UF1274: Administración y auditoría de los servicios de mensajería electrónica

Elaborado por: Raúl Vega Mateo

Edición: 5.0

EDITORIAL ELEARNING S.L.

ISBN: 978-84-16424-66-5• Depósito legal: MA 725-2015

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa:

Bienvenido a la Unidad Formativa UF1274: Administración y auditoría de los servicios de mensajería electrónica. Esta Unidad Formativa pertenece al Módulo Formativo MF0496_3: Administración de servicios de mensajería electrónica que forma parte del Certificado de Profesionalidad IFCT0509: Administración de servicios de Internet, de la familia de Informática y Comunicaciones.

Presentación de los contenidos:

La finalidad de esta Unidad Formativa es enseñar al alumno a administrar servicios de mensajería electrónica para asegurar la distribución de los mensajes entre usuarios, así como auditar los servicios de mensajería electrónica para garantizar la calidad del servicio y diagnosticar y solucionar los fallos en el mismo según las necesidades de la organización.

Para ello, en primer lugar se analizará la administración del sistema de correo y la auditoría y resolución de incidencias sobre los servicios de mensajería electrónica.

Objetivos de la Unidad Formativa:

Al finalizar esta Unidad Formativa aprenderás a:

– Administrar los servidores de mensajería electrónica para asegurar la continuidad en el servicio según las especificaciones de seguridad.

– Aplicar procedimientos de auditoría y resolución de incidencias en servicios de mensajería electrónica.

Índice

UD1

Administración del sistema de correo

1.1. Administración del sistema
  1.1.1. Gestión de cuentas de usuario
  1.1.2. Administración de recursos de almacenamiento
  1.1.3. Gestión de buzones
1.2. Optimización del rendimiento del sistema
  1.2.1. Elementos determinantes del rendimiento: Hardware. Sistema Operativo. Aplicaciones
  1.2.2. Ajustes de rendimiento del Sistema Operativo
  1.2.3. Ajustes de rendimiento de las aplicaciones: Servidor SMTP, Servidor POP/IMAP. Servidores Web, filtros antivirus/antispam
  1.2.4. Escalado de un sistema de correo: Separación de servicios. Balanceo de carga, alta disponibilidad
1.3. Monitorización del sistema
  1.3.1. Configuración de un sistema de monitorización
  1.3.2. Monitorización de los parámetros de rendimiento más importantes del sistema
1.4. Securización del sistema
  1.4.1. Adecuación a la Normativa legal (LSSI, LOPD) y a las políticas de seguridad de la organización
  1.4.2. Códigos de buenas prácticas (ISO 27002)
  1.4.3. Recuperación ante desastres y continuidad de los servicios
  1.4.4. Copias de Seguridad
  1.4.5. Gestión de actualizaciones
  1.4.6. Protección servicios: Firewall. Herramientas seguridad (Nmap, Nessus/OpenVAS, Brutus)

1.1. Administración del sistema

En esta Unidad Didáctica que acabamos de empezar vamos a profundizar en la **administración del sistema de correo de una organización**, como ya hemos comenzado a analizar en los anteriores temas.

Para ello, el/la alumno/a en esta parte del temario aprenderá los siguientes aspectos:

- **Administrar los servidores de mensajería electrónica para asegurar la continuidad en el servicio según las especificaciones de seguridad.**

- **Aplicar procedimientos de auditoría y resolución de incidencias en servicios de mensajería electrónica.**

Cómo ya hemos planteado, debemos utilizar un sistema de servidor para mostrar cómo trabajar en el entorno del sistema de correo electrónico.

La opción elegida es Microsoft Exchange Server 2010.

Exchange Server 2010 es un sistema de mensajería electrónica diseñado por Microsoft para implementar un servicio de correo electrónico, programación y herramientas de las aplicaciones personalizadas para un correcto trabajo dentro de una organización.

Las organizaciones en las que podemos trabajar pueden tener aún en funcionamiento el Exchange Server 2003. Como explica Microsoft, "puede implementar Exchange 2010 en una organización existente de Exchange Server 2003 que funcione en modo nativo ya que se admite la coexistencia de estas dos versiones".

Exhange 2003	Exchange 2007	Exchange 2010

También puede funcionar con Exchange Server 2007, que puede actualizarse siempre que cumpla los requisitos básicos para ello.

Aunque ya hemos profundizado en este tema en epígrafes anteriores, y lo veremos en algunos posteriores, las **necesidades del sistema** se centra en los siguientes aspectos:

Procesador	Memoria	Tamaño del archivo de paginación
Espacio en disco	Unidad	Resolución de pantalla

El siguiente cuadro determina las necesidades del sistema para instalar Exchange Server 2010.

COMPONENTE	REQUISITO
Procesador	– Equipo basado en arquitectura x64 con procesador Intel compatible con la arquitectura Intel 64 (anteriormente denominada Intel EM64T). – Procesador AMD compatible con la plataforma AMD64. – Los procesadores Intel Itanium IA64 no son compatibles.
Memoria	Varía según las características de Exchange instaladas.
Tamaño del archivo de paginación	El tamaño del archivo de paginación mínimo y máximo se debe establecer en memoria RAM física más 10 MB.
Espacio en disco	– Un mínimo de 1,2 GB en la unidad en la que se va a instalar Exchange. – 500 MB adicionales de espacio de disco para cada versión de idiomas que vayamos a instalar. – 200 MB de espacio de disco disponible en la unidad de sistema. – Un disco duro que almacene la base de datos de la cola de mensajes en un servidor de transporte perimetral o un servidor de transporte de concentradores con un mínimo de 500 MB de espacio disponible.
Unidad	Unidad de DVD-ROM, accesible de forma local o a través de la red.
Resolución de pantalla	800 x 600 píxeles o superior.

Exchange Server 2010 es compatible con Outlook y Entourage y admite los siguientes clientes de correo electrónico:

– Outlook 2010.

– Outlook 2007.

– Outlook 2003.

– Entourage 2008 para Mac, Web Services Edition.

– Outlook para Mac 2011.

1.1.1. Gestión de cuentas de usuario

En la anterior Unidad Formativa ya profundizamos en cómo debe ser una cuenta de correo electrónico dentro de una organización para **cumplir unos mínimos de seguridad e imagen pública**.

Una dirección de correo electrónico tiene tres partes diferenciadas:

- **Nombre de usuario.**
- **Dominio.**
- **Extensión.**

Las dos últimas vienen marcadas por la propia organización, en la que aparece normalmente su nombre, con la extensión (lo que aparece detrás del punto), que marca la finalidad de la organización (.com, .tv, .es, etc.).

El usuario normalmente puede escoger su nombre en base a unos criterios que marca la organización que desarrolla y pone a su disposición el correo electrónico. Las opciones que dan pueden variar, pero suelen ser las siguientes:

– **Combinación del nombre y apellidos del usuario** (para el usuario Carlos Sánchez Trigo).

  - carlossancheztrigo@
  - csanchez@
  - csancheztrigo

- carlos.sanchez@
- CST@

– **Nombre genérico**, independientemente del usuario. En este caso, la cuenta nunca cambia aunque la persona física que la usa sí, es decir, puede haber mucha movilidad entre puestos de la organización pero de forma externa no hay cambios porque las direcciones de correo electrónico se mantienen intactas.

Se mantiene la cuenta de correo, aunque su usuario deje la organización (cuenta hereditaria)	Cuenta de correo despersonalizada

Otro aspecto importante es la **contraseña**, que salvo indicaciones contrarias de la organización, siempre diseñará el usuario, que es el responsable último de mantener dicha dirección intacta ante ataques externos y será el garante de su vigilancia.

El **Instituto Nacional de Tecnologías de la Comunicación (Inteco)**, dependiente del **Ministerio de Industria, Energía y Turismo**, ha elaborado un amplio informe para que podamos construir contraseñas seguras, siguiendo unos sencillos pasos.

Inteco dispone de la **Oficina de Seguridad del Internauta**, con un amplio abanico de servicios e informes que podemos encontrar en el siguiente enlace:

http://www.osi.es/es

Una contraseña, según estas indicaciones, debe cumplir al menos tres de las siguientes características que enunciamos:

- Tener números.
- Tener letras.
- Tener mayúsculas y minúsculas.
- Tener símbolos ($, @, &, #).

Además de estas características, una buena contraseña debe cumplir también con los siguientes características:

- La longitud no debe ser inferior a siete caracteres. A mayor longitud más difícil de adivinar.
- No debe formarse con números y/o letras que estén adyacentes en el teclado (123456, 1q2w3e o 123QWEasd).
- La contraseña no debe contener información que sea fácil de averiguar (nombre de usuario de la cuenta, por ejemplo).
- No debe contener palabras existentes en algún idioma. Los ataques de diccionario prueban cada una de las palabras que figuran en el diccionario y/o palabras de uso común.

Como hemos comentado, muchas veces es el usuario el encargado de determinar la contraseña personal e intransferible que tendrá que custodiar, pero en cualquier caso es bueno que la organización disponga de un manual de buenas prácticas que determine cómo debe ser la contraseña.

Un buen manual debe contar con las características adecuadas que hemos descrito y planteadas por Inteco.

No obstante, la contraseña no es lo único que marca la seguridad de una cuenta de correo electrónico. Siguiendo unas pautas sencillas podemos aumentar la seguridad de la misma.

Volvemos a las pautas marcadas por Inteco, que sugiere las siguientes medidas de seguridad en el entorno de los e-mails:

No usar la misma contraseña para diferentes cuentas. Sobre todo si son de alto riesgo, como las de los servicios bancarios o comerciales.

- **La contraseña es algo privado**, no dejarla escrita en ningún sitio, y mucho menos al lado del ordenador.

- **Cambiar las contraseñas que traen todos los dispositivos y servicios en línea directamente de fábrica y por defecto**. Un ejemplo son los enrutadores WIFI, con contraseñas muy conocidas que pueden facilitar la accesibilidad al equipo que hemos adquirido por personas extrañas.

- **Limitar el uso de las contraseñas almacenadas en el navegador para los servicios críticos**.

El siguiente gráfico nos aporta dos consejos o trucos para conseguir una contraseña segura de forma muy sencilla:

– Usar una frase fácil de memorizar

  Una vez hecho esto, se pueden hacer combinaciones con las distintas palabras que componen la frase: utilizar la primera letra de cada palabra o utilizar la última letra de cada palabra, por ejemplo.

– Usar una “semilla” y aplicarle un “algoritmo”

  En cada lugar donde debamos crear una contraseña, pensamos en una “semilla”, que no es más que una palabra que ayude a recordar ese lugar. A la semilla se le aplica un “algoritmo” que es una combinación de pasos que utilizaremos para crear las contraseñas de cualquier sitio. La ventaja de utilizar este método es que sólo será necesario recordar el algoritmo.

Existen algunos sites en internet gratuitos que permiten comprobar el nivel de seguridad de la contraseña que hemos ideado.

Una de las más interesantes se puede visitar en el siguiente enlace:

http://password.es/comprobador/

Otra opción, para los usuarios con menos memoria, es conseguir un **gestor de cuentas de correo electrónico**, ya que hay varios para su almacenaje en nuestro ordenador, ya sea un PC o un Mac, o en internet.

Se trata de programas que permiten gestionar las cuentas y sus contraseñas de forma segura, almacenando las claves para que podamos acceder a ellas de forma segura y ajena a los ojos de terceras personas.

Una de estos servicios podría ser el que encontramos en el siguiente enlace:

https://www.passpack.com/

Si trabajamos con nuestro propio equipo no habrá problemas al almacenar nuestros nombres de usuarios y contraseñas. No es la mejor práctica, pero si es un ordenador seguro podríamos hacerlo. El problema radica cuando este ordenador es público o de uso compartido, donde cualquier persona puede consultar nuestra información sensible y acceder impunemente a nuestra cuenta de correo electrónico.

Para ello, lo más recomendable es utilizar una **contraseña maestra**, que no es otra cosa que una nueva clave secreta que nos pedirá nuestro ordenador cuando accedamos a algún sitio restringido en el que nuestro ordenador tenga registrada una contraseña.

En el caso de Firefox, deberemos ir al menú Herramientas, y de ahí a Opciones. De ahí debemos acceder al apartado Seguridad cliqueando en el icono correspondiente.

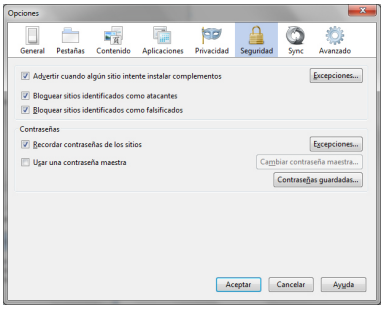

Imagen 1: Apartado de Seguridad en Firefox, donde podremos elegir una contraseña maestra.

Una vez que accedamos a este punto, Firefox nos pedirá que introduzcamos dos veces la clave y dispondremos un **medidor de la seguridad** de la misma para comprobar que realmente es apta para el fin que perseguimos.

Una vez que apliquemos los cambios deberemos cerrar este navegador para que los cambios producidos sean efectivos.

A partir de ese momento, cuando entremos en una página que guarde nuestros datos de seguridad nos pedirá esta clave. De esta forma, podremos almacenar dichas claves y nombres de usuario, pero siempre nos pedirá una clave maestra, que es siempre la misma.

Las organizaciones deben implementar también **criterios propios** de funcionamiento de sus cuentas de correo electrónico, que se deberá hacer directamente desde el propio servidor para que se pueda cumplir por parte de todos los usuarios.

Por ello, cada cierto tiempo se deberán cambiar las contraseñas, para lo que el sistema avisará con suficiente tiempo de antelación para que el usuario pueda llevarlo a cabo.

Además, dichas contraseñas serán diferentes en cada momento, y el propio sistema impedirá que se puedan repetir hasta un número de veces que el administrador determine en función del nivel de seguridad que quiera conseguir.

Todas estas modificaciones se realizan en la **Consola de Administración de Directivas de Grupo** (conocida por sus siglas en inglés, GPMC). Como descubre Microsoft, “la GPMC se compone de un complemento MMC y un conjunto de interfaces de scripts para administrar la directiva de grupo. La GPMC se incluye con Herramientas de administración de servidor remoto”.

Importante

Microsoft permite la descarga de la GPMC en el siguiente enlace:

http://go.microsoft.com/fwlink/?LinkId=130862

La Consola de Administración de Directivas de Grupo permite establecer algunas pautas, en el apartado de desactivar los requisitos de complejidad de contraseña.

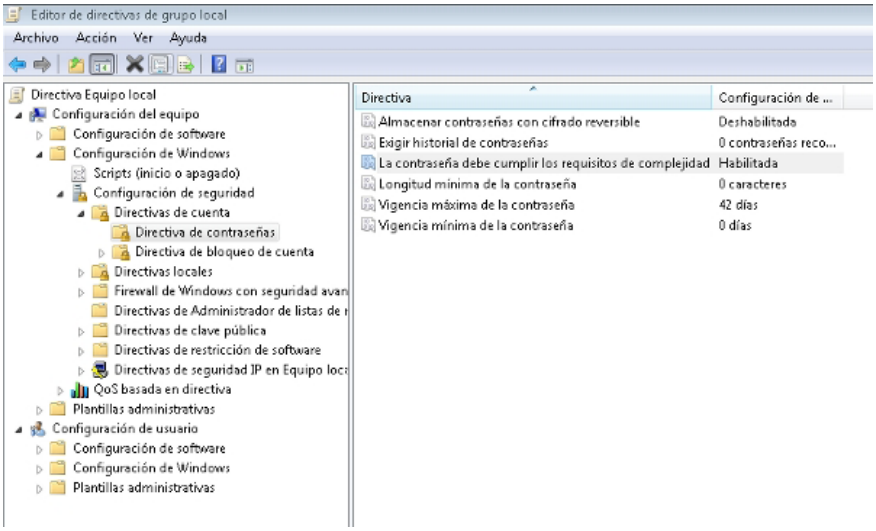

Imagen 2: Panel de la Consola de Administración de Directivas de Grupo en la que podemos determinar los distintos aspectos de seguridad sobre las contraseñas que fija Exchange Server para la organización.

Como podemos apreciar en la imagen, la citada consola nos permite llevar a cabo las siguientes acciones en materia de seguridad:

– Almacenar contraseñas con cifrado reversible.

– Exigir historial de contraseñas.

– La contraseña debe cumplir los requisitos de complejidad.

– Longitud mínima de la contraseña.

– Vigencia máxima de la contraseña.

– Vigencia mínima de la contraseña.

1.1.2. Administración de recursos de almacenamiento

Los usuarios de una organización utilizan en muchas ocasiones, por no decir siempre, **los clientes de correo electrónico como base de datos permanente de los e-mails recibidos**. Esto es especialmente cómodo porque estos programas tienen motores de búsqueda bastante potentes que permiten cribar búsquedas sistemáticas en función de distintos criterios.

Además, como podemos ver en la imagen, los correos recibidos se pueden organizar mediante carpetas e incluso posicionar los e-mails entrantes en dichas carpetas en función de funciones específicas.

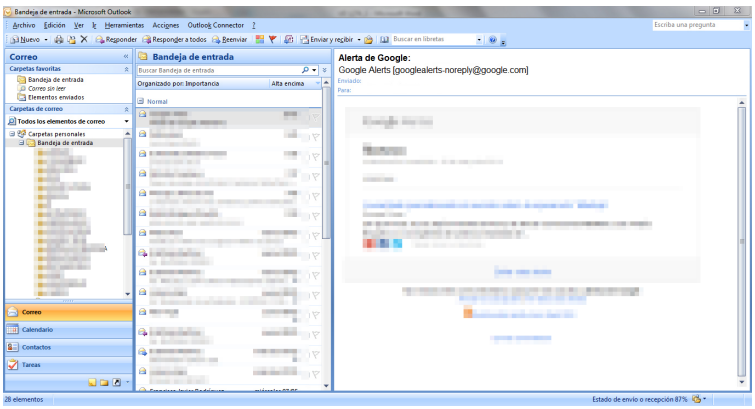

Imagen 3: Bandeja de entrada del Outlook, que es una base de datos de correos electrónicos recibidos en nuestra organización.

Además, los programas como Outlook también permiten organizar los correos electrónicos en las siguientes carpetas:

- Bandeja de entrada.
- Bandeja de salida.
- Borrador.
- Correo electrónico no deseado.
- Elementos eliminados.
- Elementos enviados.

Por lo tanto, estos clientes de correo electrónico son auténticas herramientas de documentación en el seno de las organizaciones modernas, ya que permiten almacenar los e-mails con sus archivos adjuntos en nuestro equipo, con la posibilidad de una sub clasificación en carpetas y con herramientas para la búsqueda sistemática.

Esto también obliga a mayor complejidad del sistema de servidores de una organización, porque debe destinar un espacio suficiente en disco para atender con normalidad cada buzón de correo electrónico. Es más, Microsoft, como empresa que gestiona y desarrolla Exchange Server 2010, aconseja que **por cada cuenta de correo electrónico habilitada en nuestra organización destinemos 500 MB de espacio en disco para la recepción y envío de correos**. Es el espacio de almacenaje.

Eso sin contar con otros recursos que el sistema deberá determinar, como la **memoria RAM** y otros recursos paralelos que deben funcionar para que una base de datos de correos electrónicos, como la que hemos visto, funcione correctamente y podamos almacenar y ver los e-mails recibidos y/o enviados con total facilidad.

Exchange Server prevé este tipo de incidencias, de ahí que a través de su Consola de Administración permita gestionar estas situaciones y determinar el tamaño máximo del archivo y los avisos o alertas que nos dará el sistema cuando superemos o estemos a punto de llegar a la cuota máxima predeterminada.

Para ello, tendremos dos opciones para determinar las opciones de almacenaje de nuestro correo electrónico.