Naciones Unidas A/68/7/Add.11

Asamblea General

Distr. general
4 de diciembre 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

Duodécimo informe de la Comisión Consultiva en Asuntos Administrativos y de Presupuesto sobre el proyecto de presupuesto por programas para el bienio 2014-2015

I. Introducción

1. La Comisión Consultiva en Asuntos Administrativos y de Presupuesto ha examinado el informe del Secretario General sobre los progresos logrados en la aplicación de las recomendaciones relativas al fortalecimiento de la seguridad de la información y los sistemas en la Secretaría (A/68/552) presentado de conformidad con la resolución 67/254 de la Asamblea General, en la que la Asamblea solicitó al Secretario General que le proporcionase 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. Durante el examen de dicho informe, la Comisión se reunió con los representantes del Secretario General, quienes proporcionaron información y aclaraciones adicionales, que concluyeron con las respuestas recibidas por escrito el 20 de noviembre de 2013.

2. La Comisión Consultiva recuerda que en su primera auditoría sobre 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 (A/67/651), la Junta de Auditores declaró que las Naciones Unidas no tenían un entorno de información suficientemente seguro y presentó una serie de recomendaciones para abordar los problemas detectados. En su informe sobre la aplicación de esas recomendaciones (A/67/651/Add.1), el Secretario General indicó que la Secretaría estaba elaborando un plan de acción que

consistía en diez iniciativas destinadas a atender las deficiencias más urgentes y comprendía la aplicación de medidas a corto plazo y la definición de una estrategia sostenible de seguridad de la información a mediano y largo plazo. Las diez iniciativas se centraban en tres esferas: a) controles preventivos; b) mejores capacidades de detección de incidentes y respuesta; y c) gobernanza, riesgos y cumplimiento.

3. El informe del Secretario General proporciona información sobre la situación actual en relación con la TIC, las medidas iniciales en la ejecución del plan de acción para reforzar la seguridad de la información, y las otras medidas que es necesario adoptar al respecto. El Secretario General indica que se presentará a la Asamblea General, en su sexagésimo noveno período de sesiones, una estrategia amplia de seguridad de la información, incluidos sitios web y misiones sobre el terreno, en el contexto de la estrategia general de TIC.

II. Actividades concluidas hasta la fecha

4. En los párrafos 10 y 11 de su informe, el Secretario General proporciona información sobre las actividades llevadas a cabo para ejecutar el plan de acción, a saber: a) el fortalecimiento de los controles preventivos mediante la limitación de privilegios administrativos, la actualización de los servidores para adaptarlos a los niveles de seguridad actuales, la adquisición de nuevos sistemas de filtración para el tráfico de correo electrónico e Internet, la revisión y sustitución de la infraestructura de cortafuegos por tecnología más avanzada y la adquisición de un curso de capacitación por computadora para sensibilizar a todos los funcionarios de la Secretaría acerca de la seguridad de la información; b) el inicio de una evaluación sobre los riesgos que suponen para la seguridad las aplicaciones de programas informáticos existentes en el marco de las iniciativas que ya se están llevando a cabo con el fin de determinar las aplicaciones que han de permanecer activas tras la puesta en marcha de Umoja; y c) la adquisición de un servicio gestionado para el despliegue y el funcionamiento ininterrumpido de sistemas de detección de intrusos para los centros de datos primario y secundario de la Sede (Nueva York y Nueva Jersey) y los centros de datos institucionales de la Base de Apoyo de las Naciones Unidas en Valencia (España) y la Base Logística de las Naciones Unidas en Brindisi (Italia), así como la consolidación de las fuentes existentes de ciberinteligencia en toda la Secretaría.

5. En respuesta a una consulta sobre la situación en que se encontraban la adquisición e instalación de los sistemas de filtración de Internet (web) y correo electrónico, se informó a la Comisión Consultiva de que se había adquirido un sistema avanzado de filtración de tráfico de Internet como parte de un contrato marco existente, y de que se estaban poniendo en práctica las medidas necesarias para su aplicación, incluidas las modificaciones de la infraestructura subyacente y la adaptación de la política de filtración de Internet que existía. Para adquirir el sistema avanzado de filtración del tráfico de correo electrónico era necesario realizar un ejercicio de licitación que se había iniciado en marzo de 2013 y todavía estaba en marcha. A la espera de que concluyese el proceso de licitación, se había firmado un contrato de arrendamiento de corto plazo, a modo de arreglo provisional, que estaba en vigor desde finales de noviembre de 2013. **La Comisión recomienda que se solicite al Secretario General que, en su próximo informe sobre este asunto, garantice que los productos y servicios destinados a la ejecución del**

plan de acción para la seguridad de la información se adquieran de la forma más eficaz posible en función del costo.

6. Con respecto al curso de capacitación por computadora al que se hace referencia en el párrafo 10 a) del informe del Secretario General, se informó a la Comisión Consultiva de que se había firmado un contrato, por valor de 35.826 euros, para desarrollar un curso de capacitación por computadora con el fin de sensibilizar acerca de la seguridad de la información que cubría el "contenido básico" común determinado por el Grupo Temático sobre Seguridad de la Información de todo el sistema de las Naciones Unidas. El curso será obligatorio para todos los funcionarios y se espera que se despliegue a principios de 2014 en la plataforma común de aprendizaje electrónico de la Secretaría (Inspira). **La Comisión alienta al Secretario General a que siga tratando de obtener la colaboración de todo el sistema y considere todas las opciones que permitan a las organizaciones del sistema de las Naciones Unidas seguir cooperando y compartiendo soluciones en materia de seguridad de la información**.

7. El Secretario General indica que, 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 que permitan un control más estricto del acceso y reduzcan la vulnerabilidad a la intrusión con el fin de apoyar la aplicación de Umoja, el proyecto de planificación de los recursos institucionales. Entre estos cambios cabe citar, por ejemplo, la aplicación de una nueva red mundial de área amplia, la utilización de una capa de acceso estándar (Citrix) para todos los sistemas institucionales y la migración de las aplicaciones de programas informáticos a los centros de datos institucionales de Valencia y Brindisi. **La Comisión Consultiva recomienda a la Asamblea General que solicite al Secretario General que acelere, en la medida de lo posible, la migración de las aplicaciones a los centros de datos institucionales y que informe de manera integral sobre los avances logrados en el contexto del informe mencionado sobre la nueva estrategia de TIC**.

8. El Secretario General indica, además, que la Oficina de Tecnología de la Información y las Comunicaciones decidió, en julio de 2013, obtener una evaluación independiente de la situación de la seguridad de la información en la Secretaría, centrándose principalmente en la infraestructura en la Sede (A/68/552, párr. 8). El Secretario General declara que la evaluación validó y complementó las conclusiones internas y también reveló, entre otras cosas, que: a) las Naciones Unidas no contaban 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 los sistemas que no habían sido previamente controlados de manera digital, como 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; b) el Departamento de Apoyo a las Actividades sobre el Terreno necesitaba nuevos programas informáticos para facilitar el control y la filtración de intrusos, así como cortafuegos perfeccionados, para mejorar el entorno de seguridad tanto en la Sede como en el terreno; y c) era 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 mejorar la resistencia contra la intrusión o degradación (*ibid*., párrs. 13 a 15).

9. El Secretario General también indica que 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 podría poner en peligro a todos los lugares, y que las medidas adoptadas para ejecutar el plan de acción en la Sede debían ponerse en práctica en otros lugares de destino y habían de complementarse con una mejora significativa de la capacidad de supervisión por parte de la Organización (A/68/552, párr. 18). Además, la fragmentación de la red de TIC de la Organización hacía más difícil y costosa la tarea de garantizar la seguridad de la información. El Secretario General declara que la estrategia de la Organización ha consistido en agilizar el traslado de sus centros de datos a Valencia y a Brindisi para que puedan adoptar medidas de seguridad y vigilancia con mayor rapidez y al mismo tiempo reducir los costos y que eliminar la fragmentación será un pilar central de esta nueva estrategia de TIC (*ibid*., párr. 20).

10. **La Comisión Consultiva observa los avances realizados para ejecutar el plan de acción destinado a abordar las cuestiones de seguridad de la información, así como la intención de la Secretaría de reducir la fragmentación y los costos de desplegar las medidas de seguridad y vigilancia. La Comisión reitera las opiniones expresadas en su anterior informe con respecto a la situación en materia de seguridad de la información y sigue preocupada por que se haya tardado tanto en abordar esta cuestión (A/67/770, párr. 68).**

11. **Además, dado el alcance mundial de las Naciones Unidas y el carácter amplio de sus sistema de información, la Comisión Consultiva considera que también es necesario proteger a la Organización de una vigilancia, interceptación y recopilación de comunicaciones y datos en masa, y recomienda a la Asamblea General que solicite al Secretario General que incluya en su próximo informe algunas opciones posibles para asegurar dicha protección.**

Gobernanza, riesgos y cumplimiento

12. En la esfera de la gobernanza, el riesgo y el cumplimiento, el Secretario General indica que entre las medidas adoptadas figuran: a) la comunicación de una directiva de política de seguridad de la información a todos los jefes de departamentos y oficinas como marco general para las políticas, procedimientos y directrices de la Organización en materia de seguridad de la información; b) la elaboración en curso de 52 políticas y procedimientos de TIC para ayudar a mejorar el rendimiento del sistema, así como su seguridad e integridad de producción; c) el establecimiento de un grupo de trabajo sobre la seguridad de la información, como parte del Grupo de Coordinación de la Gestión de TIC, para que aumente el nivel de comunicación entre los lugares de destino; d) el desarrollo en curso de una función de cumplimiento interno con el fin de aumentar el cumplimiento de las políticas y procedimientos internos y las mejores prácticas del sector; y e) la aprobación por la red de TIC de la Junta de los Jefes Ejecutivos del Sistema de las Naciones Unidas para la Coordinación de un conjunto de necesidades mínimas para los sitios web de uso público, desarrolladas por el Grupo Temático sobre Seguridad de la Información de la Junta en colaboración con la Oficina de Tecnología de la Información y las Comunicaciones. Además, de conformidad con un marco normativo de seguridad establecido recientemente por el Departamento de Apoyo a las Actividades sobre el Terreno se realizaron periódicamente evaluaciones de la seguridad de los sistemas de información, infraestructura y otros activos de información desplegados en Brindisi y Valencia y en las misiones sobre el terreno (A/68/552, párr. 10 d)).

13. La Comisión Consultiva solicitó más información sobre el marco normativo de seguridad mencionado en el párrafo 10 d) del informe del Secretario General, en especial, sobre la cooperación entre la Oficina de Tecnología de la Información y las Comunicaciones y el Departamento de Apoyo a las Actividades sobre el Terreno en cuestiones relativas a la seguridad de la información, incluidos los mecanismos de coordinación empleados y la correspondiente división de funciones y responsabilidades entre ellos. Se informó a la Comisión de que dicho marco se aplicaba al Departamento de Apoyo a las Actividades sobre el Terreno en la Sede y a las misiones sobre el terreno. El Departamento de Apoyo a las Actividades sobre el Terreno también había desarrollado un marco normativo de seguridad específico para las misiones sobre el terreno destinado a abordar las necesidades operacionales y el entorno y perfil de riesgo específicos del terreno. Asimismo, al seguir manteniendo contactos con el Departamento y coordinándose con él, la Oficina de Tecnología de la Información y las Comunicaciones veló por que las directrices específicas para el terreno se adaptasen adecuadamente a las normas, políticas y recomendaciones globales de la Secretaría. Por otra parte, la Oficina de Tecnología de la Información y las Comunicaciones y el Departamento de Apoyo a las Actividades sobre el Terreno celebraron consultas periódicas y mantuvieron una estrecha colaboración con respecto a los sistemas utilizados habitualmente, y compartieron información y datos sobre incidentes y vulnerabilidades relacionados con la seguridad de la información.

14. **La Comisión Consultiva observa la publicación de una directiva común sobre la seguridad en toda la Secretaría. La Comisión recomienda a la Asamblea General que solicite al Secretario General que continúe su labor y vele por que se adopten políticas y procedimientos comunes con respecto a la seguridad de la información de forma que se garantice la rendición de cuentas a todos los niveles de la Organización. La Comisión reitera que el Secretario General también debería adoptar medidas correctivas con rapidez para superar todo obstáculo que pueda surgir en la promulgación y el cumplimiento de eficaces políticas de seguridad de la información comunes en toda la Secretaría.**

15. **Además, teniendo en cuenta la declaración del Secretario General en el sentido de que un ataque o intrusión en cualquier lugar de la red de las Naciones Unidas podría poner en peligro a todos los lugares, así como la necesidad de aplicar medidas de seguridad y sistemas de seguimiento en todos los lugares de destino, la Comisión Consultiva pone de relieve la necesidad de adoptar un enfoque de la seguridad de la información y los sistemas común y aplicable a todos los organismos de la Secretaría que garantice que no se produzca una duplicación de esfuerzos o gastos en esta esfera. La Comisión recomienda que la Asamblea General solicite al Secretario General que asegure que la estrategia a medio y largo plazo para la seguridad de la información, que será presentada en el contexto de la nueva estrategia de TIC (véase párr. 3), se base en políticas y herramientas comunes y se ocupe de la actual fragmentación del entorno de seguridad de la información de la forma más eficaz en función del costo y más eficiente posible.**

Otras cuestiones

16. La Comisión Consultiva recuerda que, hasta el momento, la Asamblea General ha aprobado la utilización de las instalaciones de Valencia como un servicio activo

secundario de telecomunicaciones y un centro institucional de datos (véanse las resoluciones 63/262 y 66/264). **La Comisión reitera su recomendación de que la Asamblea General solicite al Secretario General que asegure que se designe al centro de manera coherente en todos los documentos presentados a la Asamblea para que esta los examine, denotando su uso con fines de TIC (A/67/780/Add.10, párrs. 29 a 31).**

III. Recursos necesarios

17. En respuesta a su solicitud, la Comisión Consultiva recibió información sobre el nivel general de recursos relacionados con la seguridad que aprobó la Asamblea General y los gastos efectivos realizados en los últimos cinco años, así como detalles sobre los gastos en concepto de seguridad de la información correspondientes al bienio 2012-2013. Esta información se adjunta en los anexos II y III, respectivamente, del presente informe. La Comisión observa que los gastos en concepto de seguridad de la información prácticamente se han cuadruplicado, al aumentar de unos 1,1 millones de dólares en 2010-2011 a casi 4,1 millones en 2012-2013.

18. En respuesta a su pregunta sobre el nivel de inversión previsto para hacer frente a los problemas de seguridad relacionados con los sistemas a los que remplazará Umoja, se explicó a la Comisión Consultiva que algunos de los sistemas informáticos antiguos funcionaban gracias a sistemas operativos a los que ya no se prestaba servicio y que por tanto, se encontraban en grave riesgo, puesto que los proveedores no habían proporcionado las actualizaciones necesarias para protegerlos de nuevas vulnerabilidades. Siempre que fuera posible, esos sistemas debían cambiarse por sistemas operativos a los que sí se diera servicio. Para los casos en que no pudiera cambiarse el sistema, se habían propuesto una serie de actividades adicionales de control para detectar más a tiempo los posibles fallos de seguridad y limitar sus repercusiones. **Si bien la Comisión reconoce que es necesario garantizar la seguridad de la información de los sistemas operativos para proteger los servicios de las Naciones Unidas, también destaca que cualquier nueva inversión en los sistemas que remplazará Umoja y que serán discontinuados en el futuro próximo debería reducirse al mínimo en la medida de lo posible**.

Recursos necesarios propuestos para 2014-2015

19. En el próximo bienio, el Secretario General propone, entre otras cosas: a) ampliar la cobertura del servicio de detección de intrusos y las soluciones de filtración para dar cobertura a las oficinas situadas fuera de la Sede y las comisiones regionales; b) perfeccionar la infraestructura del cortafuegos; c) aumentar la capacidad de vigilancia de la seguridad interna; d) desplegar un sistema de gestión de las vulnerabilidades que permita a la Organización detectar de forma proactiva deficiencias concretas y establecer prioridades para su mitigación; y e) realizar controles adicionales de protección y detección para los elementos de la infraestructura no tradicionales en la Sede y para el entorno de la tecnología de la información y las comunicaciones en las oficinas situadas fuera de la Sede, las comisiones regionales y los centros de datos institucionales de Valencia y Brindisi.

20. Para implantar estas medidas, se proponen unos recursos necesarios adicionales de 3.440.700 dólares para el bienio 2014-2015, principalmente en las siguientes partidas: a) otros gastos de personal (581.400 dólares) para sufragar las necesidades en concepto de personal temporario general para un ingeniero de seguridad de la categoría P-4 que proveerá los conocimientos técnicos adicionales referidos a la aplicación del sistema de detección de intrusos que se puso en funcionamiento recientemente, y dos puestos de la categoría P-3 que cumplirán las nuevas funciones de análisis de software maligno, creación de patrones y correlación de incidentes y 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 las aplicaciones web; b) viajes de funcionarios (150.000 dólares) para sufragar los gastos de viaje de dos funcionarios a todas las oficinas situadas fuera de la Sede, las comisiones regionales y los centros de datos institucionales de Valencia y Brindisi durante al menos dos semanas; c) servicios por contrata (1.325.000 dólares) para el despliegue y funcionamiento ininterrumpido de sistemas de detección de intrusos (800.000 dólares), un sistema de gestión de las vulnerabilidades (25.000 dólares); y conocimientos altamente especializados para realizar, en función de las necesidades, actividades para la ejecución ininterrumpida de la estrategia de seguridad de la información de la Secretaría (500.000 dólares); d) mobiliario y equipo (1.325.000 dólares) para introducir mejoras a la infraestructura del cortafuegos (1.000.000 de dólares), capacidades de supervisión continua (200.000 dólares) y pruebas de seguridad de las aplicaciones web (125.000 dólares); y e) gastos generales de funcionamiento (59.300 dólares).

21. En respuesta a sus preguntas, se comunicó a la Comisión Consultiva que en los recursos propuestos en la sección 29E del proyecto de presupuesto por programas para 2014-2015 se habían previsto los fondos necesarios para que continuaran desarrollándose las tareas de seguridad de la información y gestión de los riesgos siguientes: a) desarrollo y mantenimiento de la política sobre seguridad de la información y vigilancia del cumplimiento en todas las dependencias orgánicas; b) prestación de apoyo a las actividades de evaluación y mitigación de los riesgos relacionados con la tecnología de la información y las comunicaciones; c) coordinación y prestación de asistencia para gestionar incidentes relacionados con la seguridad de la información; d) coordinación de respuestas y cumplimiento de las recomendaciones de los Auditores; y e) tramitación de todas las solicitudes de acceso al IMIS, el Sistema de Archivo de Documentos (ODS), acceso remoto al IMIS y a Nucleus y otras solicitudes relativas a los registros de seguridad. Con respecto al personal existente, también se explicó a la Comisión que la Dependencia de Seguridad de la Información y Gestión de los Riesgos de la Sección de Seguridad y Arquitectura de la Oficina de Tecnología de la Información y las Comunicaciones estaba formada por un Oficial de Seguridad de la Información (P-4), un Oficial de Seguridad de la Información (P-3) y dos Auxiliares de Seguridad de la Información (Cuadro de Servicios Generales (otras categorías)). Este equipo contaba con el apoyo de dos plazas de personal temporario general equiparables a la categoría P-4 que hacían las funciones de Oficial de Cumplimiento y Especialista de Recuperación tras los Desastres. Asimismo, en la mayoría del resto de los departamentos y oficinas, las actividades relacionadas con la seguridad de la información estaban a cargo de personal y contratistas que también cumplían otras funciones. Según un estudio realizado a principios de 2013, la seguridad de la tecnología de la información y las comunicaciones de toda la Secretaría estaba en manos del

equivalente a un total de 12,5 puestos a tiempo completo del Cuadro Orgánico y del Cuadro de Servicios Generales.

22. La Comisión Consultiva recuerda que, en su resolución 67/254, la Asamblea General solicitó al Secretario General que la mantuviera al tanto sobre los problemas de seguridad de la información en el contexto del proyecto de presupuesto por programas para el bienio 2014-2015. **A pesar de la declaración realizada por el Secretario General de que sus propuestas se basan, en parte, en el resultado de la evaluación de seguridad llevada a cabo en junio de 2013, incluida la ampliación del alcance de las actividades en 2014 para reforzar aún más la seguridad de la información en las oficinas situadas fuera de la Sede, las comisiones regionales y las misiones sobre el terreno, la Comisión opina que algunos de los nuevos recursos propuestos en el informe del Secretario General podrían haberse previsto e incluido en el proyecto del presupuesto por programas para 2014-2015. La Comisión también observa que las propuestas del Secretario General hacen referencia a necesidades de naturaleza estructural y permanente, que también exigirán que se revise el programa de trabajo aprobado de la Oficina de Tecnología de la Información y las Comunicaciones para el período 2014-2015 (véase A/67/6/Rev.1, Programa 25). La Comisión recomienda a la Asamblea General que solicite al Secretario General que se asegure de que, en el futuro, se haga todo lo posible para incluir en el presupuesto por programas bienal las necesidades que sean permanentes y, de este modo, facilitar el examen de las necesidades generales de la Oficina de Tecnología de la Información y las Comunicaciones**.

23. **Asimismo, dada la necesidad de que exista un planteamiento común y global con respecto a la seguridad de la información en toda la Secretaría basado en políticas e instrumentos comunes (véanse los párrs. 14 y 15), la Comisión Consultiva también recomienda a la Asamblea General que solicite al Secretario General que prorratee los recursos necesarios para la seguridad de la información conforme a las mismas disposiciones de participación en la financiación de los gastos del proyecto de planificación de los recursos institucionales (véase la resolución 63/262)**.

IV. Conclusiones y recomendaciones

24. Las medidas que deberá adoptar la Asamblea General se indican en el párrafo 30 del informe del Secretario General. **Con sujeción a las observaciones y recomendaciones expresadas en el presente informe, la Comisión Consultiva recomienda a la Asamblea General que tome nota del informe del Secretario General. La Comisión también recomienda a la Asamblea General que solicite al Secretario General que: a) cubra los recursos adicionales para personal temporario y viajes de funcionarios con los recursos contemplados en el proyecto de presupuesto por programas para el bienio 2014-2015; y b) deje constancia en el informe de ejecución pertinente de los gastos adicionales necesarios para servicios por contrata (A/68/552, párr. 27) o mobiliario y equipo (*ibid*., párr. 29)**.

Anexo I

Resumen de los problemas de seguridad detectados y sus soluciones

Problema	*Solución*	*Descripción*
Incapacidad para controlar o detectar el tráfico en red generado por actividades encubiertas o tecnológicamente avanzadas y permanentes de grupos vinculados a ataques persistentes y tecnológicamente avanzados. Falta de visibilidad de red	Servicios de detección de intrusos	Los servicios de detección de intrusos se encargarán de colocar dispositivos estratégicamente en la red para que todo el tráfico de red sea visible. El servicio alertará de las actividades sospechosas y capturará el tráfico de red en tiempo real. Las alertas se enviarán a una empresa de servicios, donde las analizará un equipo de expertos que proporcionará notificaciones críticas con indicaciones sobre medidas a adoptar al personal de las Naciones Unidas encargado de la seguridad
Riesgo constante para los activos de las Naciones Unidas, como las estaciones de trabajo y las computadoras de escritorio, resultantes del uso de software maligno muy personalizado enviado por correo electrónico. Este tipo de ataques ha aumentado un 76% en nueve meses en 2013, frente a los riesgos detectados en 2012	Mayor filtración de correos electrónicos	El software maligno personalizado se diseña de tal forma que las soluciones de antivirus tradicionales no puedan detectarlo. Las soluciones de filtración avanzadas utilizan técnicas que analizan el comportamiento de dichos archivos y detectan el software maligno con más probabilidades de haber pasado desapercibido para las soluciones existentes
Incapacidad para proteger el sistema de ataques tecnológicamente avanzados y persistentes	Cortafuegos de próxima generación	Actualmente muchos ataques tienen por objeto eludir los cortafuegos tradicionales. En Nueva York y en dos centros de datos institucionales se han instalado cortafuegos de próxima generación o modernos, que protegen más escrupulosamente a la Organización. Se solicita llevar esta capacidad a todos los lugares de destino para que toda la red de las Naciones Unidas esté protegida de manera uniforme. El personal que se solicita es crucial para la configuración y el funcionamiento iniciales del sistema
Incapacidad para hacer correlaciones de datos procedentes de distintos sistemas para definir tendencias de actividad y hacer referencias a	Vigilancia permanente (análisis de registros)	El sistema recopila los registros de numerosos sistemas para descifrar las tendencias de ataque en toda la red, permite acceder rápidamente al historial de un ataque cuando se encuentra y es sumamente

Problema	*Solución*	*Descripción*
datos históricos (registrados) del sistema. Falta de visibilidad		importante para describir el uso general de todos los sistemas de seguridad. El personal que se solicita es crucial para la configuración y puesta en marcha del sistema
Falta de recursos para determinar adecuadamente las fuentes de los ataques y el alcance total del daño que conlleva un fallo en la seguridad de la información	Software maligno, análisis y respuesta a incidentes	Con el personal que se solicita se dispondrá de capacidad suficiente para examinar rápidamente la información que podría perderse tras un fallo o el mecanismo de ataque, complementando y aumentando de esta manera el conjunto de conocimientos del personal de las Naciones Unidas en esta esfera
Falta de cumplimiento, actualización y ajuste de los sistemas de las Naciones Unidas, lo que en su conjunto conlleva una mayor vulnerabilidad	Evaluaciones de vulnerabilidad	Vigilancia y verificación permanentes del cumplimiento mediante el uso de software automatizado para que todos los sistemas de las Naciones Unidas estén siempre “actualizados” y se detecten las vulnerabilidades restantes

Anexo II

Estimación de los gastos anuales y totales en concepto de tecnología de la información y las comunicaciones (TIC) desde 2010

(En dólares de los Estados Unidos)

	Bienio 2010-2011			*Bienio 2012-2013*		
	2010	*2011*	*Total*	*2012*	*2013*	*Total*
Puestos	318 000,00	318 000,00	636 000,00	719 600,00	773 450,00	1 493 050,00
Consultores		177 221,00	177 221,00	112 777,00		112 777,00
Capacitación				436,67		436,67
Viajes de consultores ISO 27001				14 130,00	2 995,00	17 125,00
Evaluaciones de seguridad independientes					60 000,00	60 000,00
Evaluaciones ISO 27001	24 000,00	33 025,49	57 025,49	38 170,90	1 545,00	39 715,90
Software especializado de protección de servidores		64 276,10	64 276,10	7 122,15	7 122,15	14 244,30
Software de protección de terminales	4 144,50	193 435,18	197 579,68	234 711,39	300 611,97	535 323,36
Software de gobernanza y cumplimiento				19 703,00		19 703,00
Solución avanzada para la filtración de correos electrónicos para la Sede de las Naciones Unidas					200 000,00	200 000,00
Cortafuegos para la Sede de las Naciones Unidas				307 968,80	540 000,00	847 968,80
Medidas adicionales del plan de acción para las TIC					715 158,00	715 158,00
Total	**346 144,50**	**785 957,77**	**1 132 102,27**	**1 454 619,91**	**2 600 882,12**	**4 055 502,03**

Anexo III

Gastos para mantener la seguridad de la información durante el bienio 2012-2013

(En dólares de los Estados Unidos)

Gasto	*Concepto*	*Descripción*	*Precio*	*Cantidad*	*Total*
1.	**Órdenes de compras de corto plazo (<4 000)**				
	Software para la realización de pruebas manuales de seguridad de Internet	Plataforma integrada para la realización de pruebas de seguridad a las aplicaciones web. Software único con numerosas funciones manuales orientadas a profesionales para usuarios avanzados. Herramienta de alto valor y bajo costo	300	2	600
	Software de examen básico de vulnerabilidad	Herramienta automatizada de análisis de vulnerabilidad de redes y servidores, de bajo costo, que puede utilizarse en varios servidores	3 900	1	3 900
	Herramientas de información y análisis	Aplicación de información y análisis, de código abierto, con una aplicación para el registro de incidencias	760 + 200	1	960
	Software de análisis	Herramientas punteras de análisis que pueden utilizarse en computadoras de escritorio, servidores y dispositivos móviles	2 999 + 599	1	3 598
	Herramienta de análisis del disco duro	Utilizada para conectar externamente discos duros del sistema de alerta de tecnología avanzada a una computadora para labores de copiado y/o análisis	75	2	150
	Subtotal				**9 208**
2.	**Solicitud de presupuesto (<40 000)**				
	Herramienta de examen de la seguridad para la comprobación de sitios web	Herramienta de software para el análisis y la comprobación automatizados de la seguridad de sitios web	5 950	1	5 950
	Herramienta de análisis de la seguridad para la comprobación de sitios web	Herramienta de software para el análisis y la comprobación automatizados de la seguridad de sitios web	20 300	1	15 000
	Software para la gestión de cortafuegos	Software para la gestión y el rastreo de reglas de cortafuegos	35 000	1	35 000
	Subtotal				**55 950**

Gasto	*Concepto*	*Descripción*	*Precio*	*Cantidad*	*Total*
3.	**Licitaciones (<30.000-200.000)**				
	Servicios por contrata (experto en cortafuegos)	Contratación de consultor externo para apoyar la remodelación de la red e instalación de cortafuegos. Un mes, a finales de noviembre o principios de diciembre	40 000	1	40 000
	Subtotal				**40 000**
4.	**Solicitud de propuestas (en curso, diversas)**				
	Curso de sensibilización sobre la seguridad de la información	Desarrollo de un módulo de sensibilización sobre la seguridad de la información en HTML5 para Inspira	30 000	1	30 000
	Sistema avanzado de filtración de correos electrónicos	Suministro de dispositivos y software FireEye de protección contra software maligno para correos electrónicos, incluidos servicios profesionales para la filtración avanzada de correos electrónicos	230 000	1	230 000
	Cortafuegos Checkpoint Layer 7	Compra de varios cortafuegos Checkpoint Layer 7 y blades complementarias	540 000	1	540 000
	Servicios de seguridad gestionada	Contrato plurianual para servicios de seguridad gestionada, que incluya el hardware, el software y conocimientos técnicos externos sobre seguridad para vigilancia de redes	350 000	1	350 000
	Subtotal				**1 150 000**
	Total general				**1 255 158**