S

OMPI

SCIT/7/12
ORIGINAL: Inglés
FECHA: 26 de abril de 2002

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL
GINEBRA

COMITÉ PERMANENTE DE TECNOLOGÍAS DE LA INFORMACIÓN

PLENARIO
Séptima sesión
Ginebra, 10 a 14 de junio de 2002

RESEÑA DE LAS POLÍTICAS DE LA OMPI EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Documento preparado por la Secretaría

INTRODUCCIÓN

1. La aplicación y la utilización generalizada de las tecnologías de la información y comunicación, con inclusión de las redes y entornos de procesamiento distribuido, entrañan la aparición de nuevas cuestiones. Las redes proporcionan una mayor flexibilidad para el acceso y distribución de la información y recursos que permiten el inicio de operaciones en la estación de trabajo. Sin embargo, esas ventajas tienen por consecuencia el incremento de la exposición de la información valiosa y, por consiguiente, es necesario aplicar estrategias destinadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información, así como la de los sistemas de información.

2. El presente documento contiene una reseña de las políticas de la OMPI en materia de seguridad de la información y de las estrategias para su ejecución.

ÁMBITO

3. Las políticas de la OMPI en materia de seguridad de la información a todos los empleados y miembros del personal de la OMPI, los consultores externos, el personal temporero y los contratistas externos que trabajan para la OMPI. Los empleados de la Organización deberán velar por que los contratos que se concluyan con particulares y empresas a los que se confía información valiosa, por la índole de su relación con la OMPI, sean objeto de políticas en materia de seguridad, salvo que se disponga de otro modo. Las políticas abordan todos los aspectos de la seguridad de la información, que incluyen desde el diseño inicial de un sistema de información hasta su aplicación y funcionamiento. También contemplan cualquier dispositivo utilizado para almacenar, procesar o comunicar la información de la OMPI. Las políticas se aplican independientemente de la forma en que figura la información (en forma escrita, oral, impresa, electrónica y en otras formas), de la tecnología utilizada para gestionarla y de su ubicación (por ejemplo, en la oficina, en un lugar distante, en un avión).

GESTIÓN DE LA SEGURIDAD

4. La gestión de la seguridad procura establecer controles y adoptar medidas destinadas a reducir al mínimo el riesgo de pérdida de información y de sistemas de recursos, la alteración de los datos, la perturbación del acceso a los datos y la divulgación no autorizada de la información. La gestión de la seguridad se cumple mediante la elaboración de políticas eficaces, la aplicación estricta de las normas y procedimientos a fin de garantizar la confidencialidad y la integridad de la información, los programas informáticos, los sistemas y redes de la OMPI, así como su disponibilidad para los usuarios autorizados.

Confidencialidad

5. La confidencialidad se relaciona con la protección de la información contra el acceso no autorizado, independientemente del lugar en que se encuentre o del modo en que se almacene. La información valiosa debe recibir un nivel de protección superior al que se otorgue al resto de la información. Las políticas de la OMPI en materia de seguridad de la información proporcionan un marco para la clasificación de los datos que incluye indicaciones sobre las exigencias de seguridad vinculadas con esa política.

Integridad

6. Se entiende por integridad la protección de la información, las aplicaciones de programas informáticos, los sistemas y redes contra las modificaciones no intencionales, no autorizadas o accidentales. También es importante proteger los procedimientos o programas utilizados en la manipulación de los datos. La información debe presentarse a los titulares y usuarios de la información de manera segura, precisa, completa y oportuna. Para el logro de la integridad es esencial la identificación y autorización de todos los usuarios que acceden a la información, mediante la utilización de la supervisión manual y automatizada.

Disponibilidad

7. La disponibilidad es la garantía de que los usuarios autorizados tengan acceso a la información y los recursos de la OMPI. La disponibilidad comprende dos cuestiones, a saber, la denegación del servicio causada por la falta de controles de seguridad (por ejemplo, la

destrucción de datos o del equipo, los virus informáticos), y la pérdida de servicios de los recursos de información debido a desastres naturales (por ejemplo, tormentas, inundaciones, incendios). La denegación del servicio se considera como parte de la gestión de la seguridad. La pérdida de los servicios se aborda como parte de la continuidad del procedimiento de planificación.

FUNCIONES Y RESPONSABILIDADES

8. La responsabilidad en cuanto a la seguridad de la información que se maneja diariamente es parte de la obligación cotidiana de cada empleado. Los miembros del personal deben permanecer conscientes de la necesidad de proteger los activos de información de la OMPI. Con objeto de coordinar las actividades en materia de seguridad de la información en la OMPI, se han definido tres categorías de funciones, una de las cuales se aplica al menos a cada empleado. Esas categorías definen las responsabilidades generales en la OMPI respecto de la seguridad de la información:

1) *Titular* – La OMPI es el titular absoluto de la información, las aplicaciones informáticas y los sistemas en su totalidad, en el contexto de las políticas en materia de seguridad de la información. Dentro de ese marco, los titulares son las personas a las que se atribuye la titularidad de la información o de los sistemas de información utilizados por sus unidades funcionales respectivas. Entre ellos cabe mencionar el personal directivo, los directores de programas y los administradores de programas o sus representantes, encargados de la adquisición, desarrollo y mantenimiento de los sistemas que procesan la información de la OMPI. Los titulares tienen a su cargo la determinación del derecho de acceso y el establecimiento de criterios de seguridad respecto de la información que se encuentra bajo su control.

2) *Custodios* – Los custodios son las personas que están en posesión material o lógica de la información de la OMPI o de la información que se haya confiado a la Organización. Se consideran custodios los miembros del personal y los administradores del sistema. En el caso de la información archivada en una computadora personal, el custodio será el usuario de esa computadora. En ausencia de titularidad específica, los custodios asumen la responsabilidad de los titulares.

3) *Usuario* – Los usuarios son las personas que en sus actividades cotidianas procesan información que pertenece o se encuentra bajo la custodia de otros. Los usuarios están encargados del cumplimiento de las políticas, normas y reglamentos en materia de seguridad establecidos por los titulares. En el caso de que se planteen cuestiones sobre el acceso a la información, los usuarios deben derivarlas a los titulares o custodios de esa información. Los usuarios pueden ser empleados, personal temporero, contratistas, consultores o terceros con los que se hayan concluido acuerdos especiales.

9. En razón de la índole valiosa y a la importancia de las políticas en materia de seguridad de la información, y a los fines de su ejecución eficaz, la División de Proyectos de Tecnologías de la Información está estructurada de la manera siguiente:

Director de los Servicios de Tecnologías de la Información

10. En materia de seguridad de la información, la función del Director de los Servicios de Tecnologías de la Información es informar al personal directivo sobre el riesgo que supone la aplicación de tecnologías nuevas y distribuidas, así como sobre la necesidad de elaborar la infraestructura, los procedimientos y las políticas de seguridad adecuados.

Oficial de seguridad de la información

11. El oficial de seguridad de la información de la OMPI tiene a su cargo la responsabilidad general de las cuestiones de seguridad de la información. Esas responsabilidades están encaminadas a:

– garantizar que los controles adecuados de acceso y verificación del usuario estén en funcionamiento;
– garantizar la revisión, la actualización y el mantenimiento de las políticas, normas y procedimientos documentados de seguridad;
– evaluar los riesgos de seguridad, el uso indebido o las situaciones de incumplimiento, y velar por la aplicación de los controles de seguridad destinados a prevenirlos;
– elaborar y ejecutar un programa de sensibilización en materia de seguridad.

Servicio de Asistencia Técnica

12. El Servicio de Asistencia Técnica está encargado de dar respuestas iniciales a las cuestiones relacionadas con la seguridad, de conformidad con las políticas, normas y procedimientos y, de corresponder, la remisión de las cuestiones relacionadas con la seguridad a la división de administración pertinente, de conformidad con el procedimiento jerárquico aplicable cuando se produzca un incidente que afecte la seguridad de la información. El Servicio de Asistencia Técnica es el servicio central en materia de registro del usuario y, junto con los administradores de seguridad, proporciona contraseñas de gestión.

Gestión orgánica

13. En el presente documento la expresión gestión orgánica hace referencia a todos los programas o directores de división de la OMPI encargados de la ejecución material o práctica de las políticas de seguridad de la OMPI en sus propios sectores administrativos funcionales. La gestión orgánica tiene a su cargo la elaboración de la estrategia general de seguridad respecto de la información correspondiente a la división. Esta labor incluye establecer la clasificación de la información perteneciente a la división según el nivel de sensibilidad y disponibilidad requeridos por la información. La gestión orgánica también está a cargo de autorizar el nivel de acceso a la información que se encuentra bajo su responsabilidad.

EJECUCIÓN

Recursos de información

14. La infraestructura de los sistemas de información deberá protegerse para garantizar que las personas no autorizadas no puedan acceder al sistema, no provoquen daños físicos, ni modifiquen componentes internos que puedan afectar los resultados del procesamiento de la información. Los controles en materia de entorno y de seguridad deberán ser adecuados al

nivel de riesgo. Al determinar qué controles de seguridad y de entorno son adecuados, es necesario evaluar la relación entre el riesgo y el costo que supone aplicar los controles mencionados.

15. La clasificación de los activos de información responde al objetivo de facilitar un medio de comunicar el nivel de protección que debe otorgarse. Las exigencias en materia de seguridad de información varían según la sensibilidad y el nivel de importancia de la información o de los sistemas vinculados con esa información.

16. Los usuarios deben respetar el derecho de autor, las leyes de patentes y los acuerdos de licencia de propiedad intelectual, cuyo contenido conocen o deben conocer. Los titulares garantizarán que los custodios y usuarios sean conscientes de las disposiciones pertinentes de los acuerdos de licencia.

17. El titular de los datos, los custodios y el oficial de seguridad de la información examinarán periódicamente la serie actual de derechos de acceso y actualizarán las capacidades concedidas a cada individuo del sistema para garantizar que se haya concedido el nivel de acceso adecuado y cerciorarse de que no es necesario efectuar modificaciones.

Acceso a los sistemas y a la información

18. El acceso a la información y a los sistemas se proporciona conforme a las exigencias de la actividad administrativa. Como parte de su responsabilidad en la gestión, se exige a los titulares que revisen todos los requerimientos de acceso a la información o a los sistemas, y que verifiquen que tales accesos satisfagan una necesidad justificada de la actividad administrativa. La autorización de las necesidades de acceso debe comunicarse al custodio.

19. Todos los requerimientos de información entre divisiones deben cumplir las mismas exigencias de actividad. Al adoptar la decisión de otorgar o de denegar el acceso, el titular debería considerar los beneficios para la OMPI de conceder el acceso, el tipo de acceso solicitado y cualquier riesgo vinculado con ese acceso.

20. Cuando se conceda una autorización de acceso externo a la información de la OMPI considerada secreta o confidencial, deben impartirse al receptor instrucciones detalladas, notificándole toda exigencia de seguridad, incluida la necesidad de mantener la confidencialidad de la información, cualquier restricción que afecte la distribución de la información dentro de la organización y el procedimiento para la destrucción o devolución de la información, una vez transcurrido el período de acceso.

21. Cuando se notifique al Director de una división la terminación de la relación de trabajo, la renuncia o la transferencia de un empleado, deberá revisar, antes de la transferencia o separación de la OMPI la disposición de los datos y ficheros del usuario en la red y los archivos de aplicación. El Director deberá comunicar por escrito al servicio de asistencia que esos ficheros sean transferidos o destruidos. Para la utilización de cualquier dato se deberán observar las orientaciones definidas por la Política de Conservación de Documentos o hasta la aplicación de esa política, las instrucciones del Director de Programa, con arreglo al Manual de la OMPI sobre Políticas de Seguridad de la Información (ISPM).

Supervisión de la seguridad

22. Los administradores de redes, sistemas y aplicaciones están encargados de aplicar las medidas adecuadas para detectar los intentos de comprometer la confidencialidad o integridad de la información o de los sistemas de información. Al aplicar los dispositivos de supervisión, debería considerarse, según la extensión del riesgo, qué situaciones deben supervisarse, los medios más eficaces para supervisar las actividades de seguridad, los recursos disponibles a tales efectos y las restricciones del sistema que limiten la capacidad de supervisar eventos conexos en materia de seguridad. Como parte de esas medidas deberán mantenerse actualizados los programas informáticos de detección de virus en el sector local del entorno de la red, así como en los sistemas con un alto riesgo de contaminación.

Programa de sensibilización en materia de seguridad de la información

23. La dirección está encargada de velar porque todos los usuarios de la información sepan cómo proteger los activos de información de la OMPI (incluida la información y los recursos de información) y conozcan la manera de cumplir con las políticas, normas y procedimientos en materia de seguridad.

24. El oficial de seguridad de la información, con la ayuda de la División de Gestión de Recursos Humanos, está encargado de elaborar un programa de sensibilización en materia de seguridad de la información destinado a fomentar la toma de conciencia del personal al respecto.

CONTROLES

Evaluación del riesgo

25. La evaluación del riesgo supone identificar el carácter valioso y crítico de la información y las consecuencias para la OMPI si la información es divulgada, modificada o destruida. Las técnicas de evaluación del riesgo pueden incluir métodos oficiales para determinar las repercusiones financieras y operativos de un incidente de seguridad, así como técnicas de evaluación menos formales. El procedimiento de evaluación del riesgo deberá incluir los siguientes elementos:

– establecimiento de un inventario de los activos de información que deben protegerse;
– evaluación del grado de sensibilidad de la información y de las consecuencias de su divulgación;
– evaluación de la criticidad de la información y de las consecuencias para los procedimientos administrativos en caso de falta de acceso a la información y los sistemas de procesamiento de la información;
– la confirmación por los administradores de la medida en que el riesgo será aceptado, atenuado o transferido;
– elaboración de una estrategia de control del riesgo;
– determinación de la observancia de las clasificaciones de la información efectuadas por la OMPI.

26. Corresponde a los administradores evaluar el nivel del riesgo para la OMPI relacionado con la confidencialidad, la integridad y disponibilidad de la información, así como los controles necesarios para mitigar eficazmente ese riesgo. Las medidas de control del riesgo

deberían abordar la información, los procedimientos utilizados para crear, modificar o difundir esa información, así como para presentar informes al respecto, y el entorno de esos procedimientos. Este procedimiento también debería incorporar la clasificación de la información, de conformidad con las normas de la OMPI sobre seguridad de la información, a una de las categorías siguientes:

– secreta
– confidencial
– de uso interno exclusivamente
– pública

27. El Manual de la OMPI sobre Políticas de Seguridad de la Información proporciona un marco para clasificar el grado de confidencialidad, integridad y disponibilidad de la información y las exigencias de seguridad necesarias correspondientes a cada clasificación.

Políticas de seguridad funcional

28. En el Manual de la OMPI sobre Políticas de Seguridad de la Información figuran las políticas funcionales en materia de seguridad. En él se define el marco de la estrategia de la OMPI en materia de seguridad de la información, así como su estructura y aplicación, centrado en la tecnología para el almacenamiento, el procesamiento y la transmisión de la información, así como en las prácticas administrativas y operativas destinadas a la protección de la información en todas sus formas, tanto dentro como fuera de la OMPI. Se establece y mantiene por el oficial de seguridad de la información, con la aprobación del Director General.

Normas de seguridad de la información

29. En el Manual de la OMPI sobre Normas de Seguridad de la Información (ISSM) es un documento en el que se establecen los métodos para el logro de los objetivos de seguridad contemplados en el Manual de la OMPI sobre Políticas de Seguridad de la Información. Fundándose en esas normas, se elaborarán principios básicos de seguridad para una plataforma y aplicación específica. El oficial de seguridad de la información, está encargado de establecer y mantener el Manual de la OMPI sobre Normas de Seguridad de la Información, con la aprobación del Director de los Servicios de Tecnologías de la Información.

Procedimientos en materia de seguridad de la información

30. A efectos de la aplicación de las políticas y normas de la OMPI en materia de seguridad de la información, se elaborarán diversos procedimientos. En las políticas y normas se definirán las etapas graduales que deberán cumplirse para llevar a cabo una actividad específica de seguridad de la información.

Procedimientos y orientaciones para las divisiones

31. Cada división deberá elaborar y mantener procedimientos y orientaciones adicionales propios que sirvan de apoyo a las políticas generales en materia de seguridad de la información, de ser necesario, para satisfacer necesidades específicas.

32. Se invita al Plenario del SCIT a tomar nota de la información contenida en el presente documento.

[Fin del documento]