ciberseguridad.

Logros en el 2017

Finalización de la evaluación conforme a la norma ISO 27001

5. En el 2017, la Oficina finalizó una evaluación sobre la ciberseguridad en la que se examinaron los controles implementados actualmente en relación con las mejores prácticas de la industria, descritas en la norma ISO 27001. La ISO 27001, que forma parte de la serie ISO 27000, es una norma ampliamente aceptada en la cual se indican los requisitos para establecer, implementar, poner en funcionamiento, monitorear, examinar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información. Como parte de la evaluación se examinó el cumplimiento de la norma en el contexto de la misión de la Organización Panamericana de la Salud (OPS).

6. En la evaluación se utilizó el modelo de madurez de la capacidad para medir la madurez de los controles de seguridad de la información aplicados dentro de la Oficina. En el curso de la evaluación, se determinó que la capacidad de la Oficina en materia de ciberseguridad tiene varios puntos fuertes, entre los que se encuentran:

a) introducción del puesto de oficial de seguridad de la información a tiempo completo;

b) asesoramiento continuo en materia de seguridad de la información estratégica prestado por el Centro Internacional de Cálculos Electrónicos de las Naciones Unidas (CICE);

c) esfuerzos continuos para externalizar la gestión de servicios de la seguridad de la red informática;

d) consolidación del marco de normas y procedimientos sobre la seguridad de la información;

e) capacidad de respaldo y recuperación de datos;

f) utilización de sistemas de protección contra programas maliciosos (*anti-malware)* en toda la Organización;

g) utilización de programas para detectar vulnerabilidades en los sistemas informáticos en toda la Organización;

h) integración de la respuesta frente a incidentes informáticos en el plan de continuidad de las operaciones;

i) modernización de los cortafuegos y filtros para la web para toda la Organización;

j) mejora de la seguridad de la infraestructura inalámbrica;

k) fortalecimiento de los controles del acceso físico a los centros de datos de la Oficina;

l) integración de los requisitos contractuales sobre ciberseguridad en los contratos de los proveedores.

7. En la evaluación se indicó si las recomendaciones tenían una prioridad alta, media o baja, según su grado de conformidad con los requisitos establecidos en la norma ISO. En total, se plantearon dos recomendaciones de prioridad alta, cuatro recomendaciones de prioridad media y nueve recomendaciones de prioridad baja.

8. En las dos recomendaciones de prioridad alta se insta a la Oficina a fortalecer la capacidad de respuesta frente a los incidentes cibernéticos y a aumentar la conciencia sobre la ciberseguridad en la fuerza laboral de la Organización. En el estudio también se recomienda aumentar la capacidad operativa en cuanto a la ciberseguridad para detectar y remediar los puntos débiles y las amenazas en el entorno actual de la tecnología de la información.

Finalización de la evaluación sobre la seguridad del PMIS

9. Se realizó una evaluación sobre la seguridad del Sistema de Información Gerencial de la OSP (PMIS, por su sigla en inglés). La evaluación se llevó a cabo comparando los controles aplicados en el entorno del PMIS y los controles recomendados por: *a*) la norma internacional ISO 27001 sobre sistemas de gestión de la seguridad de la información; y *b*) el grupo Cloud Security Alliance. Este grupo promueve el uso de mejores prácticas para garantizar la seguridad en la computación en la nube y ofrece programas de capacitación sobre el uso de la computación en la nube con el propósito de ayudar a preservar la seguridad en todos los sistemas informáticos. En la evaluación no se detectó ninguna vulnerabilidad crítica en cuanto a la seguridad de la información. Se presentaron nueve recomendaciones de prioridad media para seguir mejorando la ciberseguridad de esta plataforma.

Incidentes relacionados con la ciberseguridad

10. En el 2017, la Oficina no registró ningún incidente crítico relacionado con la ciberseguridad que afectara la confidencialidad, la disponibilidad o la integridad de la información o los recursos tecnológicos de la Oficina. La Oficina sí experimentó varios incidentes por intentos de suplantación de identidad (*phishing*) en el 2017, los cuales tenían como objetivo obtener nombres de usuario y contraseñas para llevar a cabo actividades no autorizadas en los sistemas de la Oficina. Con su capacidad actual de ciberseguridad, la Oficina pudo detectar estos incidentes y aplicar controles para mitigarlos, y no detectó ninguna actividad no autorizada en sus sistemas informáticos. La Oficina también observó que la capacidad del proveedor del PMIS en cuanto a ciberseguridad tuvo un papel clave en la prevención de transacciones no autorizadas. Sin embargo, el aumento de la frecuencia y la complejidad de estos intentos de suplantación de identidad demuestran que es necesario reforzar los mecanismos de control del acceso a los sistemas de información de la Oficina. Esta recomendación se incluyó en la hoja de ruta sobre ciberseguridad que se describe a continuación.

Hoja de ruta sobre ciberseguridad

11. Partiendo de las recomendaciones formuladas en las evaluaciones y de los incidentes detectados en cuanto a la seguridad, y de conformidad con el Plan Estratégico de la Organización, la Oficina elaboró una hoja de ruta sobre ciberseguridad en la cual se definen los proyectos e iniciativas que deben emprenderse para mejorarla. Algunos de ellos se pusieron en marcha en el 2017, mientras que otros se implementarán a lo largo de los años 2018 y 2019. La implementación de estas iniciativas aumentará la madurez de la capacidad de la ciberseguridad de la Oficina, y mejorará la capacidad de proteger su información.

12. Los siguientes proyectos e iniciativas se realizaron en el 2017 para mejorar la capacidad de la Oficina en cuanto a la ciberseguridad, conforme a la hoja de ruta:

a) *Contratación del oficial de seguridad de la información a tiempo completo.* En el 2017 se finalizó el proceso de contratación del oficial de seguridad de la información.

b) *Informes y monitoreo del sistema antivirus.* Se actualizó la protección del sistema antivirus en uso para utilizar la última versión disponible y mejorar la capacidad para detectar amenazas avanzadas. Además se implementó un sistema de alertas, el cual ha fortalecido la capacidad de la Organización para responder a incidentes graves relacionados con virus informáticos.

c) *Consolidación e implementación de servicios de gestión de la seguridad de los cortafuegos.* La Oficina finalizó la externalización de los servicios de gestión de la seguridad en 28 oficinas para proteger la infraestructura informática de la Organización contra las amenazas externas. El trabajo en las dos oficinas restantes se terminará en el primer trimestre del 2018.

d) *Servicios de inteligencia para detectar amenazas.* Se adquirió la suscripción a un servicio externo de inteligencia para detectar amenazas con la intención de recibir alertas tempranas de amenazas cibernéticas que puedan afectar a la Oficina. Este servicio permitirá que la Oficina reciba informes de inteligencia sobre agentes y redes que representan una amenaza y están involucrados en delitos cibernéticos, piratería informática (*hacking*) y fraude, aprovechando su acceso inigualable a comunidades maliciosas en las llamadas “web oscura” y “web profunda” de manera más amplia. La información pertinente se clasificará y se remitirá a la Oficina. La suscripción a este servicio también proporcionará a la Oficina acceso a información procedente de otros organismos de las Naciones Unidas suscritos al servicio sobre amenazas para que se pueda actuar al respecto. Además, el servicio permitirá a la Oficina monitorear la “web oscura” para detectar robos de información de acceso.

e) *Servicios de calificación de los riesgos de seguridad.* Un servicio de calificación de los riesgos de seguridad monitorea la presencia de la Organización en internet y genera alertas cuando se observa una vulnerabilidad o un incidente de seguridad. El servicio, por suscripción, también proporciona a la Oficina una

calificación de la seguridad que indica la eficacia de la capacidad de la Oficina en cuanto a ciberseguridad y le permite comparar su programa de ciberseguridad con los de otros organismos del sistema de las Naciones Unidas. Cualquier aumento o disminución en la calificación de seguridad genera una alerta a la que se le dará seguimiento.

f) *Transmisión de información sobre seguridad a todas las representaciones y los centros panamericanos.* Se puso en práctica un programa de reuniones mensuales con todas las representaciones y los centros panamericanos para difundir el progreso en la ejecución de la hoja de ruta sobre ciberseguridad.

g) *Prueba sobre penetración.* Se realizó una prueba sobre la seguridad de una aplicación crítica. El objetivo fue evaluar las medidas de ciberseguridad aplicadas para proteger la información guardada y procesada con la aplicación. En la prueba no se detectó ninguna vulnerabilidad crítica.

h) *Mejora del sistema de gestión de vulnerabilidades.* El programa que se utiliza para detectar vulnerabilidades se mejoró y se configuró para establecer una visión global de las vulnerabilidades que afectan los sistemas informáticos de la Oficina. Esta herramienta tuvo un papel determinante al proteger los sistemas informáticos de la Oficina cuando ocurrió el incidente cibernético que se conoció como "WannaCry" en el segundo trimestre del 2017. WannaCry afectó supuestamente a miles de computadoras en más de 150 países del mundo, pero los sistemas informáticos de la Oficina, protegidos mediante el seguimiento continuo que proporciona este programa de computación, no se vieron afectados.

i) *Protección avanzada contra las amenazas.* Se completó la adquisición del sistema de protección avanzada contra amenazas de Microsoft, con la intención de mejorar la capacidad de detectar y responder a amenazas cibernéticas. La implementación de este sistema brindará protección de manera preventiva y permitirá detectar ataques cibernéticos y realizar la gestión centralizada y completa de la seguridad a lo largo del ciclo de vida de los sistemas informáticos de la Oficina.

j) *La retirada definitiva de los sistemas obsoletos.* Se remplazaron aproximadamente 63 sistemas obsoletos con el objetivo de reducir las vulnerabilidades que los proveedores no estaban solucionando.

k) *Consolidación y perfeccionamiento de la gestión de parches de seguridad.* Se consolidó aún más el programa que se utiliza para aplicar parches de seguridad a las computadoras, a fin de asegurar que pueda hacérsele seguimiento de forma central.

l) *Protección del sitio web público de la OPS.* Se adquirió una aplicación cortafuegos para la web a fin de brindar una mayor protección contra ataques cibernéticos al sitio web público de la OPS. El servicio protegerá contra las persistentes amenazas avanzadas dirigidas contra el sitio web de la OPS. Además, mejorará el rendimiento y la prestación técnica de este sitio web.

m) *Concientización sobre la seguridad.* Se han enviado varios boletines en la Oficina sobre la seguridad de la información para concientizar a los usuarios sobre las diversas amenazas cibernéticas, como la suplantación de identidad (*phishing*), los programas maliciosos tipo *ransomware* o virus, y para proporcionar información general sobre ciberseguridad.

13. Se prevé que en el período 2018-2019 se finalizarán varios proyectos en el ámbito de la ciberseguridad. En los siguientes párrafos se resume brevemente estos proyectos, por categoría:

a) *Mejora de los mecanismos de autenticación y control de acceso informático.* Estos proyectos permitirán mejorar aún más los mecanismos empleados por la Oficina para proteger servicios como el PMIS, el correo electrónico y el acceso remoto. También protegerán los sistemas informáticos de la Oficina de amenazas cibernéticas que prevalecen actualmente, las cuales se valen de vulnerabilidades en los mecanismos de control de acceso y autenticación.

b) *Mejora de la capacidad de respuesta frente a incidentes cibernéticos.* Considerando que es imposible evitar siempre que ocurran incidentes cibernéticos, los proyectos de esta categoría tendrán como objetivo fortalecer aún más la respuesta de la Oficina frente a los incidentes cibernéticos y su capacidad para solucionarlos.

c) *Concientización sobre la seguridad de la información.* La Oficina seguirá desplegando su programa de concientización sobre la seguridad de la información para incluir diferentes maneras de concientizar a los usuarios que tienen acceso a los sistemas informáticos de la Oficina.

d) *Protección de los sistemas de información de la Oficina con acceso público.* La Oficina seguirá realizando varios proyectos con el fin de aumentar la protección de los sistemas de información con acceso público para que no sean objeto de ataques que pretendan comprometer la ciberseguridad de los sistemas de información de la Oficina.

e) *Mejora de la capacidad de monitoreo y alerta.* Considerando el aumento de la complejidad y la frecuencia de las amenazas cibernéticas, la Oficina incrementará y mejorará la capacidad de monitoreo de la seguridad con el fin de detectar con rapidez los incidentes cibernéticos. Estas iniciativas mejorarán considerablemente la respuesta y las técnicas de resolución que ya se están aplicando en la Oficina, y permitirá detectar y remediar de manera temprana las vulnerabilidades en los sistemas informáticos.

14. La ejecución de las diversas iniciativas descritas en la hoja de ruta sobre ciberseguridad mejorará la postura de ciberseguridad de la Oficina para que esté más sincronizada con las recomendaciones de la norma ISO 27001. Estas iniciativas están en consonancia con las mejores prácticas de la industria y mejorarán la capacidad de la

Oficina de detectar y resolver los incidentes relacionados con la ciberseguridad, así como de responder y aprender de ellos.

Intervención del Subcomité de Programa, Presupuesto y Administración

15. Se invita al Subcomité a que tome nota de este informe y brinde las observaciones y recomendaciones que considere pertinentes.

- - -