Naciones Unidas A/68/552

Asamblea General

Distr. general
25 de octubre de 2013
Español
Original: inglés

Sexagésimo octavo período de sesiones
Tema 134 del programa
Proyecto de presupuesto por programas para el bienio 2014-2015

Progresos logrados en la aplicación de las recomendaciones relativas al fortalecimiento de la seguridad de la información y los sistemas en la Secretaría

Informe del Secretario General

Resumen

Este informe se presenta de conformidad con lo dispuesto en el párrafo 18 de la parte I de la resolución 67/254 de la Asamblea General, en la que la Asamblea solicitó al Secretario General que le proporcionara información actualizada sobre la marcha de la aplicación de las medidas dispuestas para corregir los problemas de seguridad de la información en el contexto del proyecto de presupuesto por programas para el bienio 2014-2015. Una evaluación independiente y unas fallas ocurridas en la seguridad de la información en 2013 ponen de manifiesto importantes deficiencias que exponen a la Organización a un nivel inaceptable de riesgo. El presente informe incluye medidas adoptadas como protección contra las amenazas de ciberataques y recursos adicionales necesarios por un monto de 3.440.700 dólares antes del ajuste, con arreglo a la sección 29E, Oficina de Tecnología de la Información y las Comunicaciones, del proyecto de presupuesto por programas para el bienio 2014-2015, a fin de hacer frente a las necesidades más urgentes de la Organización en materia de seguridad.

13-53219 (S) 041113 061113

I. Introducción

1. En el párrafo 107 de la resolución 66/246, la Asamblea General solicitó a la Comisión Consultiva en Asuntos Administrativos y de Presupuesto que pidiera a la Junta de Auditores que realizase una auditoría y evaluase la gestión de los asuntos relacionados con la tecnología de la información y las comunicaciones (TIC) en la Secretaría, incluida la Oficina de Tecnología de la Información y las Comunicaciones, y que la informase al respecto en la parte principal de su sexagésimo séptimo período de sesiones. La Junta realizó una auditoría en octubre de 2012 y presentó su informe (A/67/651) al Secretario General el 19 de diciembre de 2012.

2. En el párrafo 95 de su informe, la Junta de Auditores señaló que las Naciones Unidas carecían de un entorno de información adecuadamente seguro y que los controles de seguridad en vigor no estaban a la altura de lo que, a juicio de la Junta, cabría esperar en una organización moderna y mundial. Dijo también que la Secretaría tenía una capacidad extremadamente limitada en materia de control de la seguridad y por consiguiente no estaba en condiciones de detectar y responder adecuadamente a todas las infracciones de seguridad, tanto los meros intentos como las que lograran los resultados buscados.

3. En un informe posterior sobre la aplicación de las recomendaciones de la Junta de Auditores (A/67/651/Add.1), el Secretario General indicó que la recomendación relativa al fortalecimiento de la seguridad de la información y los sistemas en la Secretaría se estaba atendiendo con carácter de urgencia, y que la Administración estaba elaborando un plan de acción que preveía la aplicación de medidas a corto plazo para atender las deficiencias más urgentes y la definición de una estrategia de seguridad de la información sostenible a mediano y largo plazo. El plan de acción consiste en diez iniciativas centradas en tres esferas, a saber:

a) Controles preventivos. La Secretaría reforzará los controles técnicos de la infraestructura de las TIC a fin de:

i) Establecer controles más estrictos de los dispositivos informáticos utilizados en la red de las Naciones Unidas;

ii) Prevenir las formas perjudiciales de tráfico en Internet y el correo electrónico mediante el fortalecimiento de las medidas técnicas para proteger el perímetro de la red de las Naciones Unidas;

iii) Hacer una segmentación de la red para aislar las áreas en que los virus pueden ocultar posibles ataques;

iv) Lograr una mayor sensibilización del personal de las Naciones Unidas en materia de seguridad de la información impartiendo capacitación y fomentando la divulgación;

b) Mejores capacidades de detección y respuesta a incidentes. A fin de ajustarse a un entorno en el que el riesgo de amenazas ha aumentado de manera significativa, la Secretaría incorporará sistemas adicionales de detección de intrusiones y vigilará sus redes sistemáticamente;

c) Gobernanza, riesgos y cumplimiento. Se ratificará y pondrá en práctica una directiva sobre la seguridad de la información, que establece los principios fundamentales de la seguridad de la información en las Naciones Unidas y sirve de base para los instrumentos normativos y de gobernanza.

4. La Comisión Consultiva en Asuntos Administrativos y de Presupuesto, formulando observaciones acerca del informe de la Junta de Auditores sobre la gestión de los asuntos relacionados con la tecnología de la información y las comunicaciones en la Secretaría (A/67/770), recomendó posteriormente que se solicitara al Secretario General que, cuando prepare sus propuestas sobre la aplicación del plan de acción de seguridad de la información, haga todo lo posible por determinar prioridades y redistribuir recursos y que en la medida de lo posible evite presentar solicitudes de recursos adicionales. La Comisión Consultiva señaló también que compartía las preocupaciones de la Junta con respecto a la situación en materia de seguridad de la información. Recomendó que se solicitase al Secretario General que procediera a aplicar su plan de acción como cuestión prioritaria y que se asegurase de que, sin más demoras, se aprobase la carta sobre la seguridad de la información y los documentos normativos conexos, de tal forma que la rendición de cuentas quedase asegurada a todos los niveles de la Organización. Además, la Comisión señaló que el Secretario General también debía adoptar medidas correctivas con rapidez para superar todo obstáculo que pueda surgir en la aplicación eficaz del plan de acción o la promulgación y el cumplimiento de las políticas de seguridad de la información en toda la Secretaría, y recomendó que se solicitase al Secretario General que, en el contexto del proyecto de presupuesto por programas para el bienio 2014-2015, proporcionase información actualizada sobre la situación en que esté la aplicación de las medidas tomadas para corregir los problemas de seguridad de la información. La Comisión también solicitó a la Junta de Auditores que hiciese un seguimiento de la aplicación de sus recomendaciones en esta materia.

5. En el párrafo 11 de la parte I de su resolución 67/254, la Asamblea General solicitó al Secretario General que le presentase un informe sobre las medidas adoptadas para atender las prioridades señaladas por la Junta en su informe (A/67/651), incluida la seguridad de la tecnología de la información, y en el párrafo 18 invitó al Secretario General a que, en el contexto del proyecto de presupuesto por programas para el bienio 2014-2015, proporcionase información actualizada sobre la marcha de la aplicación de las medidas dispuestas para corregir los problemas de seguridad de la información, incluidas las adoptadas como protección contra las amenazas de ciberataques.

II. Situación actual

6. El Secretario General participa activamente en el fomento del plan de acción para reforzar la seguridad de la información en la Secretaría y ha concentrado su labor en las esferas más urgentes y críticas del plan de acción en la Sede. Hasta la fecha, la Oficina de Tecnología de la Información y las Comunicaciones ha hecho todo lo posible por modificar las prioridades y redistribuir los recursos en el marco de su consignación aprobada, así como absorber, en la medida de lo posible, el costo de la ejecución de las actividades de apoyo a las iniciativas del plan de acción. Sin embargo, esos recursos han resultado insuficientes para afrontar adecuadamente todas las deficiencias detectadas. Además, desde la publicación del informe de la Junta de Auditores, las violaciones de la seguridad de la información a nivel mundial han aumentado considerablemente, tanto en frecuencia como en complejidad, y algunas de ellas han afectado directamente a la Secretaría.

7. A consecuencia de esos incidentes, el Secretario General considera que es imprescindible que se tomen medidas con carácter urgente, más allá de lo que la Oficina de Tecnología de la Información y las Comunicaciones ha hecho hasta ahora.

III. Medidas iniciales en la ejecución del plan de acción para reforzar la seguridad de la información

8. El plan de acción tenía por objeto afrontar con carácter urgente las deficiencias más urgentes en materia de seguridad de la información y definir una estrategia sostenible a mediano y largo plazo para la seguridad de la información de la Secretaría. Habida cuenta de la escasez de conocimientos especializados dentro de la Organización y de la necesidad de contar con un sólido análisis de sus operaciones de seguridad, se determinó que era necesario contratar expertos externos para validar y verificar los posibles riesgos. En julio de 2013, la Oficina de Tecnología de la Información y las Comunicaciones decidió encomendar una evaluación independiente de la situación de la seguridad de la información en la Secretaría a una empresa de consultoría externa, que validó y complementó las conclusiones internas y señaló las vulnerabilidades y deficiencias de funcionamiento de la Organización en la esfera de la seguridad de la información. Esta evaluación independiente, así como los nuevos incidentes relativos a la seguridad de la información que tuvieron lugar a lo largo de 2013, pusieron de manifiesto importantes deficiencias que exponen a la Organización a un nivel inaceptable de riesgo.

9. Sobre la base de la evaluación independiente, que se centró principalmente en la infraestructura en Nueva York, el Secretario General considera que es esencial reforzar la seguridad de la información en la Sede, expandir con urgencia la evaluación independiente habida cuenta del aumento en el número de ataques cibernéticos contra la Organización, y ampliar el alcance de las actividades para reforzar la seguridad de la información en las oficinas situadas fuera de la Sede, en las comisiones regionales y en las misiones sobre el terreno en 2014. La información proporcionada a raíz de la colaboración con dichas oficinas indica que hace falta una labor considerable para afrontar las vulnerabilidades que ellas presentan. Del mismo modo, si bien las oficinas sobre el terreno que cuentan con el respaldo del Departamento de Apoyo a las Actividades sobre el terreno pueden ser menos vulnerables, dado que el servicio se presta de forma centralizada desde la Base de Apoyo de las Naciones Unidas en Valencia (España) y la Base Logística de las Naciones Unidas en Brindisi (Italia), sus vulnerabilidades también deben ser evaluadas a fondo.

10. A continuación se detallan las actividades que se han realizado hasta el momento para poner en práctica el plan de acción:

a) Se han reforzado los controles preventivos mediante la limitación de privilegios administrativos respecto a las computadoras de escritorio y portátiles recientemente expedidas o actualizadas. Está en marcha la adquisición de nuevos sistemas de filtración para el tráfico de correo electrónico e Internet, previéndose que terminará a fines de noviembre de 2013. Por otra parte, se están reconfigurando los servidores con las medidas de seguridad vigentes para garantizar que estén al día en lo que se refiere a sus posibles vulnerabilidades. Se ha revisado la infraestructura de cortafuegos de la Sede y se la está sustituyendo por tecnología más avanzada, lo que aumentará la protección contra los ataques externos y la segmentación de la red

interna. Además, se ha adquirido un curso de capacitación por computadora para sensibilizar a todos los funcionarios de la Secretaría acerca de la seguridad de la información;

b) Se ha puesto en marcha una evaluación de todas las aplicaciones de software en funcionamiento en la actualidad para garantizar el cumplimiento de las normas de seguridad de la información y las mejores prácticas. Esta labor se lleva a cabo en el marco de la selección de todas las aplicaciones de software que han de permanecer activas tras la implementación de Umoja y otros sistemas institucionales y para asegurarse de que no representen riesgos a la seguridad;

c) Se ha obtenido un servicio gestionado para el despliegue y el funcionamiento ininterrumpido de sistemas de detección de intrusos para los principales centros de datos en los centros de datos primario y secundario de Nueva York y Nueva Jersey, así como los centros institucionales de datos en la Base de Apoyo y la Base Logística. Además, se han consolidado las fuentes existentes de ciberinteligencia en toda la Secretaría a fin de aumentar su capacidad de ajustar las medidas defensivas de manera proactiva;

d) Se elaboró una directiva de política de seguridad de la información, que se comunicó a todos los jefes de departamentos y oficinas el 7 de marzo de 2013. Se trata de un marco general para las políticas, procedimientos y directrices de la Organización en materia de seguridad de la información. En esta directiva también se ordena informar acerca de los incidentes relativos a la seguridad de la información y compartir con la Secretaría los datos conexos de inteligencia de aplicación práctica. El Grupo Temático sobre Seguridad de la Información, adscrito a la Junta de los Jefes Ejecutivos del Sistema de las Naciones Unidas para la Coordinación, elaboró un conjunto de controles técnicos y de procedimiento para las necesidades mínimas de los sitios web para uso público, basándose en un borrador de la Oficina de Tecnología de la Información y las Comunicaciones y avalado por la red de tecnologías de TIC adscrita al Comité de Alto Nivel sobre Gestión de la Junta. Además, se están elaborando 52 políticas y procedimientos de TIC para ayudar a mejorar el rendimiento del sistema, así como su seguridad e integridad de producción. En cooperación con el Departamento de Información Pública, el documento se expedirá en 2014 como instrucción administrativa para abordar la importante exposición de los sitios web para uso público y los datos históricos de varias fallas de seguridad. Además, la Oficina de Tecnología de la Información y las Comunicaciones ha reasignado recursos para crear una función de cumplimiento interno con el fin de aumentar el cumplimiento de las políticas y procedimientos internos y las mejores prácticas del sector. La Oficina creó también un grupo de trabajo sobre la seguridad de la información, como parte del Grupo de Coordinación de la Gestión de la TIC, para que aumente el nivel de comunicación entre los lugares de destino, incluidas las oficinas situadas fuera de la Sede, las comisiones regionales y las misiones sobre el terreno.

11. Además de las medidas aplicadas en el marco del plan de acción, la Organización está introduciendo cambios importantes en sus operaciones de TIC a nivel mundial, con el fin de apoyar la aplicación de Umoja y otros sistemas secundarios y acordes con ese objetivo. Entre estos cambios cabe citar la aplicación de una nueva red mundial de área amplia basada en la conmutación de etiquetas multiprotocolo (Multi-Protocol Label Switching), la utilización de una capa de acceso estándar (Citrix) para todos los sistemas institucionales, y la migración de las

aplicaciones de software a los centros de datos institucionales de Valencia y Brindisi. Estos cambios permitirán un control más estricto del acceso y una gestión más sólida de la infraestructura de TIC y reducirán su vulnerabilidad a la intrusión.

12. Por ser parte fundamental de la recuperación en casos de desastre y continuidad de las operaciones, la seguridad de las TIC desempeña también un papel importante en las misiones sobre el terreno, en vista de su entorno operacional. El Departamento de Apoyo a las Actividades sobre el Terreno ha establecido recientemente un marco normativo de seguridad situado en el Centro Operacional de Tecnologías sobre el Terreno, adscrito al Departamento y que abarca las instalaciones de las TIC en la Base de Apoyo y la Base Logística. De conformidad con este marco normativo, en el Centro Operacional de Tecnologías sobre el Terreno y en las misiones sobre el terreno se realizan periódicamente evaluaciones de la seguridad de los sistemas de información desplegados.

IV. Otras medidas necesarias

13. La evaluación independiente y las fallas ocurridas en 2013 en materia de seguridad de la información en 2013 han puesto de manifiesto que las Naciones Unidas no cuentan con suficientes controles de seguridad de la información, no solo en lo que respecta a los componentes tradicionales de la infraestructura de la información y las comunicaciones, sino también en lo referente a otros elementos de la infraestructura. La creación de sistemas de gestión, las soluciones para el control y la supervisión del acceso, los sistemas de telefonía y videoconferencia y los dispositivos audiovisuales, que tradicionalmente no han estado controlados por medios digitales, se ven ahora expuestos a amenazas de origen digital y potencialmente de Internet. Será necesario hacer nuevas evaluaciones detalladas para cerciorarse de que esos dispositivos formen parte de una estrategia amplia de seguridad de la información.

14. Una evaluación de los sistemas empleados en el Departamento de Apoyo a las Actividades sobre el Terreno ha revelado la necesidad de contar con nuevos programas informáticos para facilitar el control y la filtración de intrusos, así como cortafuegos perfeccionados, para mejorar el entorno de seguridad de la Organización en ambas localidades mencionadas anteriormente y en otros lugares. Se han puesto en práctica nuevas medidas de seguridad y ya se están realizando nuevos trabajos.

15. También se reveló que se ha visto aumentado el riesgo en materia de reputación de la Organización debido a deficiencias operacionales en la gestión de la información existente en la web. Por lo tanto, la Organización considera necesario examinar detenidamente los sitios web externos, revisar los controles de seguridad y prestar asistencia a los departamentos de la Secretaría en el rediseño de los sitios web a fin de hacer frente a la intrusión o degradación.

16. La estrategia amplia de seguridad de la información, que comprende sistemas basados en la web y sistemas tradicionales y aborda las cuestiones sistémicas subyacentes, constituirá una parte fundamental de la estrategia general de las TIC, que se presentará a la Asamblea General en su sexagésimo noveno período de sesiones para que ella proceda a su examen.

17. Por el momento será necesario adoptar de inmediato nuevas medidas para seguir mitigando los riesgos inaceptables para la Organización, aprovechando los avances hechos hasta el momento gracias a la ejecución del plan de acción para reforzar la seguridad de la información en la Secretaría.

18. Debido a la creciente necesidad de interconectividad y a la interdependencia de los sistemas de TIC en la Secretaría, un ataque o intrusión en cualquier lugar puede poner en peligro a todos los lugares. Por ende, las medidas adoptadas hasta el momento para ejecutar el plan de acción también deben ponerse en práctica en otros lugares de destino y han de complementarse con una mejora significativa de la capacidad de supervisión por parte de la Organización.

19. Se propone llevar a cabo las siguientes acciones, para las cuales se solicitan recursos en el presente informe, como medidas provisionales hasta que se presente la estrategia revisada en materia de TIC[1]:

a) Ampliación del servicio de detección de intrusos, de modo que abarque a las oficinas situadas fuera de la Sede y a las comisiones regionales. Este servicio se ha establecido y se circunscribe a los centros de datos primario y secundario de Nueva York y Nueva Jersey, así como a los centros institucionales de datos en la Base de Apoyo y la Base Logística, mediante el establecimiento de nuevas prioridades para los recursos existentes de la Oficina de Tecnología de la Información y las Comunicaciones en 2013. Sin embargo, en 2014 se necesitarán recursos adicionales para seguir sufragando el costo de los servicios en lugares ya establecidos y aumentar la cobertura a los lugares de destino en otros países;

b) Mayor cobertura y perfeccionamiento de la infraestructura del cortafuegos, y mejora de las soluciones de filtración para el correo electrónico y el tráfico en Internet de forma de incluir a las oficinas situadas fuera de la Sede y a las comisiones regionales, a fin de reforzar las capacidades de seguridad de la red a nivel mundial;

c) Mejora de la capacidad de vigilancia de la seguridad interna. Para mejorar significativamente esta capacidad, es necesario contar con herramientas adicionales y personal para supervisar el entorno de la tecnología de la información y las comunicaciones a fin de evitar todo intento de quebrantamiento de la seguridad informática;

d) Despliegue de un sistema de gestión de las vulnerabilidades que permita a la Organización detectar de forma proactiva deficiencias concretas y establecer prioridades para su mitigación;

e) Evaluaciones adicionales de los controles de protección y detección para los elementos de la infraestructura no tradicionales en la Sede y del entorno de la tecnología de la información y las comunicaciones en las oficinas situadas fuera de la Sede, en las comisiones regionales y en los centros de datos institucionales de Valencia y Brindisi.

20. Resulta evidente que la fragmentación de la red de las TIC de la Organización hace más difícil y costosa la tarea de garantizar la seguridad. La estrategia de la Organización ha consistido en trasladar sus centros de datos a Valencia y a Brindisi de forma acelerada para que puedan adoptar medidas de seguridad y vigilancia con

[1] Debido al carácter delicado de estas acciones y a fin de minimizar los riesgos operacionales, en el presente informe solo se puede dar una descripción genérica.

mayor rapidez y, al mismo tiempo mejorar el desempeño de las operaciones y reducir los costos. Además, eliminar la fragmentación será un pilar de la nueva estrategia del Secretario General en materia de las TIC, que se presentará a la Asamblea General en su sexagésimo noveno período de sesiones para que ella proceda a su examen.

V. Modificación del programa de trabajo necesario para el período 2014-2015

21. Para abordar adecuadamente el asunto de la seguridad de la información en la Secretaría, será necesario revisar el programa de trabajo aprobado de la Oficina de Tecnología de la Información y las Comunicaciones para el período 2014-2015 (A/67/6/Rev.1, prog. 25) a fin de incorporar las actividades relativas a la ejecución del subprograma 5, gestión estratégica y coordinación de la tecnología de la información y las comunicaciones.

VI. Necesidades adicionales con cargo al proyecto de presupuesto por programas para el bienio 2014-2015

22. Las necesidades de recursos adicionales enunciadas en el presente informe se derivan de una evaluación independiente realizada en 2013, tras la presentación del proyecto de presupuesto por programas para el bienio 2014-2015, del Secretario General (A/68/6 (Sect. 29E)), y se basan en un incremento en el número y la frecuencia de los ataques cibernéticos contra las Naciones Unidas. Por lo tanto, será necesaria una consignación adicional para la realización de las actividades detalladas anteriormente.

23. Tal como se describe en el cuadro 1, que figura a continuación, se estima que hará falta un monto total de 3.440.700 dólares, antes del ajuste, para un período de 12 meses con arreglo a la sección 29E a fin de atender a las más urgentes necesidades de la Organización en materia de seguridad, detalladas en el presente informe, a la espera del examen de la estrategia revisada de TIC por parte de la Asamblea General en su sexagésimo noveno período de sesiones.

Cuadro 1
Resumen de las necesidades por objeto de gastos
(En miles de dólares de los Estados Unidos)

Objeto de gastos	*Estimación 2014-2015*
Otros gastos de personal	581,4
Viajes de funcionarios	150,0
Servicios por contrata	1 325,0
Gastos generales de funcionamiento	59,3
Mobiliario y equipo	1 325,0
Total	**3 440,7**

Cuadro 2
Necesidades de recursos en virtud de la sección 29E del proyecto de presupuesto por programas para el bienio 2014-2015, antes del ajuste
(En miles de dólares de los Estados Unidos)

Objeto de gastos	*Crédito en A/68/6 (Sect. 29E)*	*Necesidades adicionales*	*Total de necesidades*
Puestos	36 168,6	–	36 168,6
Otros gastos de personal	5 634,0	581,4	6 215,4
Viajes de funcionarios	467,8	150,0	617,8
Servicios por contrata	12 697,0	1 325,0	14 022,0
Gastos generales de funcionamiento	16 574,5	59,3	16 633,8
Suministros y materiales	202,4	–	202,4
Mobiliario y equipo	948,2	1 325,0	2 273,2
Total	**72 692,5**	**3 440,7**	**76 133,2**

Otros gastos de personal

24. Con un crédito de 581.400 dólares se sufragará el costo de personal temporario general durante un período de 12 meses, para que cumpla funciones consistentes en atender las necesidades inmediatas en materia de seguridad relativas al nuevo diseño y aplicación de las prácticas de seguridad de la Oficina de Tecnología de la Información y las Comunicaciones y la consiguiente respuesta a incidentes. Se solicitan las siguientes plazas temporarias:

a) Una plaza de personal temporario equivalente a un puesto de categoría P-4 para cumplir las funciones de Ingeniero de Seguridad. El titular de esta plaza proveerá los conocimientos técnicos adicionales referidos a la aplicación del sistema de detección de intrusos que se puso en funcionamiento recientemente. Se estima que la Organización recibirá por lo menos 70.000 a 100.000 alertas de seguridad por mes. El Ingeniero de Seguridad colaborará con un contratista externo para determinar de forma sistemática y abordar las alertas de importancia fundamental que ameriten la adopción inmediata de medidas. Dado que el sistema de detección de intrusos se incorporará a las oficinas situadas fuera de la Sede y a las comisiones regionales, recopilará información a nivel mundial. La correlación de alertas entre los lugares y las actividades conexas de respuesta a incidentes debe coordinarse mundialmente. Esta función de coordinación mundial resultará fundamental para incrementar los beneficios que supone para la red el uso del sistema de detección de intrusos. Además, el Ingeniero de Seguridad ayudará en la aplicación del análisis y gestión del cortafuegos de próximo nivel;

b) Dos plazas de personal temporario equivalente a puestos de categoría P-3 para cumplir las nuevas funciones de análisis de programas informáticos malignos, creación de patrones y correlación de incidentes, que son actividades de fundamental importancia para determinar los tipos de ataques que podrá sufrir la Organización a raíz de las amenazas persistentes avanzadas, provenientes de diversos actores a escala mundial. Los titulares de estas plazas ampliarán también las capacidades existentes para las pruebas de penetración, la evaluación de vulnerabilidades y la generación y

coordinación de informes de las pruebas de seguridad de aplicación en la web. Además, los titulares de las plazas podrán interactuar con los equipos encargados de diseñar software a fin de reforzar las normas de elaboración segura y la realización de pruebas en oficinas de todo el mundo.

Viajes de funcionarios

25. Se necesita un crédito de 150.000 dólares para sufragar el costo del viaje de dos funcionarios a todas las oficinas situadas fuera de la Sede, a las comisiones regionales y a los centros de datos institucionales de Valencia y Brindisi durante un período mínimo de dos semanas, a fin de:

a) Llevar a cabo de forma inmediata evaluaciones independientes del cumplimiento de las normas de seguridad y pruebas técnicas, lo que se debe hacer para asegurarse de que los procedimientos operativos estándar se respetan y se hacen cumplir con regularidad. La misión evaluará, validará y documentará las cuestiones locales que previamente no estaban documentadas y los riesgos para la seguridad de la información. Además, ello permitirá al personal de la Sede vigilar e informar acerca de los niveles de cumplimiento, lo que es fundamental para la aplicación de la estrategia central de seguridad de las TIC;

b) Prestar asesoramiento técnico y asistencia en la aplicación de la política, así como en la verificación de todos los nuevos sistemas y aplicaciones planificados;

c) Celebrar reuniones e impartir capacitación *in situ* y práctica a todos los interesados de las esferas institucionales y tecnológicas, para asegurarse de que el diseño y la arquitectura de las medidas preventivas de seguridad de la información se entienden y aplican con eficacia en todos los lugares de destino.

26. Los recursos propuestos con arreglo a esta categoría se destinarían a viajes en los casos en que la tecnología de Internet y audio conferencia no constituyan una alternativa eficaz en vista de la confidencialidad del trabajo de que se trata. En la medida de lo posible, se seguirán realizando misiones sucesivas para posibilitar un uso más eficiente de los recursos.

Servicios por contrata

27. Con un crédito de 1.325.000 dólares se sufragarían:

a) Servicios de detección de intrusos (800.000 dólares) para el despliegue y funcionamiento ininterrumpido de sistemas contra los intrusos, que se han puesto en marcha en el marco de la ejecución del plan de acción. El despliegue inicial en Nueva York, Brindisi y Valencia se llevó a cabo gracias a la reasignación de los recursos existentes. Sin embargo, a fin de lograr una cobertura completa a nivel mundial, este servicio debe ampliarse de forma de abarcar a todos los centros de datos y lugares de destino. La capacidad de detectar los intentos de intrusión es fundamental para que la Organización pueda responder de forma oportuna;

b) Un sistema de gestión de las vulnerabilidades (25.000 dólares) que de forma sistemática y periódica escanearía todos los activos de TIC de las Naciones Unidas, como los servidores y otros sistemas críticos, para asegurar su correcta configuración y el despliegue oportuno de actualizaciones de seguridad fundamentales, ayudando en la gestión de dichos activos y detectando vulnerabilidades antes de que un ataque externo las explote;

c) Servicios personales individualizados (500.000 dólares) respecto a conocimientos altamente especializados necesarios para realizar, en función de las necesidades, actividades esenciales para la ejecución ininterrumpida de la estrategia de seguridad de la información de la Secretaría, incluidas las nuevas tecnologías, y la realización de nuevas evaluaciones de los elementos de infraestructura fundamental. Además, hará falta contar con conocimientos especializados para abordar los problemas técnicos concretos a corto plazo y para aportar capacidades forenses o de investigación adicionales que aseguren una máxima comprensión de la forma en que se subsanan las deficiencias de seguridad de la información. La naturaleza del trabajo, cuyo objeto es transmitir al personal los conocimientos obtenidos, será de corto plazo y altamente especializada.

Gastos generales de funcionamiento

28. Con el crédito de 59.300 dólares se sufragaría el costo de alquilar espacio de oficina (47.700 dólares) y un acuerdo de prestación de servicios (“A”) (6.300 dólares) para tres plazas temporarias en Nueva York; una red local (1.800 dólares); y cargos por concepto de comunicaciones (3.500 dólares).

Mobiliario y equipo

29. Con el crédito de 1.325.000 dólares se sufragarían:

a) Las capacidades de supervisión continua (200.000 dólares). La compilación y el análisis centralizados de los registros del sistema complementan la información proporcionada por el sistema de detección de intrusos y permite a la Organización detectar actividades anómalas o sospechosas que no se consideran malignas. Además de su capacidad de detectar abusos y ataques furtivos, dicho sistema aportará la capacidad de analizar la causa de fondo de las intrusiones tras su descubrimiento y de determinar su amplitud. El sistema de información sobre la seguridad y gestión de eventos, cuya compra se propone, consiste en hardware, software y concesión de licencias autorizados basados en el volumen de la información recopilada;

b) Las mejoras a la infraestructura del cortafuegos (1 millón de dólares), incluido el perfeccionamiento de los cortafuegos existentes (500.000 dólares) y las soluciones de filtración (500.000 dólares) con los cortafuegos de vanguardia conocidos como de “próxima generación” y de filtración de contenidos, que permitirá a la Organización prevenir o detectar intentos de ataque e intrusiones concebidas para evitar su detección por herramientas tradicionales. La mejora es fundamental para hacer frente a la constante evolución de los ataques contra la Organización. Ya ha comenzado la mejora en la Sede y en los centros de datos institucionales en Valencia y Brindisi reasignando los recursos existentes en 2013. Sin embargo, las mejoras deben ampliarse de forma que abarquen a todos los centros de datos y lugares de destino;

c) Pruebas de seguridad de las aplicaciones web (125.000 dólares), incluida la adquisición de herramientas actualizadas de pruebas de seguridad de las aplicaciones web en forma de licencias de web para su uso local o como software de servicios (“software as a service”) para su aplicación global. Las herramientas pueden ser usadas por personal de seguridad interno o por diseñadores de páginas web a fin de reforzar la seguridad del sitio web de las Naciones Unidas.

VII. Medidas que deberá adoptar la Asamblea General

30. **Se solicita a la Asamblea General:**

a) Que tome nota del presente informe;

b) Que apruebe una consignación adicional por un monto de 3.440.700 dólares con arreglo a la sección 29E, Oficina de Tecnología de la Información y las Comunicaciones, del proyecto de presupuesto por programas para el bienio 2014-2015, a fin de afrontar las necesidades urgentes para reforzar la seguridad de las TIC en la Secretaría, como cargo imputable al fondo para imprevistos.