

# Seguridad en Windows 2000 Server

Anita Alegre López<sup>1</sup>, Miriam Carolina Quintana<sup>2</sup>

<sup>1</sup> Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina.  
E-mail: aalegrelopez@yahoo.com.ar

<sup>2</sup> Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina.  
E-mail: ckintana@hotmail.com

**Resumen.** Mantener la seguridad de los sistemas conectados a Internet es una preocupación fundamental. Toda compañía, no importa si grande o pequeña, merece garantías de seguridad en todas las operaciones que realice a través de la red. El objetivo de este trabajo es brindar pautas para mantener la seguridad usando el Strategic Technology Protection Program (STPP).

## 1. Introducción

A medida que aumenta la interconexión global del planeta, se está convirtiendo en realidad el sueño futurista de disponer de la información en cualquier lugar, en cualquier momento y en cualquier dispositivo. Las empresas y sus clientes sólo almacenarán sus datos confidenciales en un entorno de este tipo si se les garantiza la seguridad del mismo.

La Encuesta sobre delitos y seguridad informáticos del 2001 (Computer Crime and Security Survey) publicada por el CSI (Computer Security Institute) y el FBI (Federal Bureau of Investigation) indica que el 85 por ciento de las grandes empresas y agencias del gobierno detectaron infracciones de seguridad.

En los meses recientes se ha producido una lluvia de ataques a entornos informáticos, muchos de ellos a través de Internet y a equipos con el sistema operativo Microsoft® Windows®. Sin embargo, éstos son sólo los problemas de seguridad más notorios a los que se enfrentan las empresas en la actualidad. En este estudio se describen las distintas amenazas de seguridad para dicho entorno y se explica la mejor manera de protegerse.

Independientemente de cuál sea el entorno, es muy recomendable tomarse en serio la seguridad. Muchas organizaciones cometen el error de subestimar el valor del entorno de tecnología de la información (TI), generalmente porque no tienen en cuenta costos indirectos importantes. Si el ataque es suficientemente grave, las pérdidas podrían ascender al valor de la organización. Por ejemplo, un ataque que modifique sutilmente el sitio Web corporativo para anunciar malas noticias falsas podría hundir el valor en bolsa de la corporación. Al evaluar los gastos de seguridad, debe incluirse también los costos indirectos asociados a cualquier ataque, así como los costos derivados de la pérdida de funcionalidad de los sistemas de TI.

Los sistemas informáticos más seguros del mundo son los que están completamente aislados de los usuarios y de otros sistemas. Sin embargo, en el

mundo real normalmente necesitamos sistemas informáticos que funcionen en red, a menudo en redes públicas. A continuación identificamos los riesgos inherentes a un entorno de red y determinamos el nivel de seguridad apropiado para el entorno; también indicamos los pasos necesarios para alcanzar ese nivel de seguridad. Aunque está dirigida a clientes empresariales, gran parte de esta guía es válida para organizaciones de cualquier tamaño.

### **Microsoft Operations Framework (MOF)**

Para que las operaciones del entorno funcionen de la forma más eficaz, se deben administrar de forma efectiva. Para ayudarle, Microsoft ha desarrollado Microsoft Operations Framework (MOF). Las instrucciones de MOF ayudarán a garantizar la seguridad, la confiabilidad, la disponibilidad, el soporte y la capacidad de administración de sus sistemas de producción fundamentales [1].

El modelo de procesos MOF se divide en cuatro cuadrantes integrados de la manera siguiente:

1. Cambio.
2. Funcionamiento.
3. Soporte.
4. Optimización.

Juntas, las fases forman un ciclo de vida en espiral (consulte la Figura 1) que se puede aplicar a todo, desde una aplicación específica a un entorno de operaciones completo con varios centros de datos.

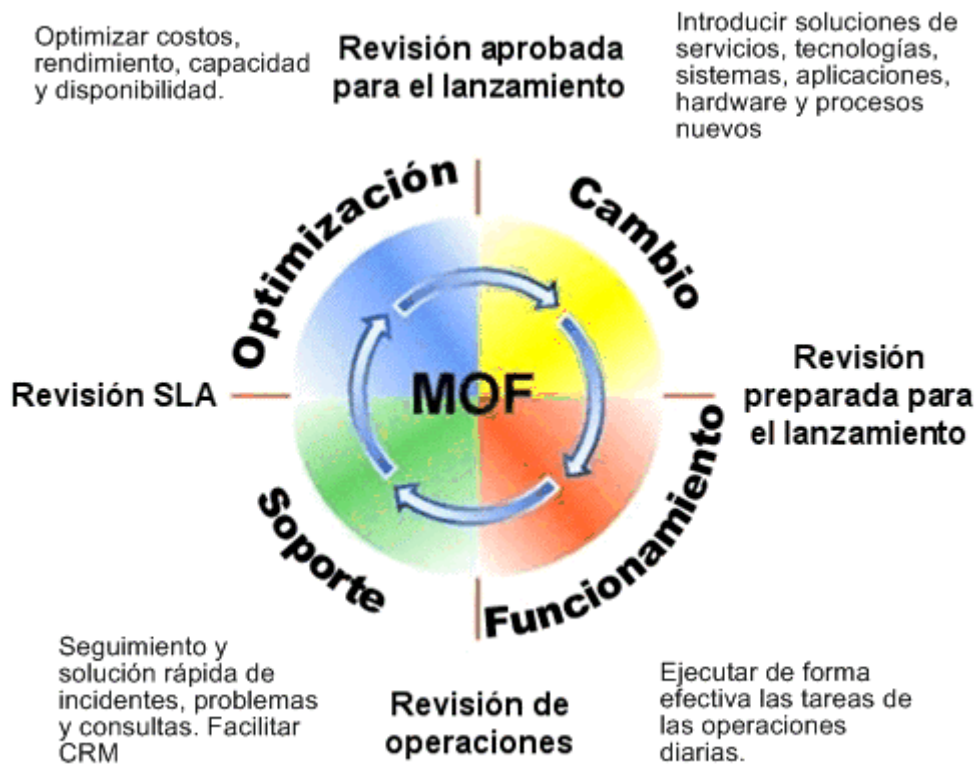


Figura 1.

### Modelo de procesos MOF

El modelo de procesos se apoya en 20 funciones de administración de servicios (SMF, service management functions) y un modelo de equipos y otro de riesgos, ambos integrados. Cada cuadrante se apoya en la revisión de administración de operaciones correspondiente (también denominada hito de revisión), en la que se valora la eficacia de las funciones de administración de servicios del cuadrante.

## **Implementar y mantener la seguridad**

En octubre de 2001, Microsoft lanzó una iniciativa denominada Programa Estratégico de Protección de Tecnología (STPP, Strategic Technology Protection Program). El objetivo de este programa es integrar los productos, los servicios y el soporte de Microsoft dedicados a la seguridad. Microsoft divide el proceso de mantener un entorno seguro en dos fases relacionadas: implementar la seguridad y mantener la seguridad.

## **2. Definición de riesgo de seguridad**

A medida que evolucionan los sistemas de TI, también lo hacen las amenazas a la seguridad que estos pueden sufrir. Para proteger el entorno de forma eficaz contra los ataques, es necesario conocer con detalle los peligros que se pueden encontrar.

Al identificar las amenazas a la seguridad, se deben tener en cuenta dos factores principales: los tipos de ataques que seguramente se sufrirá y los lugares donde pueden tener lugar.

Muchas organizaciones no tienen en cuenta el segundo factor, pues asumen que un ataque grave sólo puede venir del exterior (normalmente, a través de su conexión a Internet).

Muchas empresas pueden no estar al corriente de que se están dando ataques internos, básicamente porque no comprueban si existen.

### **Administración de riesgos**

No existe un entorno de TI totalmente seguro y al mismo tiempo útil. Al examinar el entorno, se deberá evaluar los riesgos que sufre actualmente, determinar un nivel de riesgo aceptable y mantener el riesgo a ese nivel o por debajo del mismo. Los riesgos se reducen aumentando la seguridad del entorno.

Para entender los principios de la administración de riesgos, es necesario entender algunos términos básicos utilizados en el proceso de los mismos. Estos incluyen recursos, amenazas, vulnerabilidades, explotaciones y contramedidas.

Recursos: un recurso es cualquier elemento del entorno que intente proteger. Puede tratarse de datos, aplicaciones, servidores, enrutadores e incluso personas. El objetivo de la seguridad es evitar que los recursos sufran ataques.

Amenazas: una amenaza es una persona, un lugar o un elemento que puede tener acceso a los recursos y dañarlos.

Vulnerabilidades: una vulnerabilidad es un punto en el que un recurso es susceptible de ser atacado. Se puede interpretar como un punto débil.

Explotación: una amenaza que se aprovecha de una vulnerabilidad del entorno puede tener acceso a un recurso. Este tipo de ataque se denomina explotación.

Contramedidas: las contramedidas se aplican para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo en el entorno.

### **3. Administrar la seguridad con la Directiva de Grupo de Windows 2000**

Una vez determinado el nivel de riesgo apropiado para el entorno y establecida la directiva de seguridad general, deberá empezar a asegurar el entorno. En un entorno basado en Windows 2000, esto se lleva a cabo principalmente por medio de la Directiva de grupo.

Muchos de los valores de configuración de la seguridad se definen en Windows 2000 a través de la Directiva de grupo, cuyo fin es controlar el comportamiento de los objetos en el equipo local y en el servicio de directorio Active Directory™. Es importante asegurarse de que estas directivas están correctamente configuradas y de que se supervisan para que no las modifiquen sin autorización previa.

### **4. Asegurar servidores basándose en su función**

Se deben tener en cuenta también las directivas de línea de base que pueden definirse para todos los servidores miembros y controladores de dominio de la organización, y otras modificaciones que se pueden aplicar a funciones específicas del servidor.

Este enfoque permite que los administradores bloqueen los servidores por medio de directivas de línea de base centralizadas, aplicadas de forma coherente a todos los servidores de la organización. Las directivas de línea de base sólo permiten una funcionalidad mínima, pero sí permiten que los servidores se comuniquen con otros equipos en el mismo dominio y su autenticación a través de los controladores de dominio. A partir de este estado más seguro, se pueden aplicar otras directivas incrementales más, que permiten que cada servidor realice únicamente las tareas específicas definidas por su función. La estrategia de administración de riesgos determinará si es apropiado para el entorno que se lleven a cabo estos cambios.

## **5. Administrar revisiones**

Una de las principales medidas de protección contra ataques es mantener el entorno actualizado con todas las revisiones de seguridad necesarias, las que pueden ser necesarias tanto para servidores como para clientes. Es importante explicar la forma de obtener lo antes posible las revisiones nuevas, implementarlas rápidamente y de forma confiable en toda la organización, y confirmar que están instaladas en todos los equipos.

## **6. Auditoría y detección de intrusiones**

No todos los ataques son evidentes. A veces, los ataques más sutiles son los más peligrosos, ya que pasan desapercibidos y es difícil determinar los cambios realizados.

Es conveniente auditar el entorno para aumentar las posibilidades de detectar ataques y describir los sistemas de detección de intrusos (programas diseñados específicamente para detectar comportamientos indicativos de que se está produciendo un ataque).

## **7. Responder a las incidencias**

Independientemente de lo seguro que sea el entorno, siempre existe el riesgo de ataque. Cualquier estrategia de seguridad razonable debe incluir detalles sobre cómo responderá la organización a los distintos tipos de ataque.

En esta sección se describen las mejores técnicas para responder a distintos tipos de ataque y se incluyen los pasos que hay que realizar para notificar las incidencias de forma efectiva. También se incluye el análisis de un escenario posible en el que se explica una respuesta típica a una incidencia.

### **Problemas de seguridad más frecuentes en el cliente**

1. Errores de contraseñas:
  - a. Contraseñas no seguras.
  - b. Consecuencias de compartir contraseñas entre usuarios.
  - c. Consecuencias de emplear la contraseña interna de la organización en sitios Web externos.
2. Consecuencias de no realizar copias de seguridad adecuadas o almacenar información vital localmente en vez de almacenarla en un servidor central.
3. Estaciones de trabajo abiertas y desatendidas.
4. Consecuencias de no instalar las actualizaciones y revisiones del proveedor.
5. Consecuencias de no establecer la seguridad física de los equipos.
6. Deshabilitar o reducir los controles de seguridad. Es importante dejar claro a los usuarios la importancia de mantener los controles de seguridad.
7. Consecuencias de instalar software innecesario o no aprobado.

8. Consecuencias de exponer más información personal de la necesaria.
9. Consecuencias de propagar virus y otras trampas.
10. Consecuencias de abrir archivos adjuntos de mensajes no esperados.
11. Consecuencias de no formar a los usuarios para detectar problemas de seguridad y tomar precauciones.

### **Problemas de seguridad más frecuentes en el servidor**

1. Errores de contraseñas:
  - a. Contraseñas no seguras.
  - b. Consecuencias de compartir contraseñas entre miembros del personal de TI.
  - c. Consecuencias de emplear la contraseña interna de la organización en sitios Web externos.
2. Consecuencias de no implementar todos los niveles de seguridad de la estrategia de defensa en profundidad.
3. Consecuencias de no realizar y validar copias de seguridad del sistema de forma coherente.
4. Consecuencias de ejecutar servicios innecesarios.
5. Consecuencias de no reconocer amenazas de seguridad internas.
6. Consecuencias de no aplicar la directiva de seguridad.
7. Consecuencias de conceder a los servicios más privilegios de los necesarios.
8. Consecuencias de no restringir suficientemente las aplicaciones desarrolladas internamente.

### **Referencia rápida de respuesta a incidencias**

<b>Instrucciones generales de respuesta a incidencias</b>
Anote todos los detalles. Considere la posibilidad de grabar sus comentarios en cinta. Anote quién llevó a cabo las acciones, cuándo y por qué.
Mantenga la calma. Evite la tendencia de una reacción excesiva o de entrar en pánico. Siga meticulosamente los pasos de la directiva de seguridad.
Utilice un medio de comunicación fuera de banda: teléfono, fax o comunicación cara a cara, por ejemplo. Es posible que el atacante esté a la escucha.
Permanezca en comunicación constante con otros equipos o individuos afectados.
No reinicie el equipo, ni inicie o cierre sesiones, ya que esto podría activar código dañino.

<b>Primer objetivo: hacer la valoración inicial de la incidencia</b>	
1.1	Póngase en contacto con el equipo técnico para comprobar que la incidencia no es una falsa alarma.
1.2	Examine los registros de auditoría para detectar si hubo actividad inusual, o desaparición de registros o fragmentos de los mismos.
1.3	Busque herramientas de hackers (programas de averiguación de contraseñas, caballos de Troya, etc.).
1.4	Compruebe si hay aplicaciones no autorizadas configuradas para iniciarse automáticamente.
1.5	Examine las cuentas para detectar posibles aumentos de privilegios o miembros de grupo no autorizados.
1.6	Compruebe si hay procesos no autorizados.
1.7	Piense en la forma de conservar las pruebas.
1.8	Compare el rendimiento del sistema afectado con la línea de base.
1.9	Asigne a la incidencia un nivel de prioridad inicial y un responsable.
<b>Segundo objetivo: comunicar la incidencia</b>	
2.1	Comunique la incidencia a los grupos interesados y a los miembros asociados al CSIRT (Collaboration of Incident Response Teams) pertinentes.
<b>Tercer objetivo: contener los daños y minimizar el riesgo</b>	
3.1	Determine la gravedad de la incidencia y compruebe la directiva de seguridad para decidir si tiene que desconectar de la red los sistemas afectados para aislarlos.
3.2	Cambie las contraseñas de los sistemas afectados.
3.3	Haga copias de seguridad de los sistemas para poder recuperarlos y, si fuera necesario, obtener pruebas.

<b>Cuarto objetivo: identificar el tipo y la gravedad de las intromisiones</b>	
4.1	Determine el tipo de ataque.
4.2	Determine el objetivo del ataque (ataque dirigido específicamente a la organización, automatizado o para obtener información).
4.3	Identifique todos los sistemas implicados en el ataque. Si se identifican más sistemas afectados, revise los pasos de las medidas de contención.
4.4	Evalúe de nuevo el nivel de prioridad del suceso y, si fuera necesario, asígnele otro nivel de prioridad.
<b>Quinto objetivo: conservar las pruebas</b>	
5.1	Realice lo antes posible copias de seguridad de los sistemas y guárdelas en discos de almacenamiento que no se hayan utilizado nunca en el ciclo de respuesta y recuperación.
5.2	Si es posible, realice copias de seguridad de los sistemas completos, incluidos los registros y el estado del sistema.
5.3	Mantenga una cadena de custodia comprobable de las pruebas obtenidas.
5.4	Proteja las pruebas y anote en un documento quién las obtuvo, cómo, cuándo y quién ha tenido acceso a las mismas.
<b>Sexto objetivo: notificar la incidencia a las agencias externas</b>	
6.1	Awise a las fuerzas de la ley locales o nacionales, asesorado por un consejero jurídico.
6.2	Informe del resultado a los miembros de relaciones públicas de CSIRT y proporcióneles asistencia, si fuera necesario.
6.3	Awise a otras agencias pertinentes, como CERT (Coordination Center at Carnegie Mellon University, <a href="http://www.cert.org">http://www.cert.org</a> , sitio Web en inglés). Ésta y otras agencias similares pueden proporcionar información valiosa para recuperar datos.

<b>Séptimo objetivo: recuperar los sistemas</b>	
7.1	Busque y valide las copias de seguridad más recientes que no se hayan visto afectadas.
7.2	Restaure el sistema.
7.3	Valide el funcionamiento del sistema y compare su rendimiento con líneas de base históricas.
7.4	Supervise la aparición de ataques repetidos y los cambios de configuración causados por los pasos de contención.
<b>Octavo objetivo: recopilar y organizar la documentación sobre la incidencia</b>	
8.1	Recopile todas las notas y grabaciones en un registro de actividad de la incidencia de seguridad.
8.2	Distribúyalo a los participantes en la incidencia, para que lo revisen y aprueben (incluido el consejero legal, para que determine la validez de las pruebas).
8.3	Revise la causa de la infracción de seguridad y mejore las defensas para prevenir ataques similares en el futuro.
8.4	Ayude al departamento de finanzas a evaluar las pérdidas debidas a la infracción de seguridad.
8.5	Prepare un informe para la dirección y otros grupos interesados para explicar cómo se produjo el evento e informar de las pérdidas debidas a la infracción de seguridad y las medidas de prevención que se van a adoptar.

## **8. Conclusión**

En el desarrollo del presente estudio logramos exponer los principios fundamentales para implementar un sistema de seguridad bajo el entorno Windows 2000 Server.

Es importante tomarse en serio el tema de la seguridad. Por consiguiente, identificamos los riesgos inherentes a un entorno de red y determinamos el nivel de seguridad apropiado para el entorno; también definimos los pasos necesarios para alcanzar el nivel de seguridad adecuado.

Finalmente, hemos propuesto el Programa Estratégico de Protección de Tecnología (STPP, Strategic Technology Protection Program) el cual integra los productos, los servicios y el soporte de Microsoft dedicados a la seguridad, logrando un nivel de seguridad apropiado y manteniéndolo, adoptando medidas preventivas contra las amenazas y respondiendo con eficacia cuando se producen.

## **Bibliografía**

[1] Russel, Charlie – Crawford, Sharon: Running Microsoft Windows 2000 Server. Mc Graw Hill. (2000).

## **Vínculos interesantes**

Microsoft España Site:

<http://www.microsoft.com/spain//technet/asuntos/seguridad.asp>

Microsoft TechNet Security Site:

<http://www.microsoft.com/technet/itsolutions/security/bestprac/secthret.asp>

Microsoft Security Best Practices:

<http://www.microsoft.com/technet/itsolutions/security/bestprac/secthret.asp>

How to Publish non-MSI Programs with .zap Files (Q231747):

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q231747>