Microsoft

ESQUEMA NACIONAL DE SEGURIDAD

CON MICROSOFT®

INTECO

Instituto Nacional de Tecnologías de la Comunicación

Microsoft®

CCN Centro Criptológico Nacional

GOBIERNO DE ESPAÑA

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Juan Luís García Rambla
José María Alonso Cebrián

La Administración Española lidera un encomiable esfuerzo hacia el **Desarrollo de la Sociedad de la Información en España**, así como en el uso óptimo de las tecnologías de la Información en pro de una prestación de servicios más eficiente hacia los ciudadanos.

Aunque este tipo de contenidos no siempre son fáciles de tratar sin caer en un excesivo dogmatismo y lenguaje ortodoxo, sí es cierto que en el marco de la **Ley 11/2007 del 22 de Junio**, de acceso electrónico de los ciudadanos a los **Servicios Públicos**, se anunció la creación de los **Esquemas Nacionales de Interoperabilidad y de Seguridad** con la misión de garantizar un derecho ciudadano, como el recogido en dicha ley, lo que sin duda es un reto y una responsabilidad de primera magnitud.

Microsoft Ibérica lleva **25 años** acompañando el desarrollo de la **Administración Pública Española**. Navegando juntos por la historia del progreso tecnológico más espectacular de los últimos años, aprendiendo juntos, y en definitiva siendo compañeros de viaje en el proceso modernizador de nuestro país. Y son aquellos proyectos más estratégicos para la **Administración** los que marcan nuestra estrategia y atención.

Este manual es un nexo entre las medidas con implicaciones tecnológicas descritas en el **Esquema**, y su implementación práctica en aquellos **entornos con tecnología Microsoft**. El libro toma como hilo conductor los grandes principios que conforman **el Esquema Nacional de Seguridad**, tales como sus principios, dimensiones, medidas, implementaciones, explotación, protección etc., para a continuación comentarlos de forma sencilla y detallar cuáles serían las configuraciones y recomendaciones técnicas más adecuadas para su cumplimiento.

Tenemos la esperanza de que este manual sirva para facilitar a los responsables de seguridad el cumplimiento de los aspectos tecnológicos derivados del cumplimiento del **ENS**, así como servir de vehículo de difusión de un conocimiento importante como es el relativo a la seguridad de los servicios públicos de las **Administraciones** y la garantía de seguridad hacia los ciudadanos en el ejercicio de sus **derechos reconocidos por la Ley**.

Esquema Nacional de Seguridad... con Microsoft

Juan Luis G. Rambla
José María Alonso Cebrián

Publicado por:

Microsoft Ibérica S.R.L.
Centro Empresarial La Finca
Edificio 1
Paseo del Club Deportivo, 1
28223 Pozuelo de Alarcón – Madrid (España)

Depósito Legal: M. 20.093-2011

Coordinador Editorial: Héctor Sánchez Montenegro.

Diseño y maquetación: José Manuel Díaz. / Newcomlab S.L.L.

Revisión técnica: Newcomlab S.L.L.

Imprime: Pardetres.net

Impreso en España – Printed in Spain

Agradecimientos

Héctor Sánchez Montenegro, National Technology Officer de Microsoft Ibérica y coordinador de esta obra, desea trasmitir un agradecimiento muy especial, además de a los autores y prologuistas, a las siguientes personas:

Luis Miguel García de la Oliva, Director de Plataforma de Microsoft Ibérica.

José Parada Gimeno, Chief Security Advisor de Microsoft Ibérica.

Francesca di Massimo, Directora de Seguridad e Interoperabilidad de Microsoft WE.

Carlos de la Iglesia, Director de Comunicaciones de Microsoft.

Manuel Sánchez Chumillas, de Informática 64.

Nacho de Bustos Martín, Director General de Newcomlab.

Microsoft Ibérica

La Administración Española lidera un encomiable esfuerzo hacia el Desarrollo de la Sociedad de la Información en España, así como en el uso óptimo de las tecnologías de la Información en pro de una prestación de servicios más eficiente hacia los ciudadanos.

Aunque este tipo de contenidos no siempre son fáciles de tratar sin caer en un excesivo dogmatismo y lenguaje ortodoxo, sí es cierto que en el marco de la Ley 11/2007 del 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, se anunció la creación de los Esquemas Nacionales de Interoperabilidad y de Seguridad con la misión de garantizar un derecho ciudadano, como el recogido en dicha ley, lo que sin duda es un reto y una responsabilidad de primera magnitud.

Pero lo es aún más el garantizar ese derecho con las garantías de confidencialidad, seguridad, confianza y privacidad necesarias.

No son asuntos menores, en tanto en cuanto hablamos de derechos ciudadanos. Y, desde luego, si siempre ha sido deseable el mayor alineamiento posible entre la industria tecnológica y el uso que de la tecnología hace la Administración Pública, en esta ocasión resulta más importante que nunca. Retos tan elevados como los descritos solo pueden conseguirse desde la más estrecha colaboración con la industria.

Microsoft Ibérica lleva 25 años acompañando el desarrollo de la Administración Pública Española. Navegando juntos por la historia del progreso tecnológico más espectacular de los últimos años, aprendiendo juntos, y en definitiva siendo compañeros de viaje en el proceso modernizador de nuestro país.

Y son aquellos proyectos más estratégicos para la Administración los que marcan nuestra estrategia y atención. En esta ocasión en áreas como la seguridad o la privacidad, desde donde ya hemos trabajado para acercar y ayudar a las empresas Españolas

en el cumplimiento de los requisitos tecnológicos derivados del cumplimiento del Real Decreto de la LOPD, publicando un exhaustivo trabajo sobre cómo acercarnos a su cumplimiento con la configuración adecuada de tecnologías Microsoft. O la compartición del código fuente de nuestros sistemas operativos y aplicaciones ofimáticas con el Centro Nacional de Inteligencia a través de su Centro Criptológico Nacional. Y en esa línea presentamos este trabajo centrado en el Esquema Nacional de Seguridad.

Es un trabajo eminentemente divulgativo, dirigido a los responsables técnicos de las administraciones, encargados de cumplir los requisitos y las recomendaciones del Esquema.

Este manual es un nexo entre las medidas con implicaciones tecnológicas descritas en el Esquema, y su implementación práctica en aquellos entornos con tecnología Microsoft. El libro toma como hilo conductor los grandes principios que conforman el esquema Nacional de Seguridad, tales como sus principios, dimensiones, medidas, implementaciones, explotación, protección etc., para a continuación comentarlos de forma sencilla y detallar cuáles serían las configuraciones y recomendaciones técnicas más adecuadas para su cumplimiento.

Tenemos la esperanza de que este manual sirva para facilitar a los responsables de seguridad el cumplimiento de los aspectos tecnológicos derivados del cumplimiento del ENS, así como servir de vehículo de difusión de un conocimiento importante como es el relativo a la seguridad de los servicios públicos de las Administraciones y la garantía de seguridad hacia los ciudadanos en el ejercicio de sus derechos reconocidos por la Ley.

María Garaña
Presidenta de Microsoft España

INTECO

Imagine que el banco en el que usted deposita sus ahorros, por la noche dejara las puertas sin cerrar y el dinero en los mostradores. Seguramente, esta entidad perdería su confianza. Y probablemente no pasaría mucho tiempo antes de que sus administradores fueran objeto de una justificada denuncia por negligencia.

Las Administraciones Públicas son también depositarias de activos de gran valor, entre los que destacan por su trascendencia para el correcto funcionamiento de la sociedad la información y los sistemas que la sustentan. Todos los ciudadanos españoles queremos y tenemos derecho a tener unas Administraciones Públicas de confianza, que no dejen las puertas abiertas y los activos valiosos al alcance de cualquiera. Que protejan su capacidad para seguir prestándonos servicios y nuestros datos de manera proporcionada al valor que tienen, o al daño que podría causarnos su robo, pérdida o falseamiento.

Por ello, la sociedad necesita dotarse de los mecanismos que permitan a los responsables públicos evaluar adecuadamente los riesgos para la información y los sistemas que la soportan, y que impongan la obligación de actuar en consecuencia. La seguridad de los datos que las administraciones tienen de nosotros, y la de los servicios que nos prestan, es la base fundamental de la confianza de los ciudadanos en sus instituciones.

El crecimiento económico y el progreso de la sociedad, así como unas instituciones públicas eficientes, hoy día se cimentan en el uso de las nuevas tecnologías. Y los ciudadanos no harán uso de esas nuevas tecnologías, ni de los servicios de la Sociedad de la Información, si no confían en los sistemas y procesos que los sustentan.

Por tanto, podemos decir que colaborar para la promoción, entendimiento e implementación correcta del Esquema Nacional de Seguridad (ENS) equivale a favorecer

el progreso de la sociedad, la mejora económica, el buen gobierno y la confianza de los ciudadanos en sus administraciones.

INTECO, cuya misión es contribuir a reforzar la confianza en la Sociedad de la Información y que como medio propio de la Administración General del Estado dedica gran parte de sus recursos y esfuerzos a la implantación del ENS en las Administraciones Públicas, da la bienvenida al presente manual que sin duda contribuirá a fomentar la seguridad de la información en las Administraciones Públicas, y por tanto la confianza en la Sociedad de la Información.

Víctor M. Izquierdo Loyola
Director General del Instituto Nacional de
Tecnologías de la Comunicación, S.A. (INTECO)

Ministerio de Política Territorial y Administración Pública

El Esquema Nacional de Seguridad, materializado en el Real Decreto 3/2010, tiene como objetivo fundamental crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información que se maneja y de los servicios electrónicos que se prestan, que permita a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Efectivamente, los ciudadanos esperan que el acceso electrónico a los servicios públicos se produzca en unas condiciones de confianza y de seguridad equiparables a las que puedan encontrar si se acercan de manera presencial a las oficinas de la Administración. El Esquema Nacional de Seguridad se encuentra, en definitiva, al servicio de la realización del derecho de los ciudadanos a relacionarse por medios electrónicos con las Administraciones públicas.

El Esquema Nacional de Seguridad es, por tanto, una respuesta a la obligación de las Administraciones Públicas de adoptar medidas de seguridad adecuadas a la naturaleza de la información y los servicios y los riesgos a los que están expuestos. Para ello establece la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007 y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Además, el Esquema introduce los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información y que han de facilitar la interacción entre ellas, así como la comunicación de los requisitos de seguridad de la información a la Industria.

El Esquema Nacional de Seguridad, al igual que el Esquema Nacional de Interoperabilidad, es el resultado de un esfuerzo colectivo en el que han participado todas

las Administraciones Públicas, a través de los órganos colegiados con competencia en materia de administración electrónica.

También la Industria del sector de tecnologías de la información y las comunicaciones ha contribuido a la elaboración del Esquema Nacional de Seguridad con aportaciones a través de las asociaciones de su sector; en relación con esta participación de la Industria, hay que reseñar que ésta ha reconocido en todo momento el carácter transcendente y necesario del Esquema para proporcionar una seguridad imprescindible.

El presente "Manual sobre cumplimiento del Esquema Nacional de Seguridad" es un testimonio concreto de este esfuerzo conjunto realizado por la Administración y por la Industria para facilitar que los servicios de las Administraciones Públicas disponibles por medios electrónicos se encuentren en las adecuadas condiciones de confianza y de seguridad que les son exigibles.

Fernando de Pablo
Director General para el Impulso de la Administración
Electrónica del Ministerio de Política Territorial y Administración Pública

Centro Criptológico Nacional

Nuestra sociedad actual está en Internet, nuestro modo de vida y el de nuestros hijos cada vez se encuentra más vinculado a la Red y a sus tecnologías asociadas. La Administración no es ajena a esta situación y la Ley 11/2007 está impulsando el empleo de esta vía y el esfuerzo realizado por los distintos organismos para que desde las sedes electrónicas la relación con los ciudadanos sea más fluida ha sido impresionante.

Conscientes de que no podemos generar confianza en este nuevo modo de relación sin dotarnos de los medios adecuados para la protección y el control de la información manejada por nuestros Sistemas, esta ley en su artículo 42 fijó las bases de una necesidad que ya demandaban muchos servidores públicos, el Esquema Nacional de Seguridad.

A finales de enero del año 2010 se aprobó el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Esta norma fija unos principios básicos y requisitos mínimos, así como un conjunto de medidas que permiten una protección adecuada de la información y los servicios.

El RD establece un plazo de implantación que puede llegar a los 48 meses reconociendo implícitamente la dificultad de su aplicación especialmente en este escenario de restricciones presupuestarias.

Se está realizando un esfuerzo en la serie CCN-STIC 800 para dar normas, guías y recomendaciones en el CÓMO solucionar los retos planteados en el esquema y se agradece cualquier guía práctica de aplicación en las tecnologías de mayor presencia en la Administración.

En este sentido, este libro desde el punto de vista de la empresa intenta proporcionar una aproximación práctica a cómo realizar y verificar este cumplimiento en sistemas que utilicen tecnologías de MICROSOFT.

El esquema es una pieza clave para mejorar la seguridad de los sistemas de la Administración y nos exige además un mayor esfuerzo de colaboración y trabajo

conjunto entre los diferentes organismos. Este documento es un ejemplo de esta colaboración y espero que consiga de alguna manera facilitar la comprensión de algunos aspectos de su implantación.

Javier García Candau
Subdirector General Adjunto en funciones del Centro Criptológico Nacional

Prefacio

Actualmente, en la vida cotidiana del individuo toda una serie de aspectos y mejoras hacen que ésta sea más cómoda para él. Las tecnologías de la información, los grandes avances en el mundo de las comunicaciones y su generalización en todos los ámbitos sociales, son factores fundamentales que propician esta mejora en la calidad de vida del ciudadano. Acciones que hace no mucho tiempo implicaban un serio esfuerzo o consumían un tiempo excesivo, son resueltas a día de hoy de forma ágil y asequible. No han pasado tantos años desde que el simple hecho de sacar dinero del banco implicaba necesariamente ir a una sucursal determinada que mantenía los datos de la cuenta correspondiente. El esfuerzo que esto requería parece desproporcionado a día de hoy. Sin embargo, y aunque se tenga la impresión de que se habla de un pasado remoto, no ha transcurrido tanto tiempo desde ello.

Los avances en este sentido son innumerables. Ahí está la telefonía móvil, la miniaturización de los sistemas informáticos, la conectividad a Internet en los sistemas domésticos y un largo etcétera de avances significativos. Estas mejoras han implicado múltiples cambios. En primer lugar de mentalidad, en la forma de entender las actividades o de adaptarse a la realización de nuevas tareas. Evidentemente esto no es fácil para todos. No se debe olvidar que estos avances y las nuevas formas de actuación asociadas no son igualmente aceptados por todos.

Estos cambios y mejoras han llegado también a algo tan habitual y necesario como los trámites administrativos. Es un intento de dejar atrás el "vuelva usted mañana" que ha traído múltiples complicaciones a la vida de muchos españoles: horas interminables de colas, papeles que no aparecen o el recorrer una ventanilla tras otra en espera de una respuesta a un problema que parece no tener solución. La informática también ha cambiado esto, la burocracia administrativa. El objetivo es buscar una mayor comodidad para el ciudadano. Agilizar tareas que antes podían implicar días completos perdidos y la eterna espera hasta que se recibía el deseado papel firmado.

Afortunadamente, poco a poco esos tiempos van quedando atrás. Trámites de una cierta complejidad, como la realización de la declaración de la renta o la petición de la vida laboral, han adquirido una nueva dimensión con las mejoras aportadas por los sistemas informáticos. Las nuevas tecnologías se suman a las capacidades de los sistemas tradicionales, abriendo con ello un abanico de posibilidades significativas. La capacidad de tramitar un procedimiento administrativo, fuera de las horas de aperturas clásicas de ministerios, ayuntamientos o universidades, es un claro ejemplo de ello.

Una muestra significativa en esta evolución la constituye el DNI Electrónico. Este mecanismo de validación ha convertido a España en una referencia mundial en los sistemas de autenticación electrónica. Se ha sumado a otros mecanismos ya previamente empleados para la realización de tramitaciones, garantizando que el usuario es correctamente identificado; por ejemplo, los certificados que durante algunos años se llevan suministrando a través del proyecto CERES (CERtificación ESpañola). Liderado por la Fábrica Nacional de Moneda y Timbre, establece una entidad pública de certificación que permite garantizar entre otras cosas la identificación de los ciudadanos y la confidencialidad de los datos.

El tratamiento de la información, su acceso o la disponibilidad de los sistemas facilitan sensiblemente el acercamiento a la Administración Pública. Sin embargo este cambio lleva también asociados nuevos conceptos, afrontando el uso de terminologías y escenarios que hasta la fecha estaban reservados prácticamente a la empresa privada. Portales de acceso, tratamiento automatizado de la información, disponibilidad, integridad o autenticidad son palabras que ahora forman también parte del vocabulario de la Administración Pública.

El tratamiento y utilización de sistemas informáticos por parte de los ciudadanos implica la aparición de necesidades de seguridad. De forma original ya se habían realizado avances significativos, como la garantía de los sistemas de autenticación. Sin embargo, la seguridad es mucho más que todo eso. No sirve con garantizar que "Juan" es quien dice ser. Sino que también sus datos deben estar a salvo, no pudiendo ser modificados de forma indiscriminada o accedidos por quien no debe. Igualmente, debe hacerse un uso eficiente de los mismos y asegurar que los propósitos y la disponibilidad de los servicios son los adecuados.

La seguridad va mucho más allá de lo que simplemente se ve o se intuye. Es tan importante la visión y apariencia de seguridad del portal de acceso a un servicio, como garantizar que los datos pueden ser recuperados ante una posible incidencia de seguridad. Así como que en caso de que ésta ocurra, se dispondrá de medios para detectarla y procedimientos para subsanarla y prevenirla en futuras ocasiones.

La seguridad debe tener en cuenta todos los escenarios posibles. Aunque la visión y la perspectiva de un potencial ataque parecen provenir de Internet, estudios reputados avalan que muchos incidentes se producen internamente. Por desidia o desconocimiento, los sistemas de protección definidos internamente son a me-nudo más laxos que los que se plantean perimetralmente para una defensa externa. Sin embargo, los ataques y los atacantes no conocen fronteras.

Un hacker puede operar desde fuera, pero un virus informático de forma interna puede provocar la caída de los servicios o la eliminación de información altamente sensible. El uso de redes inalámbricas proporciona mucha movilidad, pero abre nuevos vectores de ataque que puede utilizar un potencial atacante. Software malicioso en constante evolución, como son los troyanos, se adaptan para evitar los sistemas de protección que originalmente conseguían bloquearlos acertadamente.

El uso de las nuevas tecnologías lleva aparejada la palabra adaptabilidad, que en el caso específico de la seguridad es casi más evidente todavía. Tanto los sistemas externos, como los internos deben tener en cuenta esa capacidad para adaptarse, para mejorar y evolucionar con la tecnología. Sistemas o mecanismos que hoy pueden ser punteros, en un tiempo razonable han podido quedar desfasados. A veces se plantean mecanismos y sistemas de protección que deben ser rediseñados en pleno proceso de implantación, puesto que una nueva técnica descubierta los convierte en vulnerables.

La seguridad informática se encuentra en constante evolución, al igual que los sistemas de ataque que constantemente la ponen a prueba. En la actualidad, es difícil entender la informática sin la seguridad. Por tanto, cualquier mecanismo que se disponga, cualquier proyecto o iniciativa que se lleve a cabo desde la Administración Pública, debería contar desde su base con el concurso de la seguridad. Aunque en muchas ocasiones prima la funcionalidad y la usabilidad, sólo se alcanzarán los objetivos si las garantías que se ofrecen son suficientes para generar confianza en las mismas.

Por ejemplo, no se entendería la banca electrónica sin unas garantías para su uso. Si cayera la confianza de este servicio o los ataques con éxito fueran tan significativos que hicieran perder su credibilidad, acabaría este modelo de negocio. Por tanto, la seguridad es uno de sus pilares fundamentales. No deben olvidarse otros posibles factores, pero éste es siempre tan crítico o más que los otros.

La relación de los ciudadanos con la Administración Pública debe entenderse también desde esta perspectiva. La seguridad debe ser uno de los puntos neurálgicos, permitiendo que los usuarios confíen abiertamente en el servicio. Esta debe ser garantizada desde la base de la prestación del servicio. Los proyectos ya puestos en marcha deben adaptarse a esta premisa, mientras que los nuevos deberán nacer bajo el paraguas de la seguridad.

Así lo entiende la comunidad técnica y así ha sido entendido también desde la Administración. El año 2010 supone un hito en la aplicación de sistemas de seguridad en la relación de los ciudadanos con las diferentes administraciones públicas y en la colaboración electrónica entre ellas. Tras años de consultas, análisis y modificaciones, ve la luz el Esquema Nacional de Seguridad (ENS) que fue ya anticipado en el año 2007.

Su aparición inicia el ciclo de adaptación de los sistemas y tecnologías de las entidades públicas para hacerlas más seguras. No sólo técnicamente, sino conceptualmente. Deberán definirse procedimientos y casos de uso. La seguridad es cuestión ya de todos, no únicamente de los informáticos. Todo aquel que realiza un tratamiento de la información deberá ser consciente del riesgo a asumir. Será necesario disponer

de los elementos técnicos para el cumplimiento de los objetivos, pero será el colectivo que los usa el valedor de la seguridad. El Esquema Nacional de Seguridad equipara la necesidad de protección de la información con la propia prestación del servicio.

Evidentemente, tal y como demostrará el libro, el camino a recorrer no es trivial. Se requerirán esfuerzos técnicos y humanos, y lógicamente en ocasiones también económicos. Sin embargo, los mecanismos para cumplir lo exigido en el Esquema Nacional de Seguridad se encuentran disponibles. Solo habrá que utilizarlos adecuadamente. Este libro, además de introducirle en los pormenores de la normativa, intentará ofrecer resoluciones técnicas a las medidas previstas haciendo uso para ello de soluciones basadas en productos Microsoft.

Índice de contenidos

1 Antecedentes

Aunque el Esquema Nacional de Seguridad vio la luz en el año 2010, su concepción es mucho anterior. El 22 de Julio del año 2007, con la aparición en el Boletín Oficial del Estado de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a la Administración Pública (LAE), se sentaban las bases para su aparición. Entre el articulado de la ley destacaba el número 42 sobre el Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

> *"1. El Esquema Nacional de Interoperabilidad comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.*
>
> *2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.*
>
> *3. Ambos Esquemas se elaborarán con la participación de todas las Administraciones y se aprobarán por Real Decreto del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local, debiendo mantenerse actualizados de manera permanente.*
>
> *4. En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos efectos considerarán la utilización de estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos."*

Para entender en qué consiste tanto la Ley 11/2007 como el Esquema Nacional de Seguridad (ENS), es necesario conocer primeramente sus motivaciones, qué objetivos persiguen y cuáles son sus fundamentos. Los primeros antecedentes se recogen en la Ley 30/1992 del 26 Noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC). En su primera versión ya recogió, a través de su artículo 45, el impulso al empleo y la aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, por parte de la Administración. Su objetivo era desarrollar su actividad y el ejercicio de sus competencias, permitiendo a los ciudadanos relacionarse con las Administraciones cuando fuese compatible con los medios técnicos de que los que dispusieran.

Esa previsión, junto con la de la informatización de registros y archivos que corresponden al artículo 38 de esa misma ley, abría el paso a la utilización de los sistemas electrónicos para relacionarse con la Administración. Esta circunstancia fue corroborada en la redacción que le dio la Ley 24/2001 de 27 de diciembre del año 2001 sobre Medidas Fiscales, Administrativas y del Orden Social, al permitir el establecimiento de registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones por medios telemáticos.

La misma Ley 24/2001 modificó el artículo 59 de la LRJAP-PAC, permitiendo la notificación por medios telemáticos si el interesado hubiera señalado dicho medio como preferente o consentido expresamente.

> *"**Artículo 68.** Modificaciones de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común para impulsar la administración electrónica.*
>
> *Uno. Se añade un nuevo apartado nueve al artículo 38 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, con la siguiente redacción:*
>
> *Se podrán crear registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones que se transmitan por medios telemáticos, con sujeción a los requisitos establecidos en el apartado 3 de este artículo. Los registros telemáticos sólo estarán habilitados para la recepción o salida de las solicitudes, escritos y comunicaciones relativas a los procedimientos y trámites de la competencia del órgano o entidad que creó el registro y que se especifiquen en la norma de creación de éste, así como que cumplan con los criterios de disponibilidad, autenticidad, integridad, confidencialidad y conservación de la información que igualmente se señalen en la citada norma.*
>
> *Los registros telemáticos permitirán la presentación de solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro horas. A efectos del cómputo de plazos, la recepción en un día inhábil para el órgano o entidad se entenderá efectuada en el primer día hábil siguiente.*
>
> *Dos. Se añade un nuevo apartado 3 al artículo 59 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común,*

con la redacción que a continuación se señala, pasando los actuales apartados 3, 4 y 5 del citado artículo a numerarse como 4, 5 y 6.

Para que la notificación se practique utilizando medios telemáticos se requerirá que el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización, identificando además la dirección electrónica correspondiente, que deberá cumplir con los requisitos reglamentariamente establecidos. En estos casos, la notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el acceso a su contenido en la dirección electrónica. Cuando, existiendo constancia de la recepción de la notificación en la dirección electrónica, transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el siguiente apartado, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso."

Estos cambios adaptativos en las normas iban sentando las bases para la aplicación de medidas técnicas asociadas a las nuevas tecnologías. Sin embargo, el desarrollo de la administración electrónica era todavía insuficiente. La causa de ello en buena medida era que según la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, estas implicaciones son meramente facultativas. Es decir, dejan en manos de las propias Administraciones determinar si los ciudadanos van a poder de modo efectivo o no, relacionarse por medios electrónicos con ellas. Nada exigía la puesta en marcha de medios informáticos para la relación con los ciudadanos. Esta sería factible en función de que las diferentes administraciones quisieran poner en marcha aquellos instrumentos necesarios para permitir este tipo de comunicación,

La puesta en marcha de normativas como la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y la Ley 59/2003, de 19 de diciembre de Firma Electrónica, abrían también un importante camino a la necesidad de uso de las tecnologías en la Administración Pública. La informática empezaba a establecer los diferentes vínculos entre la ciudadanía y las diferentes operaciones administrativas. También desde Europa se establecía la necesidad de fomentar el uso de la tecnología en la relación de los usuarios con las diferentes administraciones. A través de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo del 12 de diciembre de 2006 relativa a los servicios en el mercado interior, se incentivaba el uso de los sistemas telemáticos para el acceso de los ciudadanos.

*"**Artículo 5**. Simplificación de los procedimientos.*

1. *Los Estados miembros verificarán los procedimientos y trámites aplicables al acceso a una actividad de servicios y a su ejercicio. Cuando los procedimientos y formalidades estudiados de conformidad coneste apartado no sean lo suficientemente simples, los Estados miembros los simplificarán.*

***Artículo 6**. Ventanilla única*

1. *Los Estados miembros garantizarán que los prestadores puedan llevar a cabo los siguientes procedimientos y trámites a través de ventanillas únicas:*

a) todos los procedimientos y trámites necesarios para acceder a sus actividades de servicios, en especial las declaraciones, notificaciones o solicitudes necesarias para la autorización por parte de las autoridades competentes, incluidas las solicitudes de inscripción en registros, listas oficiales, bases de datos o colegios o asociaciones profesionales;

b) las solicitudes de autorización necesarias para el ejercicio de sus actividades de servicios.

2. La creación de ventanillas únicas no supone una interferencia en el reparto de funciones o competencias entre las autoridades competentes dentro de cada sistema nacional.

***Artículo 7**. Derecho de información*

1. Los Estados miembros harán lo necesario para que los prestadores y los destinatarios puedan acceder fácilmente a la información por medio de ventanillas únicas.

***Artículo 8**. Procedimientos por vía electrónica*

Los Estados miembros harán lo necesario para que todos los procedimientos y trámites relativos al acceso a una actividad de servicios y a su ejercicio se puedan realizar fácilmente, a distancia y por vía electrónica, a través de la ventanilla única de que se trate y ante las autoridades competentes.

El apartado 1 no se aplicará a las inspecciones del lugar en que se presta el servicio o del equipo utilizado por el prestador ni al examen físico de la capacidad o de la integridad personal del prestador o del personal responsable.

Con arreglo al procedimiento contemplado en el artículo 40, apartado 2, la Comisión adoptará normas de desarrollo para la aplicación del apartado 1 del presente artículo, con el fin de facilitar la interoperabilidad de los sistemas de información y la utilización de los procedimientos electrónicos entre los Estados miembros, teniendo en cuenta las normas comunes desarrolladas a escala comunitaria".

Esta importante directiva marcaba las bases fundamentales para el establecimiento de dos tipos de relaciones. La de los ciudadanos con las diferentes administraciones públicas de los estados miembros, así como la relación entre ellas. También creaban figuras administrativas como las de la ventanilla única, que son ya una realidad en el estado español.

Con las metas ya fijadas, sólo quedaba esperar la salida de la normativa que permitiera cumplir las prerrogativas exigidas. Estas vieron la luz finalmente el 22 de Julio del año 2007 con la publicación de la Ley 11/2007. La Ley de Acceso Electrónico se encuentra articulada en 4 títulos principales más uno preliminar y una serie de disposiciones. El objetivo principal de la norma consiste en reconocer el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. También regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa y en las relaciones entre Administraciones. De igual

modo pasa a regular también las relaciones de los ciudadanos con éstas. Se presenta como finalidad la de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

Las diferentes Administraciones Públicas deberán para ello utilizar las tecnologías de la información de acuerdo a una serie de normas definidas en la Ley. Las máximas para ello son asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que se gestionen en el ejercicio de sus competencias. Estas premisas son procedimientos y terminologías ampliamente utilizadas entre los profesionales de TI, siendo objeto de desarrollo en cualquier proyecto informático. Muchas partes de la ley vienen a precisar cuáles son estas garantías, aunque serán desarrolladas técnicamente en el Esquema Nacional de Seguridad.

Para la resolución de los objetivos se establecen a través de la ley una serie de principios. Estos regulan los derechos reconocidos en otras normas como la LOPD o los propiamente marcados por la Constitución. Los principios más significativos que se encuentran en la norma son:

- **Principio de accesibilidad a la información y a los servicios por medios electrónicos**. Se proporcionarán mecanismos, que a través de sistemas que permitan su utilización de manera segura y comprensible, garanticen especialmente la accesibilidad universal y el diseño para todos de los soportes, canales y entornos.

- **Principio de legalidad**. Presenta como base al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas. Estas fueron establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

- **Principio de seguridad**. La implantación y utilización de los medios electrónicos exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

- **Principio de proporcionalidad**. Sólo se exigirán las garantías y medidas de seguridad adecuadas atendiendo a la naturaleza y las circunstancias específicas de los distintos trámites y actuaciones. Asimismo, sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

- **Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas**. Deberá garantizarse la independencia en la elección de las alternativas tecnológicas tanto por parte de los ciudadanos, como por parte de las Administraciones Públicas. De igual modo, será necesario garantizar la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos, las Administraciones Públicas utilizarán estándares abiertos, así como, de forma complementaria, tecnologías que sean de uso generalizado por los ciudadanos.

De los diferentes títulos que conforman la ley, y en lo concerniente a aspectos técnicos, es el II sobre Régimen Jurídico de la Administración Electrónica el más significativo. A través de éste se establecen importantes figuras como las de sede electrónica, identificación, autentificación, registros y seguridad de las comunicaciones.

Dentro de las figuras jurídicas definidas por la ley, uno de los mecanismos más importantes es el de sede electrónica. La misma ayudará con posterioridad a entender el Esquema Nacional de Seguridad y en qué entornos éste será de aplicación. La sede electrónica es aquella dirección electrónica disponible para los ciudadanos. Su acceso se realizará a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

La norma implica que el establecimiento de una sede electrónica conlleva la responsabilidad por parte de su titular respecto de la integridad, veracidad y actualización, tanto de la información como de los servicios a los que pueda accederse a través de la misma. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que éstas sean necesarias. Por tanto, la prestación de un servicio a través de un acceso web con el objeto de llevar a efecto un procedimiento administrativo define dicho sistema como una sede electrónica.

De cara al acceso a las sedes electrónicas, se establecen las formas relativas a la identificación y autentificación. Se admitirán como válidas aquellas conformadas a través de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. En este sentido, las personas físicas podrán hacer uso del Documento Nacional de Identidad electrónico y otros sistemas autorizados. Por su parte, las sedes electrónicas podrán utilizar, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medios equivalentes.

Los sistemas de firma electrónica reconocidos oficialmente son aquellas provenientes de las siguientes entidades:

- DNIe. Documento Nacional de Identidad Electrónico.
- Camerfirma. Servicio de certificación digital de las cámaras de comercio, industria y navegación de España.
- Izenpe. Proyecto impulsado por el Gobierno Vasco y las Diputaciones Forales. Constituida a través de sus sociedades informáticas: EJIE, LANTIK, IZFE y CCASA.
- CATCert. Agencia Catalana de Certificación.
- ANF AC. Sistema abierto de certificación electrónica.
- SCR. Servicio de Certificación de los Registradores.
- ACA. Autoridad de Certificación de la Abogacía española.
- ACCV Autoridad de Certificación de la Comunidad Valenciana.

- ANCERT. Agencia Notarial de Certificación.
- FNMT. Fábrica Nacional de Moneda y Timbre.
- Firma profesional. Primer prestador privado de servicios de certificación en España.
- BANESTO CA. Entidad certificadora del Banco Nacional Español de Crédito, homologado por la Agencia Tributaria.

Los objetivos perseguidos por la ley y que son inherentes al uso de los certificados electrónicos son:

- La autenticidad de las personas y entidades que intervienen en el intercambio de información.
- La confidencialidad. Tan solo el emisor y el receptor deben ser capaces de visualizar la información que se está manejando en el proceso administrativo.
- La integridad de la información intercambiada. Asegurar que no se produce ningún tipo de manipulación sobre los datos manejados. Aunque la información vaya cifrada, esto no impediría que se pudiera realizar algún cambio aleatorio que modifique y por lo tanto altere la validez del contenido de los datos a asegurar.
- El no repudio. Garantiza al titular del certificado que nadie más que él puede generar una firma vinculada a su certificado. Por otra, le imposibilita a negar su titularidad en los mensajes que haya firmado.

Para la resolución de estos objetivos y a través del certificado digital, podrán realizarse las siguientes operaciones:

- Autentificar la identidad del usuario de forma electrónica ante otros.
- Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.
- Firmar electrónicamente, de forma que se garantice la integridad de los datos trasmitidos y la legitimidad de su procedencia.

La Ley permite que los ciudadanos opten por los sistemas electrónicos como mecanismos de comunicación para sus trámites administrativos, con excepción de aquellos casos en los que una norma con rango de ley establezca la utilización de un medio no electrónico de forma específica. La opción de uso de uno u otro corresponde al ciudadano, pudiendo modificar su elección y optar por un medio distinto del inicialmente elegido. Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido éstos expresamente.

Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro

de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas. Las Administraciones publicarán, en el correspondiente diario oficial y en la propia sede electrónica, aquellos medios electrónicos que los ciudadanos podrán utilizar en cada supuesto administrativo, para el ejercicio de su derecho a comunicarse con éstas.

Para garantizar la comunicación electrónica, los requisitos de seguridad e integridad de las comunicaciones se establecerán de forma apropiada en función del carácter de los datos. Estos quedarán determinados de acuerdo a los criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal. Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, siempre y cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y la disponibilidad de los medios tecnológicos necesarios.

Las Administraciones Públicas deberán utilizar preferentemente medios electrónicos en sus comunicaciones con otras Administraciones. Las condiciones que regirán éstas se determinarán entre las Administraciones Públicas participantes en la comunicación.

Otra figura importante, definida a través de la norma para el tratamiento de información por parte de las administraciones, la constituye el archivo electrónico. Se permite el almacenamiento por medios electrónicos de todos los documentos utilizados en las actuaciones administrativas. Los archivos informáticos que contengan actos administrativos que afecten a derechos o intereses de los ciudadanos deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento inicialmente o en otro, siempre que éste permita asegurar la identidad e integridad de la información necesaria para reproducirlo. En todo caso, es necesario asegurar la posibilidad de trasladar los datos de un formato y soporte a otro distinto, que garantice el acceso desde las diferentes aplicaciones que son proporcionadas para la prestación de servicios.

Los medios en los que se almacenan los documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, deben asegurar la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos personales.

2

El Esquema Nacional de Seguridad

Aunque no existe realmente una equiparación directa entre la Ley de Acceso Electrónico y la Ley Orgánica de Protección de Datos de Carácter Personal, a menudo surgirán las comparaciones entre ambas. Un hecho común lo constituye el que en ambas circunstancias, las leyes no establecen técnicamente qué acciones o medios específicos deberán utilizarse para garantizar la protección de la información. La LOPD tuvo que esperar hasta la salida del Real Decreto 1720/2007 sobre el Reglamento de Desarrollo de la Ley. Por su parte, la LAE ha debido esperar también a la aparición del RD 3/2010 para su desarrollo técnico.

Tal y como se indicaba en páginas anteriores, es la propia ley la que marcaba la espera para la aparición de otra normativa que regulara las medidas de seguridad. En su artículo 42, se designaba que sería el Esquema Nacional de Seguridad (ENS) el que establecería la política de seguridad a aplicar en la utilización de medios electrónicos en el ámbito de la Administración Pública.

El Esquema Nacional de Seguridad (ENS) es publicado en el Boletín Oficial del Estado, el 29 de Enero del año 2010. Entrando en vigor el día después, inicializa el cómputo de tiempo para la adecuación a la normativa y condiciones que quedan establecidas. La dimensión del ENS no es exclusivamente técnica, aunque gran parte de su desarrollo sí lo sea. Las partes organizativas y funcionales también dan contenido a importantes páginas del Real Decreto 3/2010.

El Esquema Nacional de Seguridad se estructura en diez capítulos, más una serie de disposiciones y anexos. Aunque este capítulo abordará principalmente el desarrollo de los capítulos y las disposiciones, la parte fundamental, en lo que a las cuestiones técnicas, estructurales y organizativas se refiere, son tratadas en los cinco anexos que acompañan al Real Decreto.

Hay que comentar que aunque la salida del texto se realiza en el BOE el 29 de Enero del 2010, el 11 de Marzo del mismo año se publica en el Boletín una serie de

rectificaciones sobre errores que se han advertido en la norma. Aquel que desee tener acceso al texto consolidado, podrá realizarlo a través de la siguiente dirección URL perteneciente al Consejo Superior de Administración Electrónica:

http://www.csae.map.es/csi/pdf/RD_3_2010_texto_consolidado.pdf

2.1. Principios básicos

La finalidad última del Esquema Nacional de Seguridad (ENS) es la creación de las condiciones de confianza para el uso de los medios electrónicos. Para ello se definen las medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. El ENS persigue fundamentar la confianza a través de una serie de preceptos:

- Que los sistemas de información prestarán sus servicios sin interrupciones o modificaciones fuera de control.
- Que la información será custodiada de acuerdo con sus especificaciones funcionales sin que ésta pueda llegar al conocimiento de personas no autorizadas.

Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que les dan soporte. Hay que tener en cuenta respecto de este hecho que las relaciones entre las diferentes administraciones públicas son a menudo muy complejas. Deberán ser también evaluadas las relaciones existentes con entidades de ámbito privado y no exclusivamente público. El concepto de seguridad debe observar también la no existencia de parcelas de acción que puedan quedar descubiertas, en "tierra de nadie", permitiendo así la aparición de brechas y carencias de seguridad en los servicios prestados.

En la elaboración del texto del Esquema Nacional de Seguridad han participado muchas organizaciones. En este proceso, y coordinado por el Ministerio de la Presidencia, han participado tanto el Centro Criptológico Nacional (CCN) como todas las Administraciones Públicas del Estado. Entre ellas se incluyen las universidades públicas (CRUE) a través de los órganos colegiados con competencias en materia de administración electrónica: Consejo Superior de Administración Electrónica, Comité Sectorial de Administración Electrónica y Comisión Nacional de Administración Local. Para su elaboración, también han sido importantes los preceptivos emitidos por otras instituciones: Ministerio de Política Territorial, Ministerio de la Presidencia, Agencia Española de Protección de Datos y Consejo de Estado. Finalmente, se han tenido también presentes la opinión de las asociaciones de la industria del sector TIC y las aportaciones recibidas tras la publicación, el 3 de septiembre de 2009, del borrador en el sitio web del Consejo Superior de Administración Electrónica.

Sin embargo, las bases de funcionalidad del ENS son anteriores. En este sentido se tienen en cuenta las recomendaciones de la Unión Europea al respecto:

- Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento Interno.
- Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo.

La seguridad de la información perseguirá los siguientes objetivos principales:

- Proteger la información clasificada de la Unión Europea frente al espionaje, las situaciones de peligro o la divulgación no autorizada de la misma.
- Proteger la información de la UE tratada en los sistemas y redes de comunicación e información frente a las amenazas contra su confidencialidad, integridad y disponibilidad.
- Proteger los locales de la Comisión en los que se encuentra información de la UE frente al sabotaje y los daños intencionados.
- En caso de fallo, evaluar el perjuicio causado, limitar sus consecuencias y adoptar las medidas necesarias para remediarlo.

Para establecer los mecanismos de protección, se designan determinadas áreas de la seguridad que deberán ser atendidas:

- Seguridad personal.
- Seguridad física.
- Seguridad de la información.

Este último punto es el elemento más crítico en el desarrollo del ENS. Aunque la clasificación por niveles establecida por la Decisión 2001/884 EU TOP SECRET, EU SECRET, EU CONFIDENTIAL y EU RESTRICTED, difiere de las marcadas por el ENS, la aplicación de medidas presentan múltiples coincidencias. Las medidas de seguridad, en ambas circunstancias, se aplican en función de la clasificación, teniendo previsto para ello el establecimiento de las dimensiones de seguridad. Pero, ¿qué entidades están supeditadas al Esquema Nacional de Seguridad? La información recogida en el Artículo 3 sobre el ámbito de aplicación de éste, remite al Artículo 2 de la Ley 11/2007. En él se hace una exclusión del ámbito de aplicación de la normativa, para aquellos sistemas que tratan información clasificada y regulada por Ley de 5 de abril 9/1968, de Secretos Oficiales y normas de desarrollo.

*"**Artículo 2**. Ámbito de aplicación.*

1. *La presente Ley, en los términos expresados en su disposición final primera, será de aplicación:*

   a) *A las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.*

b) A los ciudadanos en sus relaciones con las Administraciones Públicas.

c) A las relaciones entre las distintas Administraciones Públicas.

2. La presente Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado."

En un análisis general del Esquema Nacional de Seguridad, su aplicación parece estar bastante relacionada con la aplicación de la norma de calidad ISO 27000. Aun así, el ENS es más preciso, aunque es cierto que algunas de las medidas de seguridad del mismo coinciden con controles de ISO/IEC 27002. De este modo, el Esquema establece un sistema de protección para la información y servicios a proteger. La norma ISO/IEC 27002 carece de esta proporcionalidad en lo que a aplicación de medidas se refiere, quedando este apartado a la mejor opinión del auditor que certifica la conformidad con ISO/IEC 27001. Determinados aspectos fundamentales como la firma o la autenticación electrónica no están recogidos en la norma ISO/IEC 27002.

El principio fundamental que regula el Esquema Nacional de la Seguridad es el de la seguridad integral. Así queda establecido a través del Artículo 5.

"1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad."

Este artículo establece esa necesidad de entender la seguridad como una tarea de todos. La totalidad de los usuarios, que de una u otra forma estén vinculados al tratamiento de datos sujetos a la aplicación del ENS, son parte importante de esa seguridad. En este sentido, no pueden ser argumentados como eximentes ni la falta de conocimiento de un hecho, ni el desconocimiento en el uso de la tecnología.

La seguridad debe ser vista como uno de los principios rectores fundamentales en el tratamiento de los datos. Tanto la tecnología como el factor humano deben ser tenidos en cuenta para ello. Este aspecto es tan preceptivo que se promueve la formación de todos los involucrados, para asegurar así el cumplimiento de sus funciones.

La implementación de un sistema de seguridad pasa inicialmente por realizar un análisis de riesgos. La premisa es, por tanto, conocerse primeramente antes de realizar esfuerzos que podrían ser infructuosos. *"La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad."*

Para la realización de los análisis de riesgos, la Administración Pública cuenta con una herramienta significativa: EAR/PILAR. Está basada en el sistema de análisis de riesgos MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que figura en el inventario de métodos de análisis y gestión de riesgos de ENISA (*European Network and Information Security Agency*). En su versión 2 se ha estructurado en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas":

- **Método**. Describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos. Esta descripción observa la metodología desde tres visones distintas:
  - Describir los pasos para realizar un análisis del estado de riesgo y gestionar su mitigación.
  - Describir las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, estableciendo las pautas, roles, actividades y documentación asociada.
  - Aplicar la metodología a los casos del desarrollo de sistemas de información. Los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento. Tanto aquellos a los que se está expuesto de forma directa, como otros riesgos que las propias aplicaciones pueden llegar a introducir en el sistema.
- **Catálogo de Elementos**. Ofrece pautas y elementos estándar en cuanto al tratamiento de los activos. Para ello se tendrán en cuenta los distintos tipos de activos, las dimensiones de valoración de éstos, los criterios de valoración de los mismos y las amenazas típicas sobre los sistemas de información, junto a salvaguardas a considerar para proteger los sistemas de información.
- **Guía de Técnicas**. Trata de una guía de consulta que proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos. Entre ellas, técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales o análisis coste-beneficio, junto a otros.

Microsoft, por su parte, también ha desarrollado su propia herramienta de evaluación de seguridad: MSAT (*Microsoft Security Assessment Tool*). Está diseñada para ayudar a identificar y abordar los riesgos de seguridad en un entorno tecnológico determinado. Su utilización ofrece una visión general de la seguridad, permitiendo con ello la cuantificación de la misma.

La herramienta utiliza un enfoque integral para medir el nivel de seguridad y cubre aspectos tales como usuarios, procesos y tecnología. Consta de más de 200 preguntas que abarcan infraestructura, aplicaciones, operaciones y usuarios. Las preguntas, respuestas asociadas y recomendaciones se obtienen a partir de las mejores prácticas comúnmente aceptadas, en estándares tales como las normas ISO 27000 y NIST-800.x, así como las recomendaciones y orientaciones normativas del Grupo *Trustworthy Computing* de Microsoft y otras fuentes externas de seguridad.

Para la obtención de resultados, la herramienta hace diversos tipos de preguntas que permiten diferenciar e identificar diversos aspectos de la organización. El primer grupo de ellas presenta como objetivo establecer el modelo de negocio de la misma. Para ello se crea un Perfil de Riesgos de Negocio (BRP), calculando el riesgo de la entidad en sus acciones de negocio según el modelo empresarial definido por el BRP.

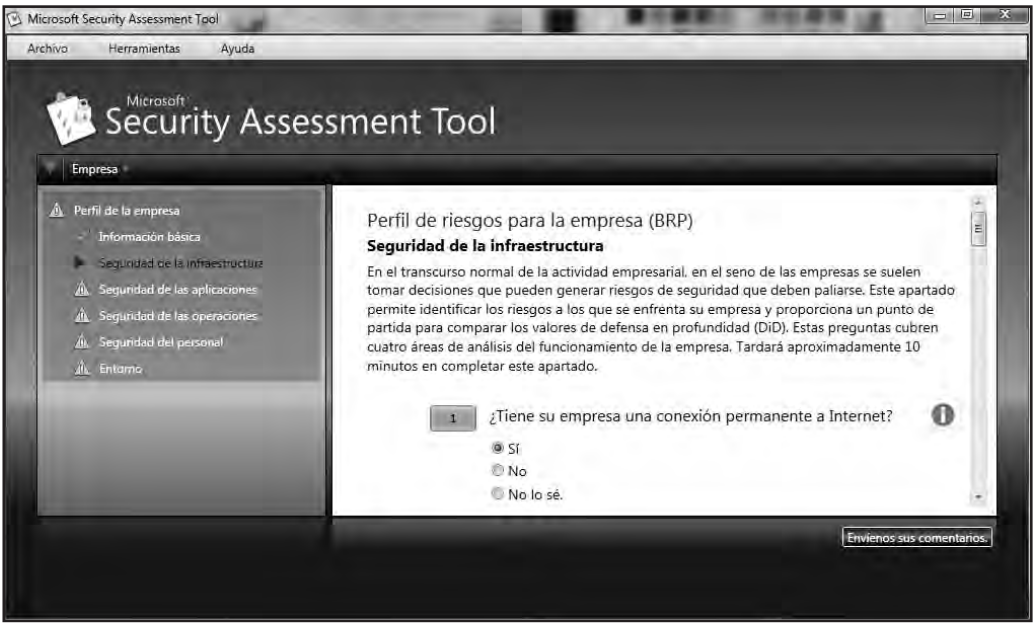


Figura 2.1. MSAT 4.0.

El segundo grupo de preguntas tienen como objetivo elaborar un listado de las medidas de seguridad que se han puesto en producción. Se realiza una evaluación de la seguridad en función de las capas de defensa. Estas proporcionan una mayor protección contra los riesgos de seguridad y vulnerabilidades específicas. Cada capa contribuye a una estrategia combinada que permite implementar una protección en profundidad. Ejemplos de ello son la capa de seguridad perimetral o la seguridad local de las estaciones de trabajo. La suma de todas ellas se conoce como *Defense-in-Depth Index* (DiDI). *Microsoft Security Assessment Tool* (MSAT) se divide en cuatro áreas de análisis (AoAs):

- Infraestructura.
- Aplicaciones.
- Operaciones.
- Personal.

La Figura 2.2 muestra la fase de preguntas sobre las cuatro áreas de análisis mencionadas.

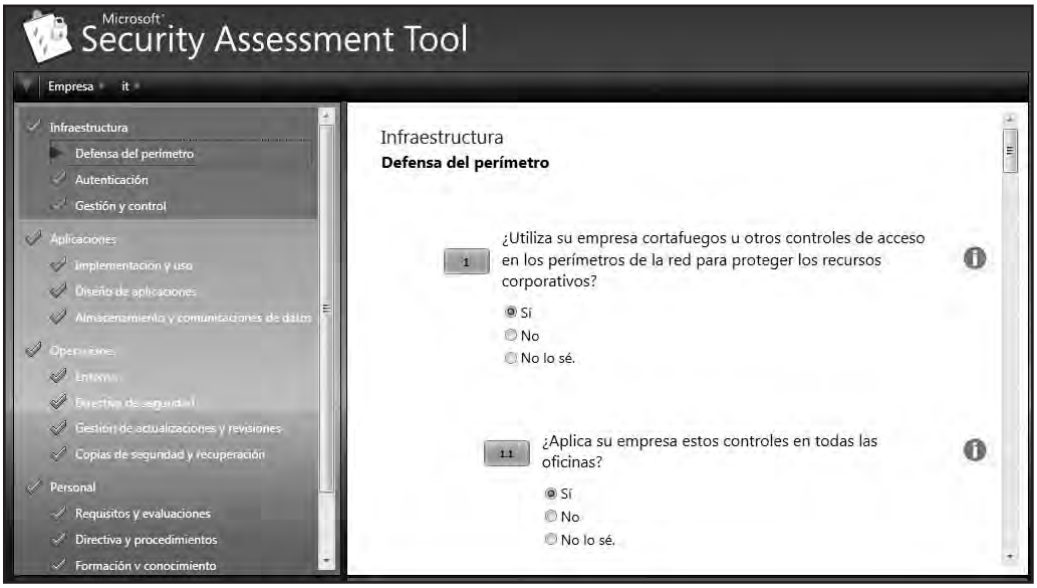


Figura 2.2. Fase de preguntas AoAs en MSAT 4.0.

BRP y DiDI se comparan entonces para medir la distribución del riesgo a través de las diferentes áreas de análisis. Además de valorar la equivalencia entre riesgos de seguridad y defensas, esta herramienta mide también la madurez de la seguridad de la organización. Esta se refiere a la evolución del fortalecimiento de la seguridad y las tareas de mantenimiento de la misma. En el extremo inferior, son pocas las medidas de seguridad empleadas, y las acciones llevadas a cabo son simplemente reacciones a los acontecimientos. En el extremo superior se prueban y establecen procesos que permiten a la compañía una mayor proactividad y una respuesta más eficiente y consistente cuando ésta es necesaria.

Finalizadas las preguntas, la herramienta de análisis muestra los diferentes informes de estado de seguridad para la organización. Estos pueden ser de tipo resumen, completo o comparativo. Este último permitiría visualizar la comparación del estado de seguridad de la organización, con respecto a otras con similares perfiles de negocio.

Por su parte, el informe resumen muestra el perfil de riesgos frente al índice de defensa en profundidad. La siguiente imagen muestra el resultado del análisis del perfil de una empresa tipo, concienciada con la seguridad de sus sistemas y que en este sentido ha aplicado medidas de índole técnico.

Los informes se acompañan también de una serie de mejoras. Las recomendaciones sugeridas para la gestión de riesgos tienen en cuenta la tecnología existente, la presente situación de la seguridad y las estrategias de defensa en profundidad. Las sugerencias van dirigidas a reconocer y aplicar las buenas prácticas más recomendadas en materias de seguridad.

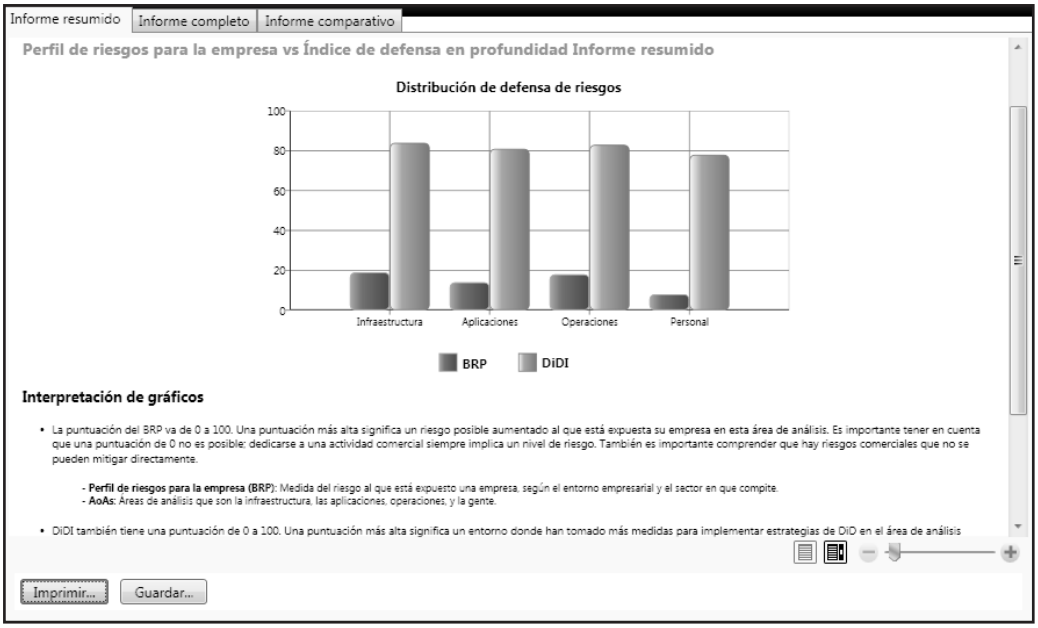


Figura 2.3. Informe resumen.

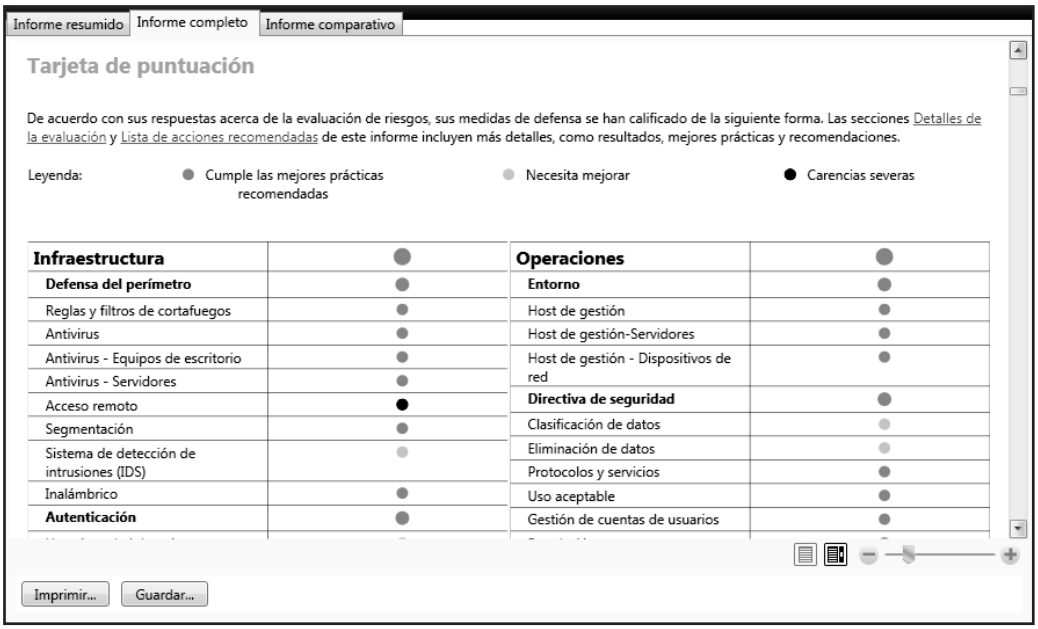


Figura 2.4. Detalle informe completo.

El análisis de riesgos permitirá evaluar el estado de situación de la organización en lo que a seguridad de sus sistemas se refiere. Pero ello sólo supone el inicio del pro-

ceso. Este deberá contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas no se lleguen a producir. En caso de que se materialicen, deberá minimizarse su impacto e intentar paliarlas lo más rápidamente posible. Para ello deberán disponerse medidas tanto reactivas como restaurativas. Estas últimas permitirán la recuperación de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los sistemas o determinados servicios de éstos.

Dentro del análisis de seguridad, un aspecto muy importante tratado en el ENS es el de la segregación de funciones. Ocurre a menudo, que los encargados de analizar el estado de seguridad de una organización son los mismos que deben poner en marcha los sistemas productivos. Este desaconsejable hecho puede producir parcialidad en la actuación de los profesionales, priorizando la producción frente a la aplicación de mecanismos de seguridad.

Con objeto de evitar este tipo de problemas de asignación de funciones, el ENS diferencia en el proceso de segregación de roles los siguientes: responsable de la información, responsable del servicio, responsable del sistema y responsable de la seguridad.

El responsable de información determina los requisitos que deben cumplir la información y los objetivos que se persiguen para su mantenimiento. El responsable del servicio, por su parte, determina los requisitos, las características y las condiciones de los servicios prestados. Este último suele estar supeditado jerárquicamente al responsable de la información.

Frente a ambos el responsable de seguridad presenta un perfil mucho más técnico. De él se espera que establezca los requisitos y condiciones de seguridad de la información y los servicios. Su objetivo fundamental es asegurar que las medidas de seguridad que se van a aplicar satisfacen los requisitos demandados por los responsables de la información y los servicios.

La relación entre todas las figuras la constituye el responsable del sistema. Este será el encargado de las operaciones del mismo y deberá conocer todos los elementos que lo constituyen. Relaciona, a través del sistema, la información, los servicios y la seguridad. Su rol y el del responsable de seguridad deben estar completamente segregados. Ambos serán complementarios, pero sus labores serán diferentes y en ocasiones sus posturas contrarias.

Inicialmente es difícil establecer una norma única de quién debería asumir los diferentes roles y funciones. Cada administración es diferente, tanto en infraestructura como en diseño y personal. Por tanto,m la ocupación de cada rol debería adecuarse a las particularidades de cada entidad o escenario.

2.2. Requisitos mínimos

Para el cumplimiento de las medidas de seguridad, todos los órganos superiores de las Administraciones Públicas deberán contar con una política de seguridad. Esta

presentará unos requisitos mínimos que deberán ser implementados por todas las organizaciones sujetas al Esquema Nacional de Seguridad.

La definición de los órganos superiores viene establecida en el Real Decreto 3/2010 a través de su artículo 11 en el punto 2:

> *"A los efectos indicados en el apartado anterior, se considerarán órganos superiores los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico, de acuerdo con lo establecido en la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado y Ley 50/1997, de 27 de noviembre, del Gobierno; los estatutos de autonomía correspondientes y normas de desarrollo; y la Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local, respectivamente.*
>
> *Los municipios podrán disponer de una política de seguridad común elaborada por la Diputación, Cabildo, Consejo Insular u órgano unipersonal correspondiente de aquellas otras corporaciones de carácter representativo a las que corresponda el gobierno y la administración autónoma de la provincia o, en su caso, a la entidad comarcal correspondiente a la que pertenezcan."*

La política de seguridad tendrá como objetivos fundamentales establecer roles, funciones y procedimientos de designación, definir los criterios para la categorización e identificación de servicios y sistemas, así como plantear los mecanismos de seguridad previstos en el Anexo II. Para ello se exigen una serie de requisitos mínimos que deberán quedar definidos en la política de seguridad:

a) Organización e implantación del proceso de seguridad.
   - Análisis y gestión de los riesgos.
   - Gestión de personal.
   - Profesionalidad.
   - Autorización y control de los accesos.
   - Protección de las instalaciones.
   - Adquisición de productos.
   - Seguridad por defecto.
   - Integridad y actualización del sistema.
   - Protección de la información almacenada y en tránsito.
   - Prevención ante otros sistemas de información interconectados.
   - Registro de actividad.
   - Incidentes de seguridad.
   - Continuidad de la actividad.

b) Mejora continua del proceso de seguridad.

El capítulo III define cada uno de estos principios mínimos, que deben ser tenidos en cuenta por las Administraciones Públicas. Muchas de las figuras descritas son ampliamente utilizadas también en los sistemas de seguridad de las empresas privadas, formando parte de los sistemas SGSI (Sistema de Gestión de Seguridad de la Información) de las mismas.

Se recogen a continuación algunos de los requisitos más notables. Otros serán tratados en mayor profundidad a lo largo de los diferentes capítulos de este libro.

*"**Artículo 16**.*

Autorización y control de los accesos. El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas."

Los procesos de autorización determinan uno de los procedimientos más significativos de cara a la seguridad. En este sentido deberán valorarse en dos circunstancias diferentes:

- Garantizar el acceso de los ciudadanos para la realización de operaciones, tras procesos de autentificación que aseguren la correcta identificación de los mismos.
- Garantizar que a los sistemas internos, sólo el personal autorizado tendrá permitido el acceso.

Una vez que un usuario ha sido autenticado correctamente, se podrá garantizar, mediante los controles pertinentes, el acceso a los recursos asociados.

*"**Artículo 20**. Integridad y actualización del sistema.*

1. *Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.*

2. *Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos."*

La seguridad planteada a través del ENS sólo puede ser observada bajo un prisma de permanente evolución y actualización. Un problema habitualmente planteado por las organizaciones es que una vez implementado un sistema, éste no se altera para evitar la posibilidad de perder su funcionalidad. Sin embargo, desde el punto de vista de la seguridad ésta es una mala práctica. Los sistemas evolucionan, detectándose potenciales fallos de seguridad que los fabricantes corrigen oportunamente y que demandan la actualización de los sistemas. La generación de actualizaciones de seguridad viene normalmente precedida por la aparición de un expediente de seguridad. La aplicación

de soluciones de mejora es por tanto una constante al tratar con elementos software, independientemente de cuál sea su procedencia. El enunciado del Esquema Nacional de Seguridad no es ajeno a este hecho y lo recoge consecuentemente. Cuando un fabricante haga pública la corrección de determinada vulnerabilidad, se deberá actuar conforme a un procedimiento estipulado para corregir el fallo detectado. No obstante, hay que tener en cuenta que una potencial solución podría afectar negativamente al funcionamiento normal del servicio. Para ello habrá de disponerse de algún procedimiento para la realización de las pruebas previas oportunas que permitan aplicar las actualizaciones de seguridad sin por ello alterar el servicio. Este tema es tratado en el Anexo II, en los apartados referidos a los sistemas de mantenimiento.

*"**Artículo 21**. Protección de información almacenada y en tránsito.*

1. *En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.*

2. *Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.*

3. *Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos."*

La salvaguarda de la información es un elemento principal en cualquier valoración respecto de la seguridad informática. No lo es menos para el Esquema Nacional de Seguridad. No se debe olvidar que en la prestación de un servicio lo que realmente aporta valor son los datos manejados por encima de la continuidad del mismo. El acceso de los ciudadanos presentará como objetivo principal el desarrollo de procedimientos administrativos, bien solicitando o bien aportando información. Debe existir la constancia de que ante una pérdida de información asociada al servicio, es posible su recuperación. Por tanto, se establece como garantía fundamental asociada a la labor de la Administración Pública que los datos existentes podrán ser recuperados y mantenidos. La evolución de la tecnología es atendida por el Esquema Nacional de Seguridad, y claro ejemplo de ello son los dispositivos móviles. Fáciles de manejar y de portar, no están exentos de fallos de seguridad. Su portabilidad incrementa el número de amenazas y se hace por ello especial hincapié en las tecnologías de cifrado para los mismos.

*"**Artículo 23**. Registro de actividad.*

Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y

a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa."

Como en otras normativas existentes en el ordenamiento jurídico español constituye una necesidad registrar los sucesos relativos a acciones sobre los servicios y la información. Estos datos permitirán principalmente depurar responsabilidades cuando sea necesario, así como detectar fallos o incidencias de seguridad que hayan tenido lugar en los servicios prestados.

Este objetivo es probablemente uno de los más complicados de cumplimentar. No obstante, no será requerido en todos los escenarios de aplicación del Esquema Nacional de Seguridad, sino exclusivamente en aquellos donde se exigen los niveles de seguridad más altos. Los sistemas a utilizar deberán contar con metodologías de registro, y utilizar procedimientos para la consolidación y correlación de los datos. El servicio sería ineficaz si no tuviera capacidad de alertar frente a una posible incidencia.

*"**Artículo 24**. Incidentes de seguridad.*

1. *Se establecerá un sistema de detección y reacción frente a código dañino.*

2. *Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema."*

Los ataques derivados del descubrimiento de una vulnerabilidad, constituyen uno de los mecanismos más ampliamente utilizado por los hackers para introducirse en un sistema. Para garantizar la seguridad no basta solamente con su planteamiento, sino también es necesario evaluar si las medidas son eficaces. Los sistemas de detección de intrusiones intentan evaluar si un sistema está siendo objeto de ataque. Los intentos de ataque, aunque no se materialicen o tengan éxito en sus objetivos, deben ser detectados e identificados como medida fundamental para mantener niveles apropiados de seguridad.

Un sistema de detección de intrusiones podría ser reactivo mediante la presentación de alertas o acciones que indiquen los intentos de ataque. Esto permitirá que los administradores, además de estar alertados, puedan calibrar el interés como foco de ataque que presentan determinados servicios. Aquellos en los que se observen intentos de ataques más frecuentes, deberían ser considerados más críticos en lo que respecta a su seguridad.

*"**Artículo 25**. Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo."

Puesto que la prestación de un servicio constituye una de las prioridades de la Administración Pública, el Esquema Nacional de Seguridad persigue también como objetivo mantener en todo momento la continuidad del servicio. Por tanto, y a través de las políticas de seguridad, deberán disponerse de mecanismos que permitan tanto la recuperación de los datos como de los propios sistemas, en caso de una potencial incidencia. No obstante, no hay que olvidar que el valor reside en los datos, y su conservación debe prevalecer incluso sobre la prestación del servicio.

> *"**Artículo 29**. Guías de seguridad.*
>
> *Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones."*

Para manejar eficazmente los sistemas con los que cuenta la Administración Pública, el Centro Criptográfico Nacional ha elaborado, y continuará haciéndolo, un conjunto de guías para el uso de diferentes tecnologías. En este sentido, Microsoft participa junto con el CCN en la elaboración de las mismas en lo que respecta a sus tecnologías y soluciones específicas.

La serie CCN-STIC-500 (Centro Criptográfico Nacional - Seguridad de las Tecnologías de la Información) recoge las diferentes guías desarrolladas conjuntamente para entornos Windows. Adicionalmente a los documentos, se proporcionan una serie de scripts que permiten, a través de las políticas de seguridad, mejorar determinados escenarios atendiendo a la normativa existente.

2.3. Comunicaciones electrónicas

Uno de los peligros potenciales que presenta el tratamiento de datos lo constituye el ataque a la información en tránsito. Existen numerosas técnicas que presentan como objetivo el ataque en redes de datos. A través de las mismas, un tercero intentará bien suplantar a una de las dos entidades participantes en la comunicación, o bien obtener la información que se estuviera intercambiando.

La alteración en tránsito de una comunicación para el desarrollo de un procedimiento administrativo podría conllevar su anulación, o lo que es peor, si el sistema permite aceptar una autenticación falsa por imposibilidad de validar correctamente un certificado digital, se inutilizaría uno de los mecanismos fundamentales en los que está basado el Esquema Nacional de Seguridad.

Los sistemas de certificación electrónica cumplen una labor muy importante. Hay que recordar que a través del uso de los servicios tipo PKI (Public Key Infraestructure) se persiguen dos objetivos fundamentales:

- El firmado, con objeto de garantizar la autenticidad, el no repudio y la integridad de los datos.

- El cifrado, para garantizar la confidencialidad de los datos.

En un proceso de comunicación se persiguen precisamente estos objetivos, por lo que los sistemas de certificación electrónica resultan indispensables: bien sea para autenticar a un ciudadano, como para garantizar una comunicación cifrada mediante SSL (*Secure Socket Layer*) o hacer un uso eficiente del correo electrónico mediante la utilización de S-MIME (*Secure / Multipurpose Internet Mail Extensions*).

*"**Artículo 31**. Condiciones técnicas de seguridad de las comunicaciones electrónicas.*

1. *Las condiciones técnicas de seguridad de las comunicaciones electrónicas en lo relativo a la constancia de la transmisión y recepción, de sus fechas, del contenido integro de las comunicaciones y la identificación fidedigna del remitente y destinatario de las mismas, según lo establecido en la Ley 11/2007, de 22 de junio, serán implementadas de acuerdo con lo establecido en el Esquema Nacional de Seguridad.*
2. *Las comunicaciones realizadas en los términos indicados en el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que resulte de aplicación.*

***Artículo 32**. Requerimientos técnicos de notificaciones y publicaciones electrónicas.*

1. *Las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos se realizarán de forma que cumplan, de acuerdo con lo establecido en el presente real decreto, las siguientes exigencias técnicas:*
   a) *Aseguren la autenticidad del organismo que lo publique.*
   b) *Aseguren la integridad de la información publicada.*
   c) *Dejen constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.*
   d) *Aseguren la autenticidad del destinatario de la publicación o notificación."*

El uso de los sistemas de certificación electrónicos se considera de obligado cumplimiento. Según lo estipulado por la normativa, será el mecanismo principal para garantizar la autenticidad de los ciudadanos que acceden a los servicios que prestan las administraciones públicas. Pero también pueden ser utilizados para garantizar el acceso del personal interno para el tratamiento de los datos.

Hay que tener presente en este sentido la importancia que implican los procedimientos de comunicación administrativos. Serán factibles y tendrán tanta validez como los sistemas tradicionales, siempre y cuando cumplan con una serie de preceptos. En todos ellos la política de firma y certificado electrónico presenta una labor muy importante:

- Cifrado de los datos.

- Firma digital de la información.
- Firma de marca tiempo para el sellado electrónico.

En el desarrollo de los procedimientos administrativos el cumplimiento temporal es crítico a la hora del establecimiento de resoluciones. Por ello, el uso de sistemas de certificación electrónica para la implementación del Time Stamp es otra de las necesidades a cubrir por los certificados digitales.

2.4. Auditoría de seguridad

Para garantizar la aplicación de medidas y evaluar el debido funcionamiento de los sistemas implementados, el Esquema Nacional de Seguridad (ENS) define la necesidad de realizar periódicamente auditorías de seguridad. El sistema de auditoría queda definido a través del Capítulo V y el Anexo III.

*"**Artículo 34**. Auditoría de la seguridad.*

1. *Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.*

   Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior."

Los sistemas de auditoría deben servir como el mecanismo catalizador que determine que las medidas técnicas aplicadas son como mínimo suficientes, que cumplen sus cometidos y que los procedimientos se realizan de acuerdo a lo estipulado en la política de seguridad. No obstante, su realización depende del tipo de categoría de seguridad que queda determinada en el Anexo I. Aunque este tema será tratado con posterioridad, es importante indicar en este momento que existen tres categorías en función de la criticidad: básica, media y alta.

En el caso de las categorías media y alta, la auditoría deberá realizarla un equipo independiente a la organización. En el caso de categoría básica, la auditoría podrá ser de tipo auto evaluativo. Un equipo interno determinará el cumplimiento y las medidas correctoras que deberían aplicarse si hubiera lugar a ello.

Puesto que el ENS no regula completamente los procedimientos de auditoría, el CCN ha emitido una guía para ello. La guía 802 de Auditoria del Esquema Nacional de Seguridad desarrolla las materias necesarias para dar cumplimiento a lo establecido en el artículo 34 y en el Anexo III del RD 3/2010. Entre estas medidas podrán encontrarse los mecanismos para la realización de las auditorías, los requisitos que deberán cumplir el equipo de auditores o la elaboración y presentación de resultados.

Con objeto de garantizar la independencia, las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas como responsabilidades de consultoría o similares. Tampoco deberá proponerse la implantación de un determinado software o solución específica. El auditor será el responsable de las opiniones y conclusiones vertidas en el informe de auditoría.

Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competente. Estos serán valorados por este último, que enviará sus conclusiones al responsable del sistema. Será éste el que deberá dictaminar y aplicar las medidas correctoras oportunas.

2.5. Respuesta a incidentes de seguridad

De cara a la coordinación de tareas frente a incidencias que pudieran darse, el CCN a través de su estructura CCN-CERT (Centro Criptológico Nacional - *Computer Emergency Reaction Team*), será el encargado de articular las respuestas de las diferentes administraciones públicas. Sus acciones se realizarán sin perjuicio de las capacidades de respuesta propias con las que pueden contar cada administración y de la función de coordinación a nivel nacional e internacional del CCN.

*"**Artículo 37**. Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.*

1. *De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:*

   a) *Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.*

      El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas.

      Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar los informes de auditoría de los sistemas afectados.

   b) *Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional - Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración."*

Tal y como se comentó previamente, existen guías de seguridad relacionadas con productos Microsoft que garantizan el cumplimiento de medidas exigidas a nivel normativo. Pero no solamente en esto existe colaboración entre Microsoft y el CCN-CERT, también trabajan estrechamente en la prevención y mitigación de incidentes. Fruto de esta colaboración se han firmado acuerdos entre los que incluye el acceso al código fuente de Windows y MS Office, así como la asistencia y suministro de herramientas para poder auditar la seguridad de un sistema. Este hecho se produce desde el año 2004, cuando el gobierno español se adhiere al programa de *Microsoft Government Security Program* (GSP).

2.6. Adecuación tras la entrada en vigor del ENS

Para la implantación de procedimientos y medidas de seguridad se han fijado unos tiempos que permitan la adecuación de los sistemas a lo establecido por el Esquema Nacional de Seguridad. El camino a recorrer no es trivial, y hay que tener en cuenta que para que un organismo pueda poner en producción un sistema de seguridad tienen que darse de forma previa una serie de condiciones:

- El órgano superior correspondiente deberá haber creado la política de seguridad.
- Deberá haberse realizado el análisis de riesgos correspondiente.
- En el Esquema Nacional de Seguridad, se diferencian dos tipos de proyectos:
- Aquellos que se desarrollan después de la entrada en vigor.
- Los existentes con anterioridad a la publicación de la norma.

Los primeros deberán iniciarse bajo el paraguas de acción del ENS. En el caso de los segundos, se establece en un año el tiempo de adecuación para el cumplimiento de la normativa. En el caso de que concurran circunstancias que impidan la plena aplicación de lo exigido, se dispondrá de un plan de adecuación que marque los plazos de ejecución. Estos plazos no podrán exceder los 48 meses, desde que entra en vigor el Esquema Nacional de Seguridad.

Como existe una relación directa entre la creación de la política de seguridad y la aplicación del ENS, se admite que mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas que puedan existir a nivel de órgano directivo. En el momento de escribirse este libro, el CCN en virtud de las funciones atribuidas en el RD 421/2004 se está encargando del estudio y realización de diferentes guías que versan sobre el ENS. Entre éstas, se incluye la Guía 805 del modelo de política de seguridad. Algunas de las mismas se encuentran ya en fase borrador, aunque no son totalmente públicas en este estado, siendo su acceso restringido.

2.7. Régimen sancionador

El Real Decreto 3/2010 no presenta entre su articulado ninguna mención relativa al régimen de tipo sancionador. Hay que tener en cuenta que la orientación del

Esquema Nacional de Seguridad es para la Administración Pública, y ésta presenta su propia normativa en cuanto a responsabilidades. Puesto que el ENS no dictamina otra cosa, será de aplicación lo previsto en 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Esta ley, además de regular el régimen sancionador y la potestad para la misma, determina los principios de responsabilidad tanto civiles como penales, y los procedimientos de indemnización que pudieran tener lugar por daños ocasionados por el incumplimiento de la normativa.

3

Principios de seguridad: seguridad por defecto

Uno de los principios más significativos que persigue el Esquema Nacional de Seguridad es el de la seguridad por defecto. La idea es sencilla, minimizar el impacto de la seguridad deshabilitando aquellos elementos innecesarios y activando todos aquellos otros que sean factibles. El objetivo es que tras la aplicación de la totalidad de mecanismos de seguridad, los posibles fallos que puedan aparecen tengan como origen exclusivamente la acción inadecuada por parte de un usuario

*"**Artículo 19**. Seguridad por defecto.*

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.

Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario."

A menudo de forma inconsciente, en la puesta en producción de un nuevo servicio se han dejado instalados determinados elementos o características que ya son innecesarios. El problema no es en sí la existencia de este tipo de servicios, sino que

seguramente no se realice un mantenimiento adecuado de los mismos, descuidando incluso aspectos de seguridad. Esto provoca un factor crítico como es el hecho de que un elemento vulnerable haga que la globalidad del sistema también lo sea, por muy asegurado que se mantenga el resto de elementos que lo componen.

Por ejemplo, si todo un sistema utiliza algoritmos de cifrado para garantizar que las contraseñas de autenticación de casi todos los servicios sean seguras, y sin embargo si en uno de ellos la información es enviada en texto plano, se pone en riesgo toda la seguridad del sistema en su conjunto. La seguridad es un sistema de engranajes que debe ser funcional en su conjunto. Un defecto hará caer el mecanismo de forma global. Para evitar esos problemas se promueve la seguridad por defecto.

Este concepto no es ni mucho menos nuevo. Desde el momento del diseño de un software, pasando por su análisis, desarrollo y puesta en producción, se debe pensar en la seguridad. El resultado final es precisamente la seguridad por defecto. La puesta en marcha de la iniciativa Trustworthy Computing (TC) por parte de Microsoft en el año 2002, como uno de los pilares básicos para el desarrollo y la implementación de todo su software, ha supuesto una mejora evolutiva en la seguridad general de sus soluciones. TC cubre cuatro directrices fundamentales en las tecnologías SD3+C: "Secure by Design", "Secure by Default", "Secure by Deployment" y "Communication" (seguro por diseño, seguro por definición, seguro en distribución y comunicaciones).

Los esfuerzos iniciales han ofrecido finalmente resultados significativos. Los sistemas operativos a partir de Windows Vista han nacido atendiendo en todo su desarrollo a esta iniciativa, cosechando de este modo grandes resultados en seguridad. Las evoluciones observadas en Windows 7 o en las versiones correspondientes de servidor, Windows Server 2008 y Windows Server 2008 R2, no hacen más que afianzar la buena respuesta de la iniciativa. Estos sistemas operativos presentan datos significativos, no sólo en lo que respecta a las nuevas tecnologías que en materia de seguridad incorporan, sino también en la disminución drástica del número de fallos de seguridad. No sólo los sistemas operativos, sino también servicios y servidores, han visto mejorado en sus diseños los elementos de seguridad.

Para que esta iniciativa fuera factible se definió un proceso complejo, donde ya la fase inicial de diseño se lleva e efecto desde la panorámica de la seguridad. Denominado Secure Development Lifecycle (SDL), el proceso se encuentra estructurado en diferentes fases. La de diseño identifica la estructura y los requisitos globales del software. Desde el punto de vista de la seguridad, los elementos clave de ésta son:

- **Definir la arquitectura de seguridad y las directrices de diseño**. Se define la estructura global del software desde el punto de vista de la seguridad, identificando los componentes cuyo correcto funcionamiento es esencial para ésta (la "base de computación confiable"). La identificación de técnicas de diseño, como el uso de capas o lenguaje con tipos inflexibles, la aplicación de privilegios mínimos y la minimización de la superficie de ataque se aplican al software de manera global. El uso de capas define componentes bien definidos que se estructuran para evitar dependencias circulares entre ellos.

Otro de los objetivos hace referencia al uso del mínimo privilegio posible. Cuanto menores sean los requerimientos para la ejecución de una aplicación, menores serán los riesgos generales que sufrirá un sistema por su utilización.

Algunas de las peores amenazas que presentan los usuarios es la navegación por Internet. A través de ésta, los riesgos de uso del sistema pueden aumentar significativamente al estar expuestos a otros sistemas que no siempre son de confianza. Reduciendo los privilegios con los que cuenta el navegador, se reduce el impacto en caso de que una amenaza procedente del exterior intente afectar al sistema. El objetivo por lo tanto es el menor privilegio posible.

- **Documentar los elementos de la superficie de ataque del software**. Teniendo en cuenta que difícilmente el software logrará una seguridad perfecta, es importante que únicamente se expongan de manera predeterminada las características que utilicen la mayoría de los usuarios y que éstas se instalen con el mínimo nivel de privilegios posible. La medición de los elementos de la superficie de ataque ofrece al equipo de producto un indicador continuo de la seguridad predeterminada y les permite detectar las instancias en las que el software es más susceptible de recibir ataques. Reduciendo la superficie del ataque se consiguen minimizar los posibles riesgos. Esa reducción tanto en la superficie como en el uso de privilegios se ha trasladado a los sistemas operativos. Windows Vista trajo consigo muchos cambios de seguridad en este sentido, pero la división de las capas, la segmentación y la aparición de servicios restringidos o los controles de gestión de sesiones han sido avances que aparecen justamente con la iniciativa TC.

- **Realizar un modelado de las amenazas**. Se debe pensar en el diseño de un sistema desde los riesgos. Igualmente que el Esquema Nacional de Seguridad requiere la realización de un análisis de riesgos para la implementación de la seguridad, en el diseño del software se evalúan desde el inicio las amenazas por las que éste podría verse afectado. El equipo de trabajo debe realizar un modelado de riesgos por componentes. Mediante una metodología estructurada, se identificarán los activos que debe administrar el software y las interfaces que permitirán el acceso a dichos activos. El proceso de modelado identifica las amenazas que pueden dañar a estos activos y se realiza una estimación del riesgo entre los casos de uso. Esto permitirá determinar las medidas que podrán contrarrestar las amenazas. Fruto de este tipo de análisis, no sólo se han creado metodologías y procedimientos, sino un software que puede ser utilizado para el que desee un desarrollo basado en un diseño seguro: Threat Analisys & Modeling (TAM).

- **Definir los criterios de publicación adicionales**. En el proceso de desarrollo deben evaluarse las vulnerabilidades de seguridad y solucionarlas antes de que se detecten. Desde un punto de vista funcional la idea es acotar los fallos de seguridad identificados en las versiones previas del desarrollo de un software. Todas ellas deberán ser corregidas, evaluando las caracterís-

ticas que propiciaron este hecho y determinando la posibilidad de nuevos modelos para paliar posibles defectos de diseño. El resultado final será un menor número de vulnerabilidades desde el inicio del desarrollo, que se verá plasmado en la disminución de expedientes de seguridad.

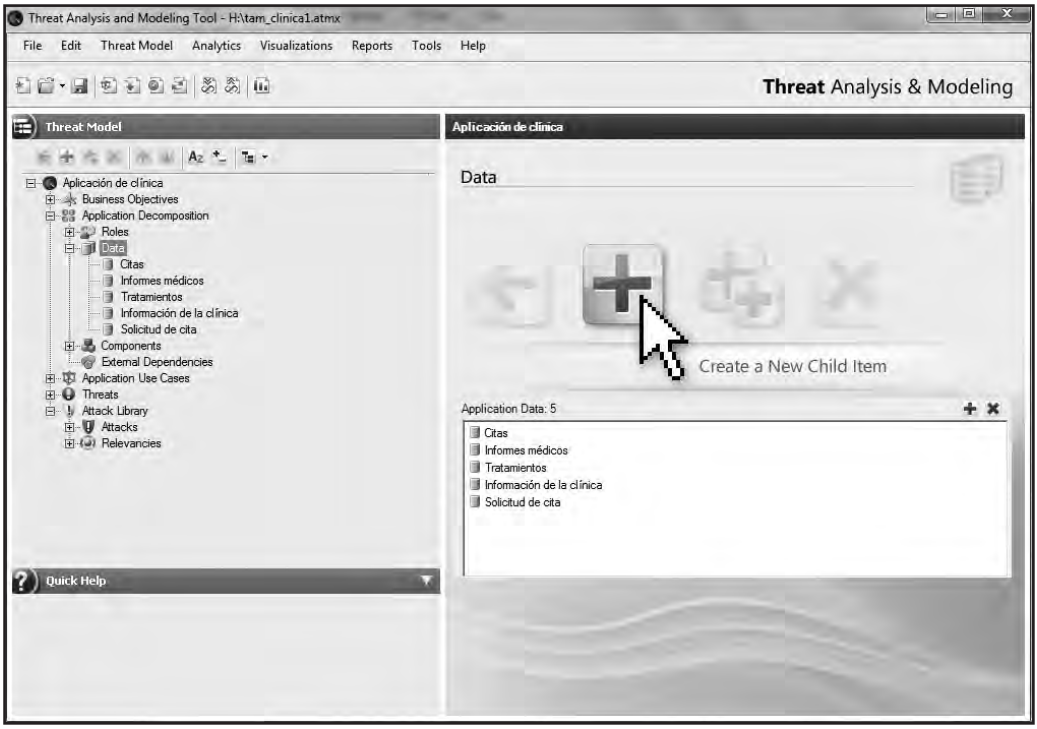


Figura 3.1. Threat Analisys & Modeling.

Durante la fase de implementación, el equipo de trabajo se encargará de programar, probar e integrar el software. Durante los pasos previos se han destinado esfuerzos para eliminar los errores de seguridad o minimizarlos y evitar desde el principio su inclusión. Valorando inicialmente los distintos tipos de amenazas, se consigue que al consolidar los diferentes módulos se tenga una visión clara de los riesgos finales. A la hora de la realización de las pruebas de seguridad, será de gran utilidad conocer los riesgos posibles y las contramedidas que se diseñaron en función de los mismos.

Desde su comienzo, en la fase de implementación se aplican estándares de codificación y de pruebas que evitan que los programadores incluyan errores que produzcan vulnerabilidades de seguridad. Se utilizan también herramientas de testeo que probarán la funcionalidad segura del código. No basta que un desarrollo haga la función para la que ha sido diseñado, sino que debe única y específicamente desarrollar esa función y además salvaguardando la seguridad del sistema. Alguna acción adicional no controlada ni documentada podría incidir negativamente en aspectos de seguridad. Así surgen muchos exploits, atacando funciones no controladas.

Las siguientes dos fases son muy importantes para la comprobación de la seguridad final con la que contarán los módulos de nuevo diseño: fases de comprobación y fase de lanzamiento. Estas fases son consecutivas y comienzan desde el punto en el que el software presenta ya casi toda su funcionalidad operativa. Durante estas fases, mientras se prueba la versión beta del software, el equipo de producto realiza un nuevo análisis de seguridad que incluye revisiones del código de seguridad. Estas son adicionales a las ya realizadas en la fase de implementación, recogiendo además todas las impresiones que proporcionan los usuarios que participan en los programas Beta.

En la fase de lanzamiento, el software se someterá a una revisión final de seguridad (FSR). Esta deberá responder a una pregunta: "Desde el punto de vista de la seguridad, ¿está este software preparado para los clientes?" Esta revisión se realiza en un plazo de dos a seis meses antes de la finalización del software, según el alcance de éste. Para ello, el software deberá ser estable antes de la realización de los análisis FSR y es de esperar que con antelación al lanzamiento sólo se realicen cambios mínimos y no relacionados con la seguridad.

El SDL (*Secure Development Lifecycle*) no finaliza bajo ninguna circunstancia con el lanzamiento del software. La última fase, y la más larga, consiste en su reanálisis y mantenimiento en todo el ciclo de soporte para el mismo. Se asume que ningún software aparece en el mercado completamente seguro, aun cuando en el proceso de desarrollo se hubieran podido eliminar todas las vulnerabilidades de seguridad conocidas. Con certeza y como mínimo, se descubrirán nuevos ataques y el software considerado "seguro" pasará a presentar vulnerabilidades. Por tanto, los equipos de producto deben prepararse para responder a nuevas vulnerabilidades, reconocer los nuevos expedientes de seguridad que se produzcan, conocer las nuevas técnicas de ataque, intentando con todo ello paliar lo más rápidamente posible los nuevos fallos de seguridad detectados.

La iniciativa *Trustworthy Computing Secure Development Lifecycle* presenta muchos puntos en común con el Esquema Nacional de Seguridad, y es que pensando o diseñando seguridad, los objetivos a perseguir son lógicamente similares. TC se apoya en el SDL, y la visión de S3D+C también se persigue en el ENS. La seguridad por defecto es uno de los pilares de la iniciativa Trustworthy Computing. Sus objetivos de seguridad se han visto favorecidos reduciendo la superficie de ataque, no habilitando servicios innecesarios e introduciendo nuevas tecnologías para la consecución de esta tarea. Por ejemplo, si un administrador desea una determinada funcionalidad, y ésta se encuentra asociada a un servicio no instalado por defecto, será necesario desplegarlo de forma intencionada. Esto favorece el hecho de que el administrador sea conocedor de los nuevos elementos instalados. Si esta misma circunstancia se diese por defecto, incorporando de forma automática elementos que no son demandados de forma específica, implicará que seguramente no se tenga constancia de su existencia o que su mantenimiento no sea el adecuado.

En este sentido, desde Windows Vista y Windows 2008 han surgido una serie de mecanismos enfocados a conseguir precisamente esos objetivos; nuevas tecnologías que proporcionan mejoras significativas en seguridad. Algunas veces éstas son más

visibles, como el control de cuentas de usuarios (UAC), pero en otras, como en la gestión de roles y características, no ocurre así. Sin embargo, todas ellas presentan como objetivo el minimizar el impacto en la seguridad. Servidores como Windows Server 2008 y Windows Server 2008 R2 han visto tan minimizado el tipo de aplicaciones y servicios instalados por defecto que el simple hecho de querer utilizar un cliente Telnet requiere de su instalación consciente en el servidor.

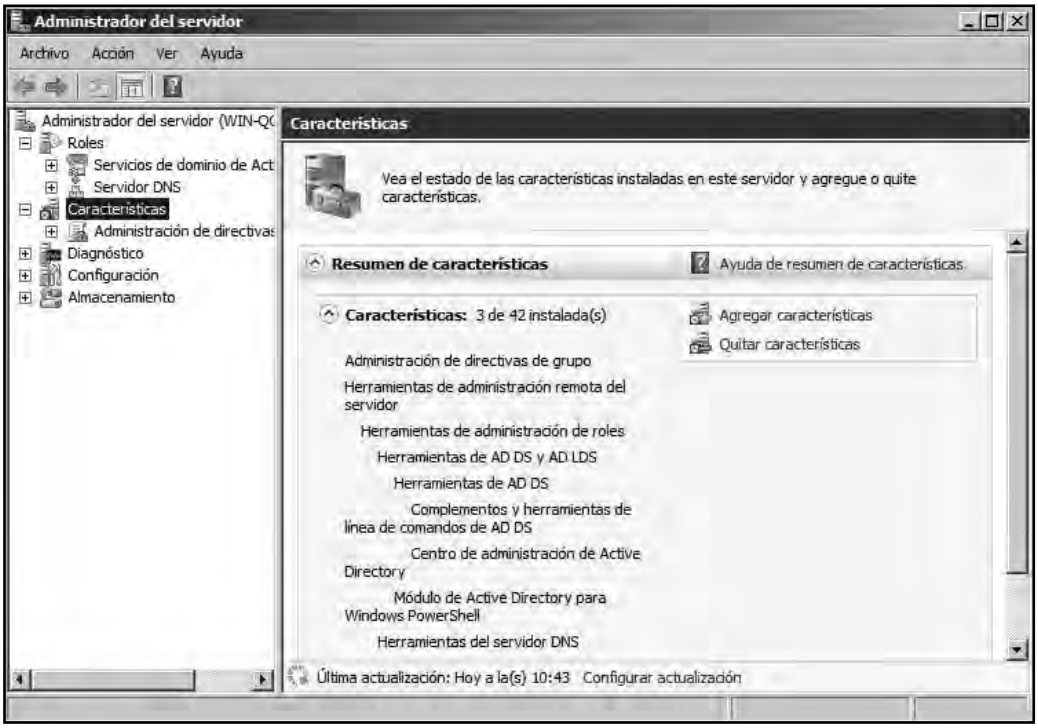


Figura 3.2. Administrador de roles y características en Windows Server 2008 R2.

Pero la seguridad por defecto no atiende por ella misma todas las demandas que en este sentido realiza el Esquema Nacional de Seguridad. Se necesita una labor evolutiva en diferentes fases desde la puesta en producción hasta la retirada final de un servicio. La primera suele ser considerada como una de las fases más críticas. Microsoft plantea determinadas iniciativas y programas dirigidos a la comunidad TI, con el objeto de que los profesionales conozcan cómo adaptar y configurar los mecanismos de seguridad necesarios y disponibles sobre sus elementos en explotación.

Programas como STPP (*Strategic Technology Protection Program*), persiguen elevar el nivel de seguridad en los sistemas. Para ello se plantea la estrategia en relación a tres elementos fundamentales que conectan directamente con el ENS:

- **Personas**. La formación de los administradores y usuarios es un aspecto crítico que se recoge en los artículos 14 y 15 del RD 3/2010: gestión de per-

sonal y profesionalidad. De nada vale disponer de los sistemas más eficaces y seguros si las malas prácticas propician los fallos de seguridad. Aunque se han enfocado esfuerzos para minimizar este impacto, como el uso del UAC, finalmente son siempre dependientes del usuario.

- **Procesos**. Plantear procedimientos de aplicación de modelos de seguridad y establecer los mecanismos de seguridad a utilizar son una referencia a considerar en todo momento. El uso de procedimientos es una práctica habitual en los ciclos de uso de la seguridad. Evaluar el cumplimiento de las normas requeridas o el uso eficaz de los servicios desplegados son garantías para un uso seguro de los sistemas.

- **Tecnología**. Para completar un sistema de seguridad, además de poseer los conocimientos, debe contarse con una serie de herramientas que faciliten la administración de la seguridad y sean capaces de reducir la dedicación de tiempos administrativos. El inventariado de los activos y el mantenimiento de los mismos se persigue también como un objetivo en el ENS. De hecho, está contemplado en su parte técnica dentro del conjunto de medidas destinadas a la explotación.

Fruto de esa seguridad por defecto se han implementado nuevas tecnologías. Pretenden cumplir con los objetivos planteados en seguridad y que son coincidentes en el Esquema Nacional de Seguridad. Aunque algunas de estas tecnologías serán tratadas minuciosamente en el Capítulo 6, donde se trata la implementación técnica, merecen en este momento una mención como muestra de la evolución que está teniendo lugar en el uso de los sistemas.

- *User Account Control* (UAC). Referenciado con anterioridad en este manual, supone un paso significativo en la relación de la seguridad con el uso cotidiano de los sistemas operativos. Habitualmente, y quizás motivado por el uso de los sistemas previos, las cuentas con derechos privilegiados son utilizadas con frecuencia para la realización de tareas comunes como la navegación en internet o el tratamiento de documentos, que no requieren de dichos privilegios. Estas dos acciones tan usuales pueden introducir serias amenazas en el sistema. Esta circunstancia se evitaría no actuando con una cuenta de administrador si no es necesario y el riesgo puede minimizarse con el uso de UAC. Este, que se encuentra activo de forma predeterminada, proporciona a los usuarios detalle de cuándo una de las acciones que se están llevando a cabo requiere de privilegios para completarse. Puede ilustrar esta circunstancia el hecho de que navegando por internet el acceso a una página requiera la instalación de un componente. En el caso de que UAC se encuentre activo, se advertirá que este nuevo elemento requiere modificar el sistema, alertando del potencial riesgo que esto podría implicar. De este modo, el usuario conscientemente evaluará con mayor criterio las consecuencias derivadas de este hecho.

- *Mandatory Integration Control* (MIC). El módulo MIC consolida un método de control adicional a las DACL (*Discretionary Access Control*) para la ejecución

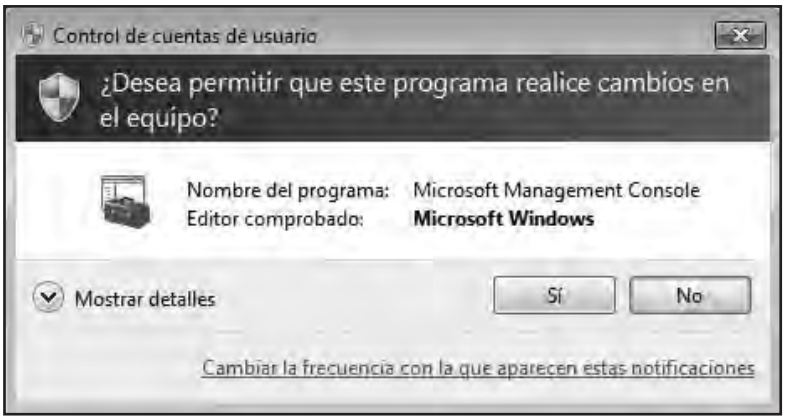


Figura 3.3. Control de cuentas de usuarios en Windows 7.

de las aplicaciones que pudiera soportar un sistema. MIC gestiona una serie de niveles de integridad, de tal forma, que en función del tipo de usuario, se tendrá o no acceso a la ejecución del nivel de integridad correspondiente. El tipo de aplicación será el factor fundamental en este caso. Los niveles de ejecución que se corresponden con los niveles de integridad son cinco: integridad 0 (sin confianza), integridad 100 (bajo), integridad 200 (medio), integridad 300 (alto) e Integridad 400 (sistema). Cada cuenta presenta unos tokens con niveles de integridad específicos. En función del token de usuario y el nivel de integridad de la aplicación o servicio, un usuario podrá o no ejecutarla. Esto evitará que un usuario pueda ejecutar una aplicación con un nivel de integridad superior al que se le asigna de forma predeterminada.

- *User Interface Privilege Isolation* (UIPI). Esta tecnología bloquea aquellos procesos que con una menor integridad intentan acceder a un servicio, proceso o aplicación con mayor nivel de integridad. Los ActiveX, componentes de ayuda a la navegación o toolbars, son algunas de las aplicaciones que pueden ser bloqueadas en los procesos de navegación, dado que intentan acceder al sistema para su alteración. Si uno de estos elementos con un nivel de integridad bajo desea interactuar por ejemplo con una aplicación del sistema para modificarla, esta acción será bloqueada de forma predeterminada.

- *Data Execution Prevention* (DEP). Bajo este epígrafe, Microsoft ha generado un mecanismo de seguridad que tiene como objetivo evitar la ejecución de aplicaciones desde las páginas de memoria de datos. Numerosos elementos de malware y ataques por desbordamiento de buffer escriben información nula para sobrepasar la longitud de memoria reservada para el uso de sus parámetros. Intentan de este modo sobrescribir la dirección de retorno del contador de programa. Para ello se buscan parámetros en procedimientos que no han sido correctamente comprobados antes de ser utilizados. De esta forma se intenta introducir el programa que se quiere ejecutar, por ejemplo una shell ajena al sistema. Por tanto, DEP tiene como objetivo prevenir este tipo de ataques, monitorizando las aplicaciones, para hacer un uso correcto de la pila de memoria.

- *Address space layout randomization* (ASLR). Esta tecnología propicia un uso aleatorio de la memoria. De este modo el sistema operativo en el momento de cargar las librerías (que sólo debían ser utilizadas por éste) propicia que éstas se carguen en diferentes lugares de la RAM, haciendo complicado la repetición y exportación de un exploit. De esta forma, en cada arranque de la máquina las direcciones son distintas impidiendo su exportación y repetición al no conocer el mapa de memoria, distinto en cada caso.
- *Bitlocker y Bitlocker to go*. Las tecnologías de cifrado constituyen también una tónica general de uso en la aplicación de las normativas jurídicas relacionadas con las tecnologías. Microsoft ha evolucionado también en este sentido, sumando algunas nuevas técnicas a las más tradicionales como EFS (*Encripted File System*). En Windows Vista (para discos de sistema) y finalmente con Windows 7 (también para elementos extraíbles), se han consolidado los sistemas por defecto para el cifrado de los datos, tanto en el propio sistema como en el uso de los medios extraíbles. No solamente es importante la protección de un equipo contra ataques offline, sino también la de los dispositivos móviles frente al robo o la pérdida accidental de los mismos.

Estas tecnologías son solamente la punta del iceberg de diferentes elementos que con respecto a la seguridad se han ido incluyendo y provocando la evolución de los sistemas y servicios en productos de factoría Microsoft. Estas nuevas tecnologías se encuentran activas de forma predeterminada, ayudando a que la seguridad por defecto sea una realidad.

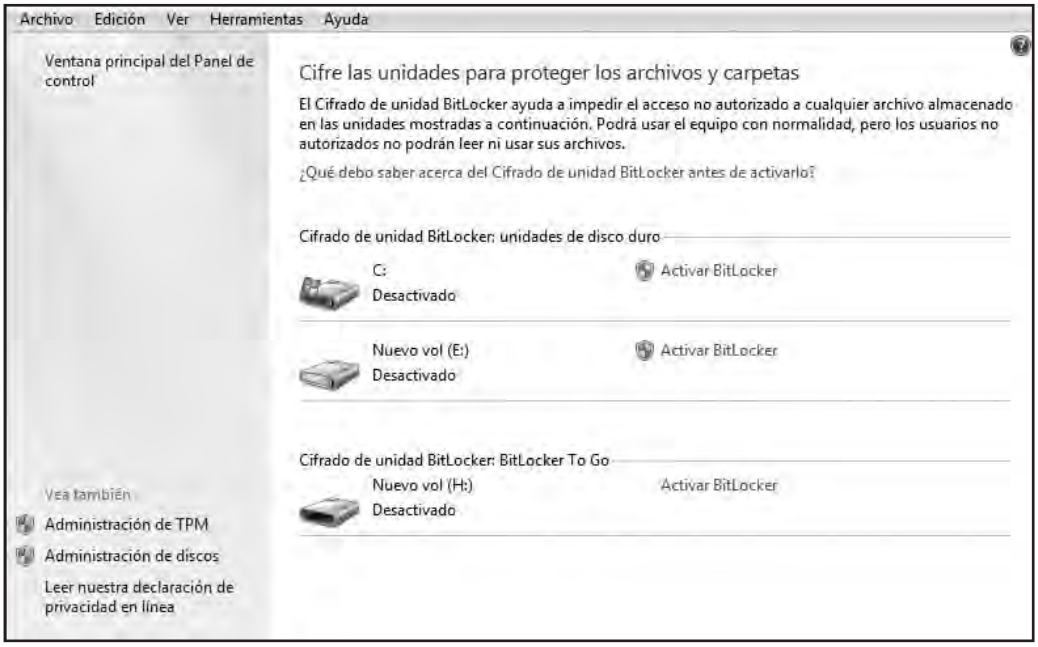


Figura 3.4. Implementación de Bitlocker y Bitlocker to go en Windows 7.

4

Dimensiones de seguridad

Para el cumplimiento de los objetivos previstos en el Real Decreto 3/2010, se definen y valoran los fundamentos que permiten categorizar un sistema. Cuando se intenta proporcionar seguridad, se debe valorar el impacto que tendría un incidente que afectara a los datos o servicios que se están proporcionando. Para ello se establece la repercusión en la capacidad organizativa para diversos aspectos:

- **Alcanzar sus objetivos**. La prestación de un servicio al ciudadano constituye el fin último de toda Administración Pública. La seguridad en el Esquema Nacional de Seguridad (ENS) plantea como necesidad que se cubran los objetivos para los que fue creado un determinado servicio.
- **Proteger los activos a su cargo**. El planteamiento de un servicio tiene como premisa el facultar el acceso o proporcionar datos a los ciudadanos en función de sus necesidades para el desarrollo de un procedimiento administrativo. Esta información se corresponde con uno de los mayores bienes con los que cuenta un usuario del servicio, obtener un papel para un procedimiento administrativo posterior o almacenar información en una base de datos. Proteger la información y todo lo que le rodea y lo hace factible se encuentra cubierto por el ENS.
- **Cumplir sus obligaciones diarias de servicio**. Relacionado con los anteriores puntos, los sistemas deben encontrarse activos y cumplir la función para los que fueron originalmente diseñados. Para ello se esperan que los servicios lleven a efecto una serie de acciones diarias y que éstas cumplan con los objetivos previstos.
- **Respetar la legalidad vigente**. Partiendo de una ley, la prestación de un servicio por parte de la Administración Pública no podría exigir otra cosa que no sea el respeto a todas las normas vigentes. Si se proporcionan datos de carácter personal de forma inadecuada y no controlada, se estaría en

contra de lo exigido por la Ley Orgánica de Protección de Datos de Carácter Personal. Por tanto, se persigue con el ENS que una potencial incidencia de seguridad no conlleve a que el servicio no cumpla con la legalidad vigente.

- **Respetar los derechos de las personas**. No debe olvidarse que en todo momento existen una serie de garantías y derechos para la protección del ciudadano que deben ser observados de forma prioritaria. En el caso de que datos críticos, como pueden ser los referidos a la salud, se hiciesen públicos se estaría rompiendo con uno de los principios fundamentales regulados en la Constitución.

Por tanto, estos elementos definirán en qué medida se cumplirán o no las atribuciones de cada Administración Pública. Si por una amenaza o un descuido no se atendieran a estas necesidades, se estarían vulnerando los derechos de los ciudadanos.

Atendiendo a la importancia de esa capacidad organizativa de la Administración Pública correspondiente, se define la figura de las dimensiones de seguridad. Estas diferencian y determinan el tipo de impacto que una amenaza podría efectuar sobre un servicio. Las dimensiones definen figuras ampliamente utilizadas en el ámbito de la seguridad y serán reconocidas a lo largo de todo el Esquema Nacional de Seguridad por sus iniciales:

- Disponibilidad [D].
- Autenticidad [A].
- Integridad [I].
- Confidencialidad [C].
- Trazabilidad [T].

Cada dimensión exigirá de la aplicación de una serie de medidas. Evidentemente, no todas ellas deberán ser puestas en marcha sobre todos los sistemas en producción. Es posible que atendiendo a la criticidad del servicio se deban disponer unas u otras. Posteriormente se tratará la metodología para determinar la criticidad de los servicios prestados.

4.1. Disponibilidad

Dentro de las medidas previstas en el ENS, la capacidad para garantizar la continuidad de un servicio es tratada especialmente. Muchas de las medidas no se encuentran íntimamente relacionadas con aspectos técnicos de la seguridad. Sin embargo, la disponibilidad es uno de los pilares básicos para la prestación del servicio. Si no hay servicio, no se cumple el objetivo estipulado para la Administración Pública.

¿Qué pasaría si en el momento álgido de la campaña sobre el Impuesto de la Renta, la prestación del programa PADRE no fuera factible durante días por problemas de suministro de energía? Evidentemente, se plantea un caso extremo, pero problemas de

energía, inundaciones y otro tipo de incidentes mayores son evaluados para resolver en todo momento la necesidad de disponibilidad.

Cualquier contingencia que no permita la prestación del servicio deberá ser evaluada para valorar alternativas. Dentro de éstas, el Esquema Nacional de Seguridad contempla:

- Dimensionamiento.
- Usos de medios alternativos.
- Energía eléctrica.
- Protección frente a incendios.
- Protección frente a inundaciones.
- Instalaciones o personal alternativos.
- Copias de seguridad.

Son tan dispares en su naturaleza, que aunque algunas, como la copia de seguridad, son de índole técnico, otras deben prever situaciones problemáticas derivadas de posibles catástrofes.

Uno de los problemas derivados del atentado del 11-S contra las Torres Gemelas fue que numerosas empresas afectadas no tenían previstos planes de continuidad y todos sus sistemas, servicios y datos se encontraban en las mismas ubicaciones. La caída de los edificios trajo consigo que los servicios no se pudieran dar de forma alternativa puesto que no estaba previsto.

Desafortunadamente, un error bastante común en la puesta en marcha de un servicio es la falta de previsión y dimensionamiento para su correcta prestación. Si se espera un determinado número de accesos concurrentes y no se proporciona la infraestructura de hardware acorde a ello, se podría producir una posible caída del servicio o bien que éste no se preste de la forma adecuada. Si el acceso a una página web tarda minutos en realizarse, el usuario no completará las acciones que tenía previstas y, por tanto, no se habrá cubierto el objetivo fundamental del servicio. Para ello se exige, a través de las medidas, un estudio previo para calibrar:

- Necesidades de procesamiento.
- Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
- Necesidades de comunicación.
- Necesidades de personal: cantidad y cualificación profesional.
- Necesidades de instalaciones y medios auxiliares.

Disponer de diferentes proveedores para la conectividad a Internet, disponer de sistemas de alimentación ininterrumpida o de diferentes proveedores eléctricos son

acciones que deben ser tenidas en cuenta bajo determinadas circunstancias. Los locales donde se ubiquen los sistemas y datos deben contar con mecanismos que prevengan contra incendios siguiendo las normativas industriales pertinentes. También deberán disponer de sistemas que prevengan contra incidentes intencionados o fortuitos causados por el agua.

El uso de locales alternativos para poder trabajar en caso de una contingencia no prevista, que inhabilite las instalaciones habituales, deberá ser tenido en cuenta en los niveles más críticos de prestación de servicios. También en la misma línea se incluye la necesidad de disponer de personal alternativo para dar continuidad a las funcionalidades en caso de indisponibilidad del personal habitual. En ambas circunstancias se deberán garantizar las condiciones de seguridad tal y como se establecían de forma convencional.

4.2. Autenticidad

Dentro de la gestión o el uso de un sistema informático, el primer elemento visible lo constituye el de la autenticidad. Cuando se accede a un equipo o a un servicio web la autenticación constituye la primera prioridad. Este proceso ofrece una serie de garantías en la prestación del servicio:

- Garantiza la personalidad de quien está realizando el acceso.
- Permite la protección de la información que en custodia guarda la entidad.
- Impide accesos no autorizados según lo establecido en las políticas de seguridad.

La autenticación debe verse siempre como una garantía de protección y no como una incomodidad. El sistema más común de autenticación es facilitar credenciales a través de contraseña. El uso de éstas es una garantía a pesar de no ser siempre bien aceptado por el usuario. Si alguien accediera a las credenciales de otro, podría suplantar su personalidad con facilidad y posibles consecuencias muy negativas.

Pero precisamente es la autenticación la que permite también depurar acciones; que éstas puedan ser trazadas y se diriman las responsabilidades correspondientes cuando sea necesario. Cuando se solicita una contraseña compleja, que tenga una longitud mínima o que deba ser cambiada cada cierto tiempo, el objetivo no es otro que mejorar el nivel de seguridad. Se hace para garantizar que ésta sea segura, que nadie más que el que la ha asignado la conozca y que solamente él la puede utilizar.

Sin embargo, no todo se reduce a credenciales basadas en contraseñas. Así lo hace ver el Esquema Nacional de Seguridad, que permite el uso de sistemas alternativos tales como la biometría o las tarjetas inteligentes, como es el propio DNIe. Promueve su uso frente a las primeras y bajo determinadas condiciones desaconsejan e incluso prohíben el uso de contraseñas. Pero no toda la autenticación se reduce a la gestión de las credenciales. También existen otros factores que intervienen en el proceso. Las siguientes medidas están relacionadas con el factor de autenticación:

- Identificación.
- Requisitos de acceso.
- Segregación de funciones.
- Proceso de gestión de derechos de acceso.
- Mecanismos de autenticación.
- Acceso local.
- Acceso remoto.
- Bloqueo del puesto de trabajo.
- Protección de la autenticidad y la integridad.
- Firma electrónica.

Se dan también una serie de acciones, eminentemente técnicas, enfocadas a la creación de procedimientos. La segregación de roles o los procedimientos para dar de baja a usuarios que ya no trabajen en la organización son algunos ejemplos. La autenticación permite su cumplimiento. Los procedimientos para que puedan ser llevados a cabo deberán estar documentados para que todo el que se relaciona con la acción sepa cómo actuar.

4.3. Integridad

Asumir que algo es por lo que dice ser, se debe considerar un error. En informática todo el mundo es consciente que los datos y los sistemas pueden alterarse de forma accidental, pero también intencionadamente. Las técnicas basadas en la suplantación son un hecho y son ampliamente utilizadas, bien haciendo uso de la ingeniería social, bien desplegando ataques más o menos complejos técnicamente que tienen como objetivo hacer creer cosas que no son.

La integridad tal y como se entiende, afecta a muchos aspectos, tanto técnicos como organizativos. Garantizar la validez de un documento, el tránsito de datos por la red o las acciones humanas son algunos de los escenarios donde intervendrán las medidas relacionadas con la Integridad. Estas deberán evitar hechos potencialmente maliciosos mediante el uso de sistemas de evaluación de la integridad.

Las técnicas de ingeniería social permiten a un atacante que pueda suplantar telefónicamente a otra persona. De este modo, poniéndose en contacto con el departamento técnico correspondiente podría solicitar el cambio de la contraseña del usuario suplantado. Aunque pueda no parecerlo, es una estrategia ampliamente utilizada para acciones de suplantación. Las auditorías realizadas en las empresas, revelan desgraciadamente que no disponen de procedimientos para solucionar estos casos. A menudo, la buena fe o la pericia del técnico que recoge la llamada marca la diferencia de la acción a realizar.

¿Qué ocurriría si alguien es capaz de alterar un documento oficial y nadie es consciente de este hecho? Los procedimientos administrativos, y de forma más acusada en el caso de uso de las tecnologías informáticas, requieren de mecanismos que den veracidad a los hechos y que impidan, en la medida de lo posible, que una alteración los invalide.

Aunque los procedimientos de integridad y autenticación consignan acciones diferentes, a menudo son comunes sus propósitos. Aunque empleen medidas específicas en cada caso persiguen un objetivo común. En el caso definido anteriormente para la asignación de una contraseña nueva a quien lo solicite, el fin último es garantizar el acceso, pero el medio debe ser la confianza en el procedimiento de asignación.

Las medidas definidas para determinar la dimensión de la integridad son:

- Requisitos de acceso.
- Segregación de funciones.
- Proceso de gestión de derechos de acceso.
- Mecanismos de autenticación.
- Acceso local.
- Acceso remoto.
- Protección de la autenticidad y la integridad.
- Firma electrónica.
- Criptografía.

4.4. Confidencialidad

Se entiende por confidencialidad los procedimientos que impedirán la obtención de datos por parte de un potencial atacante, bien porque se encuentren cifrados o bien porque hayan sido eliminados correctamente. Se suele identificar la confidencialidad con el cifrado, pero el primer concepto va mucho más allá de la mera aplicación de una tecnología específica.

Son diversos los ejemplos posibles: cuando un documento presenta metadatos que permitan que un potencial atacante extraiga información de la estructura de la organización, cuando se desecha material y éste no ha sido tratado adecuadamente, cuando existe una fuga de información propiciada porque personal interno está revelando, a menudo inconscientemente, información privilegiada en una red social, y un largo etcétera de otros escenarios posibles.

La confidencialidad constituye en ocasiones la última de las barreras de protección que se proporcionan para garantizar la seguridad de un sistema frente a un ataque. Si alguien ha conseguido robar un dato en tránsito, un disco extraíble o situarse en mitad

de un proceso de autenticación, el cifrado de la información preservará finalmente el sistema. La confidencialidad suele plantearse como un mecanismo adicional a otros procedimientos.

A menudo un proceso mezcla los procedimientos de confidencialidad con los de integridad. El caso más claro lo proporcionan los mecanismos de autenticación. Se utilizan algoritmos que permitan el cifrado derivado de la contraseña proporcionada y a su vez se utilizan firmas para garantizar la integridad.

Los sistemas de confidencialidad son tan comunes en su uso que a veces se consideran inherentes a la informática: por ejemplo, el uso de protocolos seguros como HTTPS en los procesos de autenticación para garantizar el cifrado de la contraseña. Sin embargo, no siempre es así. A veces se utilizan protocolos menos seguros como HTTP y sobre ellos procesos de autenticación donde las credenciales viajan en texto plano, o bien las contraseñas de acceso a un sistema web se almacenan en claro en la tabla de una base de datos. Estos procesos son los que se pretenden erradicar con el Esquema Nacional de Seguridad. Evitar un potencial ataque a veces puede resultar imposible, por lo que las garantías de cifrado deben permitir que se confíe en la seguridad del procedimiento.

En el Esquema Nacional de Seguridad, la confidencialidad se entiende en muchos de los escenarios habitualmente utilizados por las diferentes Administraciones Públicas:

- **Prestación de servicios web**. Los datos que manejan los ciudadanos y que circulan a través de Internet deberán estar cifrados para garantizar su confidencialidad.
- **Comunicaciones internas de la organización**. Bien a través de redes Wi-Fi o dentro de la red cuando no se puedan consignar otras medidas, los datos deberán estar asegurados entre los extremos de la comunicación.
- **Comunicaciones externas de la organización**. La seguridad deberá prestarse en usos tales como el acceso a través de VPN (Redes Virtuales Privadas) o en el intercambio de correos electrónicos.
- **En los procesos informáticos**. Mecanismos como los de autenticación o creación de copias de seguridad deberán contar con tecnologías que garanticen su confidencialidad.
- **En el uso de sistemas informáticos**. Las unidades locales o externas y los soportes que salgan fuera de la organización deberán contar en función de su uso y objetivo con tecnologías para su cifrado.

Los sistemas de cifrado que pueden emplearse son múltiples, pero también hay que tener en cuenta que algunos de ellos no son tan fiables como se espera. Deberían utilizarse exclusivamente aquellos que sean más seguros y minimizar el uso de los que no lo sean. Por ejemplo, para el almacenamiento de los hashes derivados de contraseñas que en los sistemas Microsoft se realiza localmente, debería evitarse el uso

de LM (*LAN Manager*), frente al más seguro y moderno NTLM (*New Technology LAN Manager*). De igual modo, frente a un protocolo de túnel para VPN como PPTP (*Point to Point Tunneling Protocol*), debería emplearse uno más eficiente y seguro como SSTP (*Secure Socket Tunneling Protocol*). A través del análisis y la formación, los administradores deberían saber cuáles son las tecnologías más eficientes para el cumplimiento de medidas previstas en el ENS. Con respecto a la confidencialidad, estas son las fundamentales:

- Requisitos de acceso.
- Segregación de funciones.
- Proceso de gestión de derechos de acceso.
- Mecanismos de autenticación.
- Acceso local.
- Acceso remoto.
- Etiquetado.
- Criptografía.
- Borrado y destrucción.
- Limpieza de documentos.

4.5. Trazabilidad

Se trata de la última dimensión de seguridad y es la más compleja de gestionar y, a menudo, no se le da el valor que le corresponde. Se asume que si un sistema es seguro por defecto, nada puede fallar y, por tanto, no se producirán ataques efectivos. Sin embargo, es evidente que esto no es así. Cualquier sistema es susceptible de fallo. Por nuevos descubrimientos o por errores humanos los problemas a la larga ocurrirán, siendo entonces necesario su descubrimiento.

Un ataque que ha resultado efectivo, a menudo sólo es descubierto por casualidad o porque los sistemas de registro han funcionado correctamente. La realización de peritajes forenses requiere para su validez de sistemas efectivos de trazabilidad. Sin ellos, muchas veces las evidencias y conclusiones quedarán inconexas.

Es cierto que habitualmente la puesta en marcha de los servicios de registro requiere de múltiples esfuerzos administrativos, económicos y temporales. Sin embargo, son la única garantía para saber qué ha podido suceder en una determinada situación. ¿Cómo identificar quién ha eliminado una tabla de una base de datos? Sin un sistema de registros sería imposible. O si se ha utilizado determinada técnica de SQL Injection sobre un portal web, no podría ser advertido si la acción no hubiera quedado registrada.

La trazabilidad es necesaria, pero requiere de elementos de consolidación y correlación para que su gestión pueda ser eficiente. Si no se pueden manejar adecuadamente

los datos, éstos son inútiles. En múltiples ocasiones, para obtener conclusiones válidas es necesario su estudio exhaustivo. A veces sólo se depuran convenientemente cuando ha sido necesario utilizarlos tras haber sufrido una incidencia.

El Esquema Nacional de Seguridad valora la trazabilidad técnicamente, pero también organizativamente. Es importante tener los datos, consolidarlos y tratarlos apropiadamente. Pero también es importante que se segreguen las funciones. Quien analice la información debe ser una persona diferente a la que la ha originado. Además, su almacenamiento debe ser seguro y los factores de disponibilidad han de ser tenidos en cuenta.

Se valora su uso desde dos posibles tipos de acciones: reactivas y preventivas. Preventivas, en análisis periódicos que permitan determinar si las acciones rutinarias siguen los procedimientos marcados en la política de seguridad. Así como que ésta es realmente efectiva, siendo a veces necesario ajustarla por detalles descubiertos a través de las trazas. Pero también deberán ser reactivas, utilizándose cuando se conozca la existencia de una incidencia para que pueda ser subsanada. Si se ha producido un ataque contra un portal web, deberá conocerse el método que se ha empleado contra él. Si los registros del servidor están activos, posiblemente quedarán en ellos definidos los métodos utilizados para el ataque.

La trazabilidad se presenta en la aplicación de las siguientes medidas:

- Identificación.
- Requisitos de acceso.
- Segregación de funciones.
- Proceso de gestión de derechos de acceso.
- Mecanismos de autenticación.
- Acceso local.
- Acceso remoto.
- Registro de la actividad de los usuarios.
- Protección de los registros de actividad.
- Sellos de tiempo.

4.6. Niveles de la dimensión de seguridad

El conjunto de un servicio prestado por una Administración Pública lo configuran diferentes elementos sujetos a dimensiones de seguridad. Cada una de ellas se adscribirá a diferentes niveles en función de su criticidad y, en consecuencia, se aplicarán las diferentes medidas previstas en el Esquema Nacional de Seguridad. Si una determinada dimensión no se aplicara sobre un servicio, las medidas asociadas tampoco deberán aplicarse.

No es lo mismo un servicio web en el que se preste únicamente información pública, indicativa y estática de cómo se realizan determinados procedimientos administrativos, a si este sistema autenticara previamente, y en función de quién fuera el usuario se prestarán unos u otros servicios. En el segundo caso, mucho más complejo, intervendría como dimensión de seguridad la autenticación, integridad, confidencialidad y trazabilidad que no serían preceptivas en el primero.

Se dará la tendencia a equipar el ENS con la LOPD, pero aunque en la aplicación de medidas pueden ser coincidentes, la categorización de los servicios es muy diferente. La criticidad en la LOPD se mide atendiendo a la naturaleza de los datos personales afectados. En el caso del ENS se valora en función del perjuicio que afecte a las dimensiones de seguridad sobre las funciones de la organización, sus activos o los individuos afectados.

Atendiendo a esa criticidad estos son los tres niveles existentes:

a) **Nivel BAJO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

   Se entenderá por perjuicio limitado:

   1º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.

   2º El sufrimiento de un daño menor por los activos de la organización.

   3º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

   4º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.

   5º Otros de naturaleza análoga.

b) **Nivel MEDIO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

   Se entenderá por perjuicio grave:

   1º La reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.

   2º El sufrimiento de un daño significativo por los activos de la organización.

   3º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

4º Causar un perjuicio significativo a algún individuo, de difícil reparación.

5º Otros de naturaleza análoga.

c) **Nivel ALTO**. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

2º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

3º El incumplimiento grave de alguna ley o regulación.

4º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5º Otros de naturaleza análoga.

Atendiendo a esta naturaleza, si una organización presta un único servicio indispensable para los ciudadanos y éste es de tipo informático exclusivamente, sus dimensiones de seguridad se identificarían como de nivel alto. Esto es debido a que si se produce un incidente que anule su capacidad para prestar el servicio, no habría mecanismo alternativo para que éste siguiera operativo.

Evidentemente cada escenario presentará su particularidad y a veces será complicado valorar la criticidad de un determinado servicio. El CCN está desarrollando, en base a sus atribuciones, unas guías aclaratorias y de uso para definir entre otros aspectos las medidas y los mecanismos que deben seguir las organizaciones para medir el nivel de sus dimensiones de seguridad. La Guía 803, aún en borrador, versará sobre la valoración de sistemas en el Esquema Nacional de Seguridad

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel general del sistema será aquel en el que cada dimensión sea la mayor de las declaradas. Por ello se establece:

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

Para una mejor gestión y evitar esfuerzos innecesarios en la aplicación de medidas, los servicios se podrán segregar cuando sea posible. Se atenderá para ello la naturaleza de las dimensiones de seguridad que se den en cada caso.

5

Medidas de seguridad. Naturaleza de las medidas

El objetivo final que presentan las dimensiones de seguridad lo constituye la posibilidad de que un sistema puede ser categorizado en los niveles vistos anteriormente: bajo, medio o alto. Sin embargo, a través de ellas también se proporciona el mecanismo para la segregación de acciones que con respecto a un sistema se pudieran establecer. La evaluación de un servicio permitirá conocer las dimensiones de seguridad que le pueden afectar. Anteriormente ya se expuso un ejemplo sobre un portal de autenticación para el ciudadano. Este hecho es bastante crítico, porque la aplicación de medidas vendrá definida y dependerá precisamente del tipo de dimensiones que se vean afectadas.

En la mayor parte de las circunstancias las dimensiones de seguridad vendrán marcadas por la esencia del servicio. En otras, sin embargo, se necesitará un estudio más en profundidad para determinar si éste se ve o no afectado por una determinada dimensión de seguridad. En esta última circunstancia será a veces el conocimiento del tipo de medidas a aplicar el que podría marcar las pautas a seguir. Por ejemplo, se podría pensar que un servicio web de presentación de noticias no debe disponer de un sistema de autenticación, al menos visible. Sin embargo, éste sí debería darse para que el servicio accediera a una base de datos donde se encuentra la información a proporcionar. Si la cadena de conexión, credenciales incluidas, se encuentra inmersa en el mismo código y la base de datos almacena además otras tablas con datos de carácter personal, se infringiría la norma si no se aplicaran las medidas de autenticación estipuladas. Algo que parecía no ser necesario por el tipo de servicio, se convierte sin embargo en una obligatoriedad.

La categorización del sistema y la evaluación de las dimensiones servirán finalmente para conocer las medidas de seguridad que se deben disponer. Estas, para una mejor visión de las mismas, se han segmentado en lo que se conoce como la naturaleza de las medidas. Se intenta de una u otra forma agruparlas atendiendo a criterios de aplicación y usos comunes. Para ello se han dividido en tres categorías.

- Las medidas de marco organizativo.
- Las medidas de marco operacional.
- Las medidas de protección.

Las dos últimas a su vez se han dimensionado en subcategorías que bajo un mismo epígrafe determinan en qué modo un servicio podrá ser afectado. Por ejemplo, en la categoría del marco operacional se define una serie de medidas bajo la subcategoría servicios externos. Su epígrafe define qué tipo de servicio se verá afectado por la aplicación de las medidas.

Cuando se definen las dimensiones de seguridad, se piensa inicialmente en figuras de índole informático que tienen que ver con la seguridad. Sin embargo, el Esquema Nacional de Seguridad también tiene en cuenta otro tipo de medidas que siendo genéricas no se circunscriben a un tipo concreto de dimensión. Estas se reconocen porque en la información de dimensión afectada en vez de D, A, I, C o T (las siglas de las dimensiones), figuran con la leyenda "categoría". Definen medidas que afectarán a todos los servicios de forma independiente a las dimensiones de seguridad declaradas y suelen ser de naturaleza organizativa o estructural.

Para entender mejor la naturaleza de las medidas y su relación con las dimensiones de seguridad, en la Figura 5.1 se expone una imagen sobre las mismas, ofreciéndose una explicación de sus convenciones.

				op	Marco operacional
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)

Figura 5.1. Medidas de marco operacional.

La imagen muestra algunas de las medidas relacionadas con el marco operacional y subcategorías de planificación y control de acceso. La tabla presenta una serie de columnas donde los códigos de colores establecen criterios de aplicación de medidas en función de su criticidad.

La primera de las columnas hace referencia al tipo de dimensión de seguridad que se verá afectado por la medida. Tal y como se definió anteriormente, se reconocen por las iniciales correspondientes a cada una de ellas. En aquellas circunstancias en las que aparezca la palabra categoría en vez de alguna de las iniciales de la dimensión de seguridad, se indica que afecta a cualquier servicio independientemente de su naturaleza.

Por ejemplo, en la medida de inventario de activos correspondiente a explotación, se aplica realmente a todos los servicios y no se relacionan con ningún tipo de dimensión. Este tipo genérico suele corresponder principalmente a medidas de índole organizativo frente a las más técnicas que sí se encontrarán habitualmente asociadas a un tipo de dimensión concreta.

Las diferentes medidas pueden verse afectadas por más de una dimensión de seguridad, como en el caso del acceso local, donde intervienen las de autenticación, integridad, confidencialidad y trazabilidad. En otros casos la medida solamente se verá afectada por una dimensión, como es el caso del dimensionamiento y gestión de capacidades que se ve asociado exclusivamente a la disponibilidad.

Las tres siguientes columnas definen la necesidad de su aplicación atendiendo a la categorización realizada sobre el servicio: básica, media o alta. La primera columna referencia si se aplicará a sistemas catalogados como básicos, la segunda a medios y la tercera a altos. Los colores informan respecto de si las medidas a aplicar son más severas que las que deberían observarse para la de categoría inferior. Para ello se establecen por simbología las siguientes indicaciones.

- **Aplica**. Identifica que esa medida es de aplicación a partir del nivel para el que se establezca. En la imagen, la gestión de la configuración se aplica a partir del nivel medio, mientras que la identificación lo hace desde el básico.
- El **símbolo '='**. Implica que las medidas previstas para el nivel son iguales que las aplicadas en niveles inferiores. Por ejemplo, las medidas previstas para identificación se aplicarán igualmente independientemente del tipo de nivel de criticidad que haya sido asignado. En el caso de acceso remoto las medidas para el nivel medio se aplican en la misma medida en el nivel alto.
- El **símbolo '+'** referencia aquellas medidas que aplicables en el nivel medio son más estrictas en contenido que las que se aplican en el nivel inferior.
- El **símbolo '++'** referencia aquellas medidas que aplicables en nivel alto son más estrictas que las que se aplican en los dos niveles inferiores. Existe un ejemplo en la imagen de los dos últimos símbolos asociada al análisis de riesgos.

- Las **siglas 'n.a.'** significan no aplicable. Expresa que las medidas de seguridad para ese control no se aplicarán en función del nivel que se haya definido. En la imagen, los componentes de certificados solamente serán aplicados cuando se haya categorizado un sistema como de nivel alto.

Entender estos conceptos, conociendo las dimensiones del servicio y la categorización del mismo, permite establecer de forma inicial en qué medida se verá afectado por la seguridad marcada en el ENS. Para cada medida se especifican diferentes controles. El Capítulo 6 de esta publicación versará completamente sobre cómo aplicar las medidas de índole técnico. Otras consideradas organizativas o estructurales se citarán y analizarán a continuación.

5.1. Marco organizativo

Bajo este epígrafe se reúnen aquellas medidas genéricas que definen los procedimientos iniciales a tenerse en cuenta para la gestión de la seguridad. Como indica la palabra organizativo, las medidas aquí planteadas son de carácter no técnico y observan aquellos aspectos de gestión afectados por el ENS.

Fruto de estas acciones surgirán documentos tales como las políticas y normativas de seguridad, junto a los procedimientos básicos de seguridad y de autorización de tareas, para los diferentes servicios que plantea la organización. Cuatro son las subcategorías en las que se divide el marco organizativo:

- Política de seguridad.
- Normativa de seguridad.
- Procedimientos de seguridad.
- Proceso de autorización.

Como es obvio, la aplicación del resto de medidas se basará en los resultados obtenidos tras la implantación de estas medidas organizativas. Algunas, como la correspondiente a la política de seguridad, no deberán ser definidas por la propia entidad administrativa, sino como ya se ha indicado, por el órgano superior correspondiente. La política marcará la norma en cuanto a la seguridad y los diferentes procedimientos que deberán ser llevados a cabo para que la seguridad sea eficiente.

La política de seguridad se concretará en un documento que deberá contener los siguientes elementos:

- **Los objetivos o misión de la organización**. Al marcar sus funciones, se estarán definiendo las obligaciones y con ello las responsabilidades y el alcance para el cumplimiento de objetivos. Será la base fundamental para poder establecer la categorización de niveles en básico, medio o alto.
- **El marco legal y regulatorio en el que se desarrollarán las actividades**. Las acciones de una determinada Administración Pública se verán afectadas además de por la Ley 11 / 2007, por otras tales como la LOPD. Por ello deberá

tenerse en cuenta la necesidad de aplicar medidas que atiendan a todas las normas existentes.

- **Los roles o funciones de seguridad**, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación. Páginas anteriores definieron los diferentes roles que con respecto al ENS deberán existir en una organización. La política definirá quién o en qué condiciones se asumirá cada rol.
- **La estructura del comité o los comités para la gestión y coordinación de la seguridad**, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización. La aplicación de determinadas condiciones, como la adquisición de un determinado software, podrían ser consensuadas a través de un comité. La política dirimirá su proceso de creación, así como las funciones del mismo.
- **Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso**. La política sienta las bases para el establecimiento de las medidas organizativas asociadas a la seguridad del sistema.

Para un uso seguro de los sistemas se estipula la necesidad de crear una serie de documentos que establezcan diferentes normas de actuación. Difícilmente se puede exigir a alguien que cumpla con unas normas si no tiene claro cómo hacerlo. Los documentos que se consignan a través de las normativas de seguridad permitirán clarificar los usos y delimitar las responsabilidades en caso de actuación incorrecta. Para ello, los documentos de seguridad deberán expresar lo siguiente:

- El uso correcto de equipos, servicios e instalaciones.
- El establecimiento de lo que se considerará uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Estos documentos permitirán que todos los integrantes de los servicios de la Administración conozcan cómo afrontar los principios de seguridad. Su incumplimiento llevará a cabo un procedimiento sancionador regulado a través del régimen disciplinario del personal que presta servicios en las administraciones públicas.

Relacionados con las normas de seguridad están íntimamente ligados los procedimientos de seguridad. Estos marcarán las tareas que se deberán llevar a cabo con respecto a la misma. Cómo establecer el cambio de contraseña o cómo actuar en caso de que no se pueda iniciar una sesión, son algunos de los procedimientos que deberán estar documentados. Los documentos deberán detallar:

- Cómo llevar a cabo las tareas habituales.
- Quién debe realizar cada tarea.
- Cómo identificar y reportar comportamientos anómalos.

Quizá el componente más complejo sea identificar y reportar las anomalías que con respecto a la seguridad puedan identificarse. En ocasiones es incluso complicado para un especialista de seguridad. Pero a veces acciones lógicas, como reportar el robo de un disco que contiene información critica, no se realiza porque se desconoce el procedimiento para ello o bien se hace a través de cauces no reglamentarios.

Los procedimientos son la base de la seguridad. Muchas organizaciones esperan a tener los sistemas en marcha para después procedimentarlos. Esto constituye normalmente un error de base, porque los procedimientos se ciñen así a los sistemas planteados, partiendo en ocasiones de malas prácticas iniciales. Planificando inicialmente los procedimientos, se consiguen mejores resultados finales. Un caso paralelo sería el desarrollo de un software, donde primero se genera el código y finalmente se realiza el análisis funcional.

El último de los elementos del marco organizativo lo constituye el de los procedimientos de autorización. En lo referente a la seguridad se espera una rectitud que exige de procesos jerarquizados. Cuando a alguien se le asigna un rol, se espera de él el cumplimiento de unos objetivos por las capacidades que ha demostrado. Podrá delegar el cumplimiento de las tareas en alguien que considere que se encuentre preparado para ello. Sin embargo, esto no le exime de su responsabilidad en caso de que las tareas no se realicen adecuadamente.

La seguridad presenta como base una estructura fuertemente jerarquizada, donde cada uno representa una función que lleva implícita una serie de responsabilidades. Por ejemplo, nadie debería introducir en los sistemas un punto de acceso inalámbrico sin el debido conocimiento expreso y la autorización correspondiente de la persona responsable de este hecho. Es muy posible que la persona que desea la conexión Wi-Fi desconozca las implicaciones de seguridad que tiene su acción. El ENS recoge también estas circunstancias y requiere que existan procedimientos de autorización en los siguientes casos:

- Utilización de instalaciones, habituales y alternativas.
- Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- Entrada de aplicaciones en producción.
- Establecimiento de enlaces de comunicaciones con otros sistemas.
- Utilización de medios de comunicación, habituales y alternativos.
- Utilización de soportes de información.
- Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDAs u otros de naturaleza análoga.

5.2. Marco operacional

Las medidas de tipo operacional se constituyen para proteger la operativa del sistema desde un punto de vista global, así como de sus componentes individualmente.

La naturaleza de las medidas es de diferente índole y han sido estructuradas en las siguientes subcategorías:

- Planificación.
- Control de acceso.
- Explotación.
- Servicios externos.
- Continuidad del servicio.
- Monitorización del sistema.

La planificación constituye el ámbito formal organizativo para plantear las medidas técnicas y funcionales. Son la base de la seguridad y la primera de sus medidas así lo muestra: el análisis del riesgo. Este tendrá como objeto definir los activos con los que cuenta la organización y las amenazas a las que se enfrenta. De su dimensionamiento se establecerán las medidas preceptivas que tendrán que salvaguardar los activos, teniendo en cuenta para ello las amenazas que pueden llegar a darse. Su aplicación difiere en función del nivel de categoría que se haya asignado. Su elaboración será menos formal cuando el nivel sea básico y más formal y específico en sus contenidos según se incremente la criticidad de la categoría a medio o alto nivel.

La documentación de los elementos y sistemas que intervienen en la prestación de un servicio es una necesidad prioritaria que debe ser atendida. Los distintos componentes, ya sean físicos o tecnológicos, deberán encontrarse detallados para facilitar las tareas de análisis o auditoría. A veces, los sistemas planteados son tan intricados que sin tener presente una visión gráfica del diseño es imposible conocer cómo operan y se interconectan entre ellos. No es posible gestionar una organización con más de mil equipos en su infraestructura y múltiples dispositivos de red sin elementos gráficos para ello. Los tiempos y esfuerzos se reducen considerablemente cuando esta labor se encuentra realizada correctamente.

El Esquema Nacional de Seguridad exige de las organizaciones los siguientes documentos:

- Documentación de las instalaciones:
  - Áreas.
  - Puntos de acceso.
- Documentación del sistema:
  - Equipos.
  - Redes internas y conexiones al exterior.
  - Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

- Esquema de líneas de defensa:
  - Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet.
  - Cortafuegos, DMZ, etc.
  - Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.
- Sistema de identificación y autenticación de usuarios:
  - Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.
  - Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.
- Controles técnicos internos:
  - Validación de datos de entrada, de salida y datos intermedios.
- Sistema de gestión con actualización y aprobación periódica.

La planificación presenta como importante tarea la del dimensionamiento de los sistemas. Como se recogió previamente, la incapacidad para prestar un servicio por estar incorrectamente dimensionado implicaría a todos los efectos como si este no se estuviera ofreciendo. En el caso de los niveles medio y alto realizar un estudio previo de necesidades es requisito indispensable antes de que se inicie el proceso de la puesta en marcha de un servicio.

Como parte fundamental de la seguridad, la adquisición de nuevos componentes constituye una necesidad a la hora de plantear nueva medidas. Este aspecto, junto con el último elemento de la planificación, los componentes certificados, será tratado en el Capítulo 7 de este libro.

El siguiente grupo de medidas se dedican al control de acceso. Siendo eminentemente técnicas cubren el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción. Se prima la comodidad en los sistemas básicos, frente a la seguridad en aquellos catalogados como de nivel alto. Estas medidas serán recogidas en su faceta técnica en el próximo capítulo.

La explotación define todas aquellas tareas que de forma convencional una organización realiza para llevar a cabo operaciones convencionales. La preparación de los sistemas, el mantenimiento de los equipos o la instalación y la configuración de aplicaciones tales como los antivirus se clasifican como tareas de explotación. Muchas organizaciones cuentan con un departamento con este mismo nombre, encargado de la realización de estas funciones.

Algunas de las tareas que deben llevarse a cabo, tales como los inventarios, constituyen sin embargo una alta carga de trabajo. Se desconocen cuántos sistemas

o aplicaciones existen en la organización. Los servidores a veces son tantos que se ha descontrolado su número, situación que se agrava por la potencia que ofrecen las tecnologías de virtualización. Pero seguridad también es esto. Una organización no podrá estar segura si no es capaz de cuantificar sus activos. Sin un inventario de software se desconocerá la existencia de un potencial programa que de forma interna podrá constituir una brecha de seguridad. Estas tareas de explotación serán tratadas extensamente en el Capítulo 6 del libro.

Los dos siguientes grupos de medidas, servicios externos y continuidad del servicio, tienen relación directa con el funcionamiento de los sistemas. En estos grupos se incorporan medidas a partir del nivel medio, no siendo necesaria su aplicación en el básico. Ambos prescriben la necesidad de utilizar medios alternativos a los habituales y definir planes de contingencia de personal y material para dar cobertura al servicio prestado. Para ello deberá disponerse de un análisis de impacto, definiéndose en qué medida deberán aportarse recursos para dar la continuidad al servicio. La relación existente con personal externo hace extensiva la aplicación de seguridad recogida en el ENS a éste. Los planes de gestión de continuidad deberán prever que en caso de prestación de servicios externos la seguridad de los sistemas deberá ser extrema.

Las últimas medidas tienen relación con la monitorización de un sistema. Se entiende como tal no el control del servicio en sí, sino el control de la seguridad del mismo. En este sentido la implementación del sistema de prevención de intrusiones y la cuantificación de las amenazas constituyen una necesidad tal y como recoge el ENS.

5.3. Medidas de protección

El último conjunto de medidas constituyen el número más significativo de categorías. Lo conforman las medidas de protección y tienen como fundamento la salvaguarda de los activos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. Frente a las medidas operacionales, más genéricas con respecto a los servicios, estas son mucho más específicas.

Se encuentran diferenciadas en las siguientes categorías:

- Protección de las instalaciones e infraestructuras.
- Gestión de personal.
- Protección de los equipos.
- Protección de las comunicaciones.
- Protección de los soportes de comunicación.
- Protección de las aplicaciones informáticas.
- Protección de la información.
- Protección de los servicios.

Aglutinan por igual medidas de índole técnico como de tipo estructural, cubriendo un amplio abanico de aspectos relacionados con la seguridad que van desde la gestión de agresiones de índole física como el fuego o las inundaciones, a otras de factura más tecnológica como los sistemas de criptografía para medios extraíbles. El nexo común es ese factor definido anteriormente de la protección de activos concretos, frente a las medidas de aplicación de ámbito más general.

Las medidas de protección de instalaciones e infraestructuras tienen como objetivo el prevenir incidencias estructurales marcando las bases para la realización de las tareas en unos espacios acondicionados adecuadamente. Si encima de los servidores o en el centro de comunicaciones existen tuberías, debe tenerse en cuenta que será algo previsible que el paso del tiempo aumentará el riesgo de que éstas se dañen afectando a los sistemas. Deberá buscarse una ubicación para los servidores y los sistemas de comunicaciones donde esta incidencia no pueda darse. Si un edificio es proclive por su orografía a sufrir inundaciones, no sería lógico disponer su centro de procesamiento de datos en los sótanos del mismo. Aunque parezcan cuestiones de lógica, no serán pocas las organizaciones que se encuentren en esta situación y la aparición del Esquema Nacional de Seguridad les exigirá un esfuerzo para la reorganización de sus infraestructuras.

La gestión de personal constituye una necesidad que con el ENS adquiere también otra dimensión particular. La seguridad aporta a cada persona una participación importante en la gestión de los servicios. Tan importante puede ser en un momento dado el administrador de una base de datos como la persona que simplemente introduce datos en la misma. Evidentemente, el primero tiene originalmente más responsabilidad, pero el segundo seguramente pueda extraer los datos y tratarlos inadecuadamente, por ejemple exponiéndolos a través de un sistema P2P (*Peer to Peer*).

La asignación de un rol o puesto de trabajo relacionado con la prestación de un servicio, máxime si está relacionado con la seguridad, requiere de criterios adicionales a los convencionales para su asignación. De forma natural, el análisis de riesgos con los que contará la organización será el encargado de definirlo, pero para evitar errores el ENS establece los siguientes criterios:

- Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición se basará en el análisis de riesgos.
- Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad.

  Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.
- Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

Condiciones similares se aplicarán en el caso del personal contratado a través de un tercero.

El factor humano es muy importante en términos de seguridad. Sus aciertos permiten que los sistemas sean confiables y funcionen correctamente; los errores por el contrario pueden ser críticos. Por ello, en el ENS se recoge la necesidad de promover tanto la formación para el desarrollo de las funciones como los procesos de concienciación en materia de seguridad. Todo aquel que trabaje en un sistema debería conocer, aunque fuera mínimamente, las consecuencias de sus posibles acciones. Por ejemplo, desactivar un antivirus para instalar un software que éste no permitía tiene consecuencias mucho más negativas de las que el usuario puede pensar inicialmente. Acceder a un sistema mediante HTTPS y recibir una advertencia de seguridad con respecto al certificado requiere la cualificación del empleado para entender y evaluar las consecuencias que determinarán aceptar o rechazar el mensaje que le pudiera estar advirtiendo.

Las siguientes medidas reciben el epígrafe de protección. Bien sea de un equipo local o de las comunicaciones, el objetivo es minimizar el impacto de potenciales ataques que de diversa naturaleza puedan llegar a suceder. ¿Por qué minimizar y no impedir? Porque se asume que la seguridad completa no existe y aunque hay muchas técnicas conocidas que pueden ser erradicadas aplicando las medidas adecuadas, otras requieren medios tan desproporcionados que no quedará otra opción que limitar su acción.

Sobre un sistema web se pueden plantear múltiples técnicas de ataque. *SQL Injection*, *Cross-site Scripting* (XSS), *LDAP Injection*, *Connection String Parameter Pollution* (CSPP) o *Remote File Inclusion* (RFI) son algunas de ellas. Estas podrán ser detectadas y detenidas de una u otra forma. Sin embargo, es factible que mañana aparezca una nueva técnica desconocida o que un componente del servidor presente una vulnerabilidad que sea atacada mediante un *exploit* que hasta la fecha no haya sido publicado. Evidentemente, intentar frenar todos los ataques es imposible, pero se puede minimizar el riesgo mediante medidas alternativas. Por ejemplo, al segmentar las redes se minimiza el alcance de un ataque, o diferenciando las contraseñas de los administradores locales de los diferentes servidores se propicia que si uno de ellos ha sido afectado por una amenaza, ésta no se haga extensible al resto de servicios de la organización. La aplicación de medidas de protección se recoge extensamente en el siguiente capítulo.

6

La implementación del ENS con tecnología Microsoft

La cantidad de servicios que prestan las diferentes administraciones públicas seguramente son innumerables. De diferentes tipos y con distintos objetivos, todos ellos sin embargo estarán supeditados a las normativas que en materia de seguridad establece el Esquema Nacional de Seguridad. Servidores web, bases de datos, correo electrónico, servidores de ficheros, sistemas operativos de estación de trabajo y un largo etcétera de escenarios y tecnologías implicados. Tantos que sería imposible enumerarlos a todos.

Con toda certeza serán muchos los escenarios en los que los productos Microsoft participen en algún término. A veces, las medidas de seguridad deberán aplicarse sobre ellos, como en el caso de los sistemas operativos. En otras, por el contrario, serán participantes de las medidas a implementar como en el caso de los productos MS System Center o MS Forefront. Este capítulo aportará información sobre la aplicación de éstas en escenarios con soluciones Microsoft, así como el aprovechamiento para el cumplimiento de la normativa de los distintos productos del fabricante.

A veces un producto que se emplea con un fin determinado puede sin embargo aportar funcionalidades que permitirían dar respuesta a algunas de las medidas exigidas por el Esquema Nacional de Seguridad (ENS). En la actualidad, muchas organizaciones contarán con la presencia en sus infraestructuras de MS System Center Configuration Manager 2007 R2. Aunque tradicionalmente esta solución se utiliza para la distribución de aplicaciones y el inventario de software y hardware, algunos de sus componentes se pueden utilizar para dar cobertura a los procedimientos de inventariado o mantenimiento de los sistemas que exige el ENS. La inclusión, únicamente como solución proxy, de MS ISA Server o MS Forefront Threat Management Gateway supone una falta de aprovechamiento de sus posibilidades cara al cumplimiento de lo establecido en el ENS. MS Forefront TMG 2010 presenta una plataforma nativa de sistemas de detección/prevención de intrusiones o capacidad para la eliminación de malware en los sistemas perimetrales. Estas, entre otras características, aportan grandes posibilidades cara al despliegue de medidas de seguridad.

Aunque cada punto de este capítulo tratará medidas técnicas asociadas a los diferentes marcos de aplicación en el Esquema Nacional de Seguridad, es necesario analizar inicialmente en qué medida los productos Microsoft pueden ser partícipes de procedimientos o medidas organizativas. En muchas circunstancias la gestión eficiente de la documentación relacionada con la seguridad constituye una de las primeras medidas a considerar, antes incluso de empezar a plantear un modelo determinado.

Cómo se establecerán los mecanismos de comunicación de incidencias, los procesos de solicitud de autorización o simplemente la asignación de tareas son procedimientos que deberán ser planificados cuidadosamente. Un sistema común parece la opción más interesante para que estas labores puedan efectuarse con eficacia. En este sentido y considerando experiencia probadas, las soluciones basadas en MS SharePoint ofrecen notables posibilidades para la gestión de documentos y procedimientos de control. La última versión, Microsoft SharePoint Server 2010, presenta especialmente una gran amplitud de posibilidades y funcionalidades para este tipo de tareas.

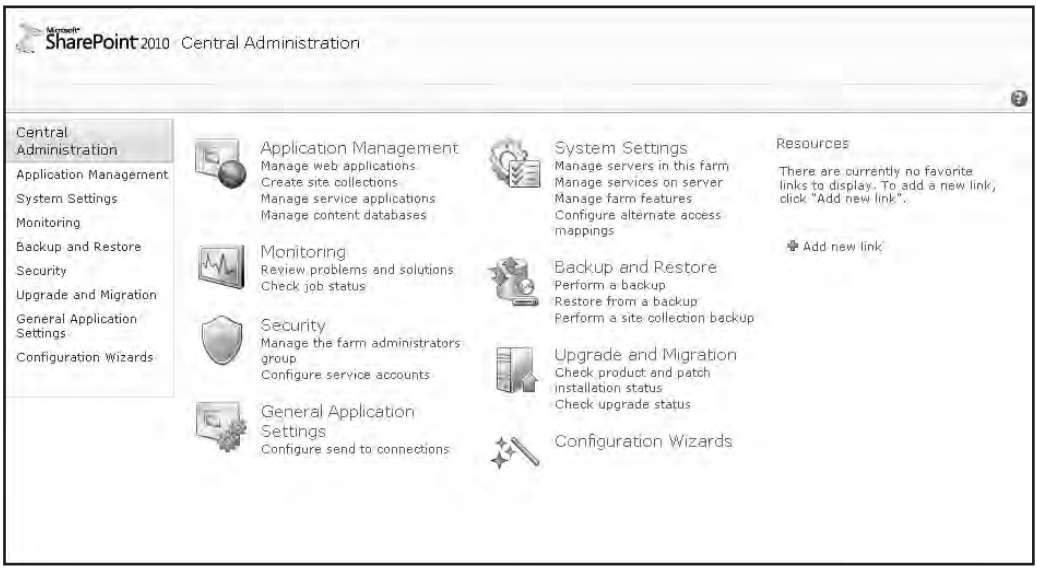


Figura 6.1. Panel de administración de Microsoft SharePoint Server 2010.

MS SharePoint Server permite aportar soluciones en situaciones como las siguientes:

- **Almacenamiento de toda la documentación con la que trabajará la Administración**, relacionada con el Esquema Nacional de Seguridad. Desde la política de seguridad, hasta los diferentes esquemas de diseño de las infraestructuras de servicios o diagramas de red, pueden ser almacenados y gestionados desde MS SharePoint.
- **Proporciona mecanismos para que lo usuarios conozcan sus funciones y obligaciones**, accedan a casos de uso y dispongan de información para

afrontar algunas tareas que dentro de sus funciones sean relativas a la seguridad. A través de Microsoft SharePoint Server 2010 pueden ofrecerse con garantías la publicación de documentos con fines formativos y el soporte documental para el desarrollo de tareas comunes o específicas en función del perfil del usuario.

- **Gestión de procedimientos a través de un sistema de flujo documental**, como pueden ser la solicitud de servicios, la gestión de autorizaciones o los procedimientos para la resolución o la comunicación de incidencias. Para ello, existen ya plantillas predefinidas que permitirán crear estrategias integradas con las cuentas de usuarios de una organización del Directorio Activo, quedando definido el flujo de datos y las condiciones para publicar o autorizar determinados procesos.

El sistema de gestión documental constituye un elemento fundamental en el tratamiento de la seguridad. Los especialistas dedican gran parte de su tiempo en documentar las distintas situaciones sobre las que actúan. Se espera también del sistema documental que ofrezca un alto nivel de seguridad, debido a la importancia y el carácter crítico de los datos que se almacenan. Desde claves para el acceso a servicios hasta toda la estructura y organigrama de funcionalidad de estos. Esta información, en manos de personal ajeno a la organización, permitiría que determinadas amenazas que originalmente no eran muy peligrosas, se conviertan en altamente agresivas.

Microsoft SharePoint Server 2010 cuenta con sus propios mecanismos de seguridad, implementados de forma nativa, pero no obstante se puede beneficiar del concurso de otros productos. Actualmente, los documentos se han convertido en un posible sistema para la dispersión de malware. De este modo, estos archivos de uso general pueden distribuir determinados tipos de software malicioso de forma eficiente. Lejos quedaron los tiempos en que el malware era asociado exclusivamente a ficheros con extensión de tipo ejecutable. Es por ello que los esfuerzos de las compañías en proteger también las plataformas de gestión de contenido con seguridad adicional, dotándolas de soluciones antimalware, es una necesidad.

En este sentido, Microsoft proporciona MS Forefront Protection for SharePoint 2010. Su sistema multimotor antimalware ha cosechado en múltiples estudios realizados unas estadísticas impresionantes. La técnica de análisis a través de escaneo en la memoria que emplea resulta mucho más que eficaz que otras tradicionalmente utilizadas. Esta metodología no solamente aporta la capacidad para trabajar con más motores, sino que lo hace de forma más rápida y eficaz. Adicionalmente a sus funcionalidades contra el malware, proporciona también otros sistemas de filtrado de contenido. No deberían mezclarse documentos relacionados con la seguridad con otros de distinta índole. El sistema de filtrado protegerá contra estos hechos. Por otra parte, las métricas aportadas permiten determinar en qué medida una organización está sufriendo ataques a través de este medio.

Debe tenerse en cuenta que es tan importante la seguridad de la infraestructura como la de los recursos que ésta suministra. Si el sistema de gestión de contenido que

Figura 6.2. Gestión de la seguridad de un MS SharePoint 2010 con MS FPSP 2010.

se ofrece no es seguro, se inutiliza el escenario de la seguridad y a la postre incide en el incumplimiento de lo establecido en el ENS.

La monitorización de los sistemas es crítica cara a la disponibilidad de los mismos. Evaluar su rendimiento o los fallos que se estén produciendo es algo fundamental para determinar si se están ofreciendo los mecanismos más idóneos de funcionalidad. Si un sistema que no se encuentra correctamente monitorizado deja de funcionar porque el espacio libre de disco ha caído significativamente, podría pasar un tiempo crítico antes de que alguien advirtiera de este hecho. En ocasiones, los administradores son informados de que un servicio no está operando a través de las llamadas que reciben por parte de los usuarios del mismo. Situaciones como estas suponen no solamente un problema de control de funciones, sino que la falta de confianza en el servicio prestado se pueda convertir en una crítica generalizada.

Aunque no está definido específicamente en el texto del ENS, las organizaciones deberían contar con elementos que permitan evaluar si sus servicios están trabajando correctamente. Que esto se haga de forma eficiente es un hecho diferenciador muy importante. Hay que recordar que uno de los requisitos que se establecen en el Esquema Nacional de Seguridad es que la prestación de servicios hay que realizarla de la forma más óptima y, para ello, en algunas circunstancias se exige un estudio previo de dimensionamiento. Cuando las previsiones fallan a la larga, sólo una monitorización

continua del servicio se traduce en descubrir que es necesario redimensionarlo. La plataforma MS System Center Operation Manager 2007 R2 (SCOM 2007 R2) proporciona los mecanismos para una correcta monitorización de los sistemas, servicios y periféricos. Estas labores no son nuevas en los productos y soluciones Microsoft; sin embargo, a partir de MS SCOM 2007 R2 se ha modificado la forma de entender la monitorización de los sistemas.

La orientación original de las versiones anteriores era la monitorización de los servidores, pero a la larga se ha visto que resulta mucho más eficiente una orientación dirigida a la monitorización de los servicios. Que un servicio dentro de un servidor pueda presentar un error, no implica que el resto se encuentren operando incorrectamente. Esta estrategia es mucho más cercana al Esquema Nacional de Seguridad, donde lo que preocupa precisamente es la prestación de los servicios, claro está sin descuidar los sistemas servidor o estación de trabajo que los hacen factibles.

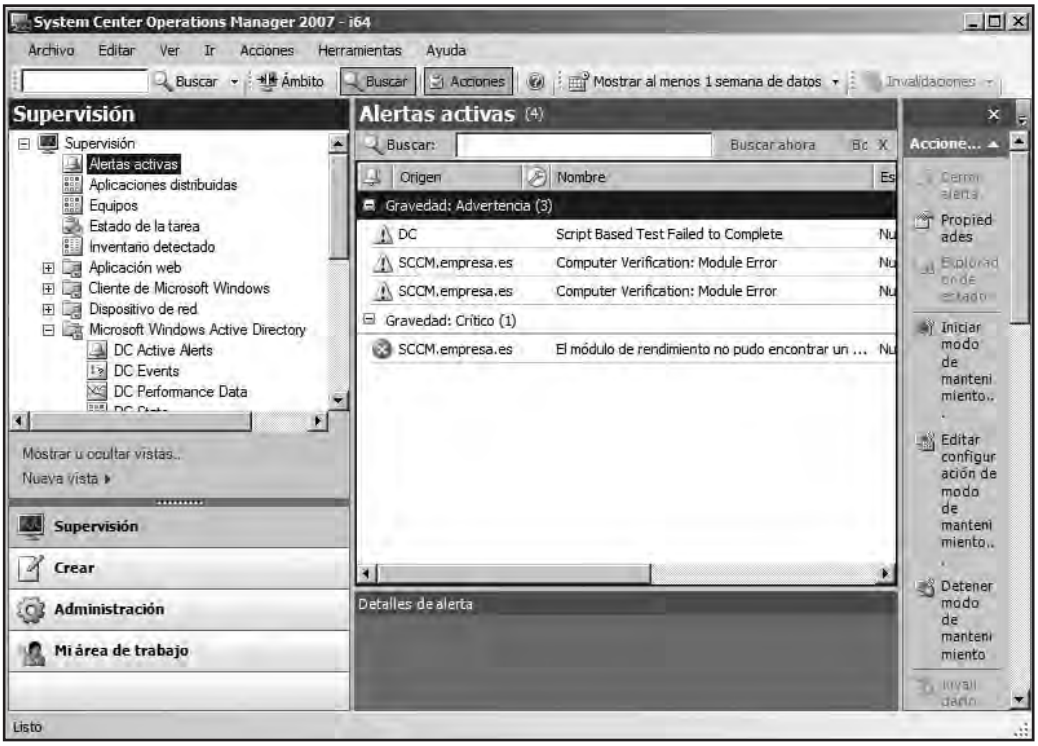


Figura 6.3. Panel de Control de MS System Center Operation Manager 2007 R2.

MS System Center Operation Manager 2007 R2, a través de una arquitectura de agentes y haciendo uso de los Management Pack correspondientes, proporciona al administrador consolas de operación donde evaluar el estado general de sus servicios. Las mismas pueden ser planteadas a través de la representación gráfica de las infraestructuras y una monitorización en tiempo real. Esto permite atender al máximo

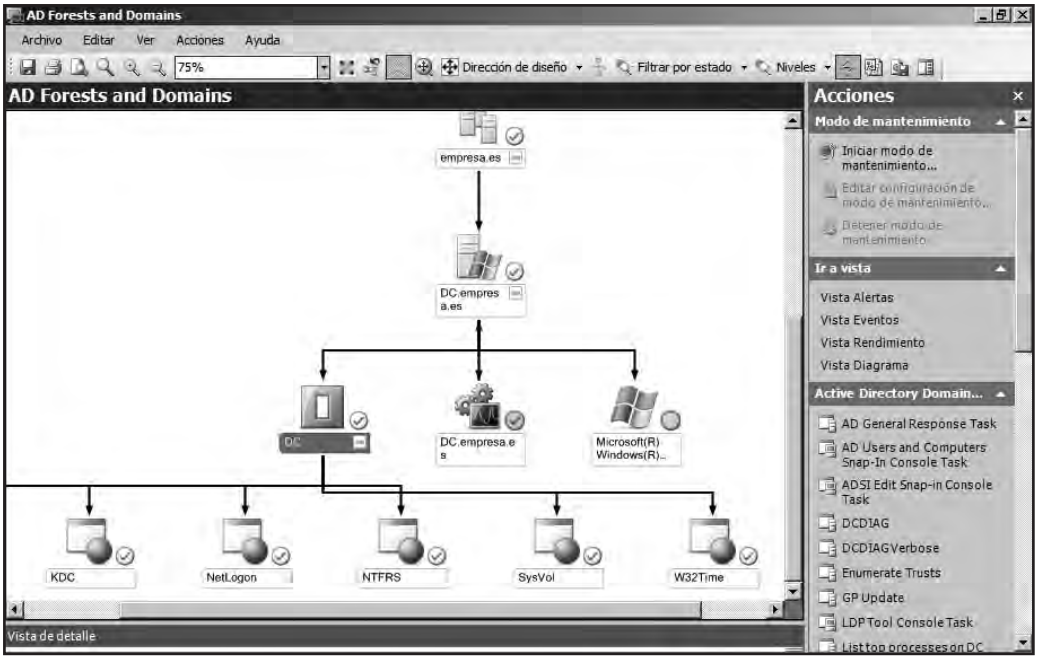


Figura 6.4. Esquema de infraestructura y monitorización con SCOM 2007 R2.

las necesidades estipuladas por el ENS de mantener a través de las arquitecturas de seguridad los mapas de estado de las infraestructuras.

Puesto que los Management Pack se han diseñado para productos que van más allá de las plataformas Microsoft, MS SCOM 2007 R2 permite la gestión de infraestructuras muy heterogéneas. Mapas y monitorización de la plataforma de red, estado de las soluciones de seguridad o de la DMZ (Zona desmilitarizada) en una infraestructura de defensa perimetral son algunas de las situaciones en las que se obtendría ganancia de esta solución.

Hay que tener en cuenta que el producto cuenta también con un aspecto de reactividad ante un imprevisto o una posible contingencia, pudiéndose programar una respuesta automatizada. Si determinado servicio indispensable cae, se podría iniciar un proceso para reiniciarlo automáticamente. Si éste falla, se podría generar una alerta en la consola de operación o enviar un correo electrónico.

Las posibilidades evidentemente son amplias y deberán ser tenidas en cuenta. SCOM 2007 R2 también aporta otras características, relacionadas con la trazabilidad, menos conocidas pero interesantes desde el punto de vista del ENS. A través de su rol de ACS (Audit Collection Services) se puede utilizar como plataforma para la consolidación y correlación de logs.

La línea de productos MS Forefront participará también activamente en las implicaciones de seguridad que exige como norma el Esquema Nacional de Seguridad.

Se estima necesaria la aportación de sistemas de Firewall como plataforma de soporte multired y la segmentación de servicios. Pero también las soluciones antimalware son parte activa de las medidas a plantear. La protección se hace extensiva a todos los niveles. Cuanto antes se disponga del nivel apropiado de protección menor será la capacidad para que un ataque tenga éxito.

La tendencia general es disponer la solución antimalware en los sistemas finales, clientes y servidores. Sin embargo, una buena práctica consiste en prevenir los ataques en el perímetro, antes de que puedan interactuar con el usuario. Las aportaciones de todos los productos de la línea MS Forefront Protection, en sus variantes para MS Exchange Server o MS SharePoint Server, constituyen una primera línea defensiva fundamental. Los correos electrónicos y más recientemente los documentos, se han convertido en elementos significativos para la dispersión del malware.

Pero también ataques encubiertos, como el spam, afectan negativamente a las organizaciones. Quizás no sean conceptuados como un factor de ataque directo, pero indirectamente generan un gran perjuicio a la organización. Obligan a desviar recursos para la realización de copias de seguridad de correos electrónicos que no aportan nada significativo. Molestan al usuario final, y en ocasiones consiguen su fin al hacer que el usuario lo atienda e, incluso, acceda a los vínculos que estratégicamente proporcionan. Son una de las fuentes de ataque tipo phising, pero también de suplantación de identidad en las redes sociales más habituales.

La gestión del perímetro también es tratada en el RD 3/2010. Sistemas como MS Forefront Threat Management Gateway 2010 o MS Forefront Unified Access Gateway 2010 aportan medidas adicionales para la protección de los servicios de cualquier Administración. La protección y el control del cliente final, la publicación segura y controlada de los servicios o el suministro de mecanismos de conexión remota basados en las últimas tecnologías son algunos de esos aportes.

El compromiso de estos productos con escenarios multiplataforma hace factible que sean utilizados en un gran número de ellos. A modo de ejemplo, MS Forefront Unified Access Gateway 2010 acepta como cliente final para el control de su seguridad no sólo clientes Windows, sino también sistemas Linux y MacOS.

Dentro de las plataformas heterogéneas que conforman las diferentes Administraciones Públicas, se requieren sistemas de homogeneización que permitan la integración y a la vez faciliten la tarea de los usuarios. En esta línea se encuentra MS Forefront Identity Manager 2010. La diversificación en los sistemas de autenticación aumenta formalmente los riesgos de seguridad.

Ante la ausencia de unificación para los procedimientos de autenticación, los usuarios deben utilizar múltiples credenciales para los diferentes accesos. Esto indiscutiblemente repercute negativamente en la seguridad, al incrementar el grado de incomodidad del usuario. Esta situación puede minimizarse con una gestión unificada de la identidad.

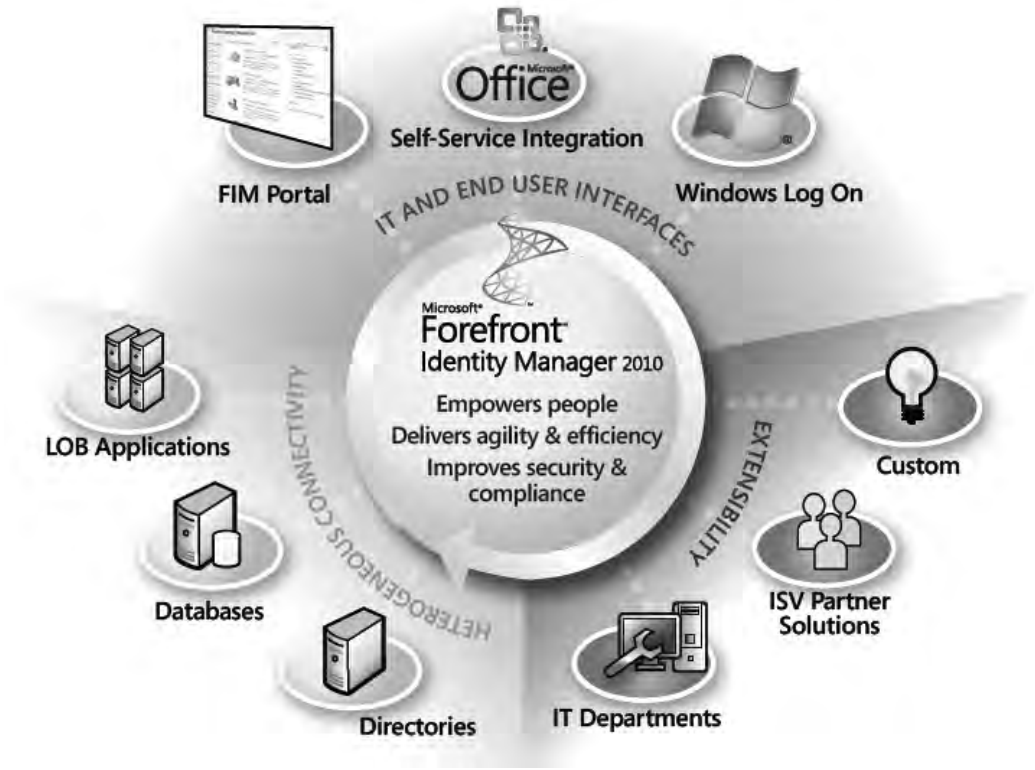


Figura 6.5. Microsoft Forefront Identity Manager 2010.

Desde que en el año 2002 Microsoft publicara su iniciativa Trustworthy Computing, muchas han sido las soluciones que se han generado a través de ella. Se han sumando a elementos que ya existían, como los sistemas de gestión de certificados que han progresado en sus capacidades. Pero también se han aportado soluciones innovadoras y novedosas. Microsoft, en la generación de sus productos, se encuentra totalmente concienciada de que los aspectos de seguridad son totalmente prioritarios.

6.1. Control de acceso

El control de acceso es uno de los aspectos más importantes en lo que a seguridad informática se refiere, más concretamente en el campo de la auditoría, ya que proporciona la capacidad de conocer en todo momento quién, cuándo, dónde y qué ha ocurrido en un sistema. Por este motivo era de esperar que el Esquema Nacional de Seguridad (ENS) dedicara un apartado (Anexo II, apartado 4.2) a definir el nivel de configuración de esta característica.

Lo prioritario es acotar y comprender el término de control de acceso, para posteriormente poder cumplir las necesidades que exige el Esquema Nacional de Seguridad.

Se entiende por control de acceso aquella acción que se realiza por parte de una entidad para identificarse ante un sistema antes de desempeñar su función. Se puede incluir dentro del concepto de entidad a todo usuario, máquina, servicio o incluso proceso.

El control de acceso que se implante en un sistema deberá ser, según el ENS, un punto de equilibrio entra la comodidad de uso y la protección de la información. Según el nivel de seguridad que requiera cada organismo se primará la comodidad frente a la protección en nivel bajo, mientras que en nivel alto se primará la protección frente a la comodidad de uso.

Todo control de acceso válido para el ENS debe cumplir siempre los siguientes aspectos de comportamiento y configuración:

- Principio del menor privilegio posible. Todo acceso está prohibido, salvo concesión expresa a la acción o información requerida.
- Toda entidad debe quedar identificada de forma unívoca. Cada usuario, servicio, equipo o proceso deben tener una cuenta única en el sistema.
- Los recursos se protegerán por defecto. El acceso a la información debe estar protegido bajo mecanismos de control, como las listas de control de acceso (ACLs) que establecen las entidades que tienen derecho al mismo.
- Establecer procedimientos de baja y alta prioridad, concediendo los derechos de acceso a las diferentes entidades atendiendo a la autorización necesaria en cada caso.
- La identidad de la entidad debe quedar siempre suficientemente autenticada. Son necesarios mecanismos de autenticación que permitan identificar correctamente a la entidad con la mayor seguridad posible.
- Se debe controlar tanto los accesos locales como remotos a la información.
- Debe quedar registrado el uso del sistema para poder detectar y actuar ante cualquier fallo accidental o deliberado.

El ENS define claramente cómo se deben establecer todas las características anteriores según el nivel de criticidad de la información a manejar y proteger. Como es posible observar en la tabla que aparece a continuación, el ENS establece para cada uno de los aspectos relacionados con el control de acceso el nivel de medidas a aplicar.

A continuación se detallarán cada uno de las medidas de seguridad en lo que a control de acceso se refiere y cómo la tecnología de Microsoft ayuda a conseguir los requisitos exigidos.

6.1.1. Identificación

"La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

a) Se asignará un identificador singular para cada entidad (usuario o proceso) que accede al sistema, de tal forma que:

1º Se puede saber quién recibe y qué derechos de acceso recibe.

2º Se puede saber quién ha hecho algo y qué ha hecho.

b) Las cuentas de usuario se gestionarán de la siguiente forma:

1º Cada cuenta estará asociada a un identificador único.

2º Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.

3º Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención."

El Esquema Nacional de Seguridad establece que el procedimiento de identificación debe ser idéntico en los tres niveles de seguridad, como se puede observar en la siguiente tabla. El ENS exige que los procesos de identificación deban cumplir los siguientes aspectos:

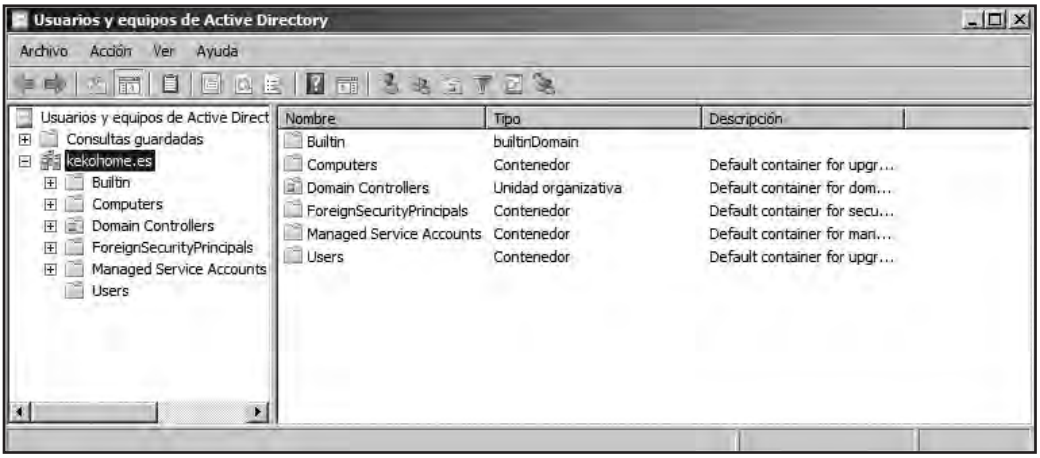
- Todos los usuarios y servicios deben ser identificados de forma inequívoca, para poder identificar cada acción realizada sobre la información a proteger.
- El sistema tiene que tener la capacidad de deshabilitar las cuentas de usuarios y servicios cuando estos dejen de ser operativos, pero sin eliminarlas para atender a las necesidades de trazabilidad de los registros de actividad.

A pesar de contar con el mismo nivel de exigencias de seguridad, es necesario distinguir los distintos tipos de identificación que existen en los entornos de Microsoft, Active Directory e identificación local. A continuación se detalla en qué medida soportan los distintos tipos los requisitos establecidos por el ENS.

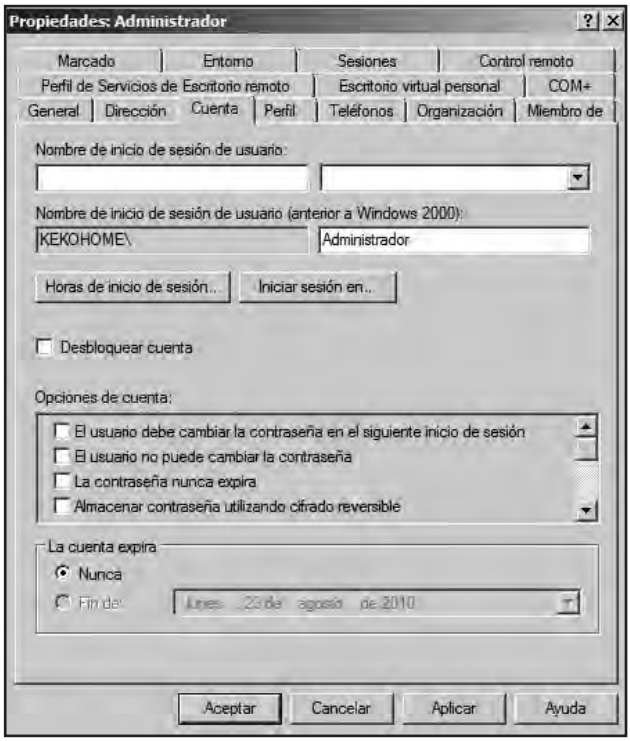
Active Directory

La totalidad de los productos de Microsoft soporta el mecanismo de autenticación basado en Active Directory, lo que significa que la gestión de la identificación de los usuarios y servicios la realizan de forma centralizada los controladores de dominio Active Directory permite cumplir de una forma sencilla los requisitos que establece el ENS en lo que a identificación se refiere. En primer lugar permite mantener una cuenta en el sistema para cada usuario o servicio que se ejecute en él. En este punto es necesario un alto grado de concienciación por parte de los responsables de esta labor, ya que serán los encargados de garantizar que cada usuario y servicio utiliza una cuenta inequívoca en el sistema. Para la creación de las cuentas necesarias en los controladores de dominio Windows Server 2008 R2 es necesario detallar los dos tipos

disponibles, usuarios y servicios. La creación de las cuentas de usuarios se realiza del modo tradicional a través de la consola de usuarios y equipos de Directorio Activo.



Otro de los requisitos que establece el ENS es la capacidad de bloquear las cuentas sin necesidad de eliminarlas. Este requisito es soportado por Active Directory, ya que una de las propiedades de las cuentas permite deshabilitarlas sin eliminarlas definitivamente del sistema.



En lo que a las cuentas de servicio se refiere, Active Directory en Windows Server 2008 R2 proporciona para los servicios que se ejecuten con cuentas de dominio, las denominadas cuentas de servicio.

Cuentas de servicio

Las cuentas de servicio son cuentas de dominio administradas que proporcionan las características necesarias para cubrir los requisitos de identidad y restos de exigencias establecidas por el Esquema Nacional de Seguridad.

La creación de estas cuentas se lleva a efecto a través de un procedimiento específico y muy distinto al utilizado en la creación de cuentas de usuario de carácter estándar. Este proceso de creación de cuentas de servicio se encuentra sujeto a una serie de requisitos previos a nivel de Active Directory.

Los requisitos previos que debe cumplir Active Directory para poder trabajar con las cuentas de servicio son los que se detallan a continuación:

- Nivel funcional de dominio Windows Server 2008 R2.
- En un dominio con el nivel funcional Windows Server 2008 o Windows Server 2003 con al menos un controlador de dominio Windows Server 2008 R2.

En un dominio con nivel funcional Windows Server 2008 o Windows Server 2003 también se pueden usar cuentas de servicio sin instalar un controlador de dominio Windows Server 2008 R2, si para ello se implementa en un controlador de dominio existente el servicio de puerta de enlace de Active Directory.

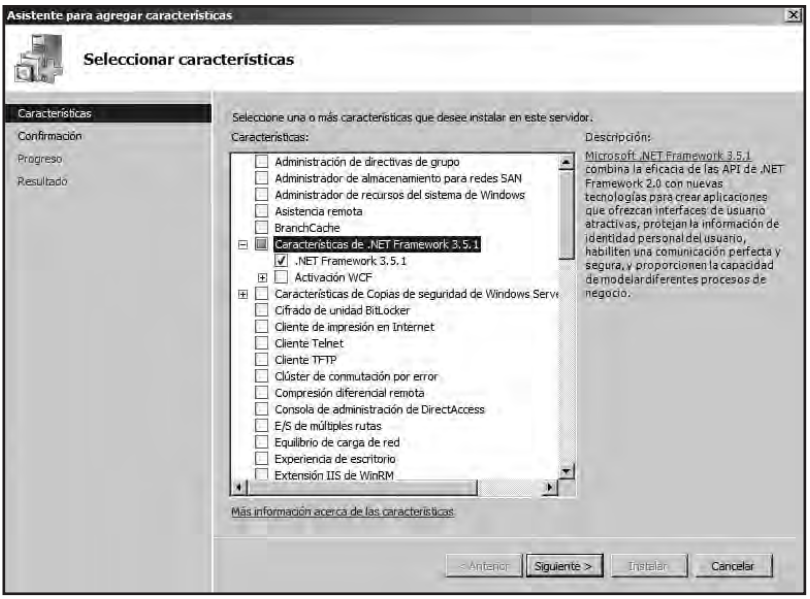
La creación de las cuentas de servicio se debe realizar siempre en el equipo donde se vaya a ejecutar el servicio. Los sistemas operativos que pueden crear este tipo de cuentas son únicamente Windows Server 2008 R2 y Windows 7. Los requisitos que deben cumplir dichos sistemas para la creación de las cuentas de servicio son los que se detallan a continuación:

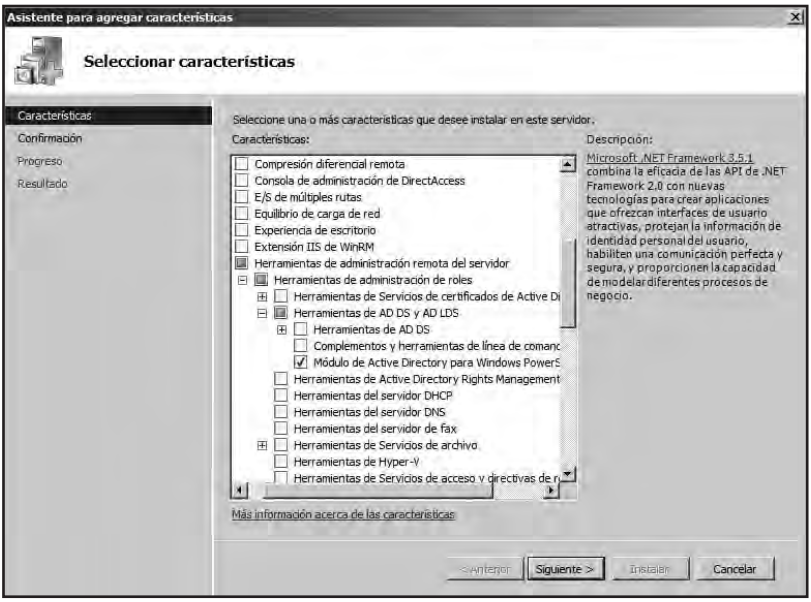
- Microsoft .NET Framework 3.5.1 (véase la figura superior de la siguiente página).
- Módulo de Active Directory para Windows PowerShell (imagen inferior de la siguiente página).

Una vez cumplidos los requisitos previos y desde el equipo donde se ejecutará el servicio, se debe realizar la creación de la cuenta. Esta se lleva a efecto a través de MS Windows PowerShell y es necesario para ello seguir los pasos siguientes:

1. En primer lugar es necesario importar el módulo de Active Directory que permitirá posteriormente crear y gestionar las cuentas de servicio. La importación del módulo se consigue a través de la ejecución del siguiente cmdlet (nombre que reciben los comandos de PowerShell):

   Import-Module ActiveDirectory





Es necesario ejecutar esta instrucción cada vez que se desee realizar cualquier tipo de cambio con cuentas de servicio.

2. Seguidamente, la creación de una cuenta de servicio se debe realizar mediante la ejecución del siguiente *cmdlet*:

   New-ADServiceAccount NameService -SamAccountName SAMName -AccountPassword (convertTo-SecureString -AsPlainText "Password" -Force)

-Enabled $True -ServicePrincipalName “Service/FQDN_Host:PortService/DistinguishedName”

3. Al configurar el servicio para que se ejecute con la cuenta recién creada es necesario recordar que el nombre de las cuentas de servicio siempre finalizarán con el símbolo ‘$’ (por ejemplo, Dominio\SAMName$).

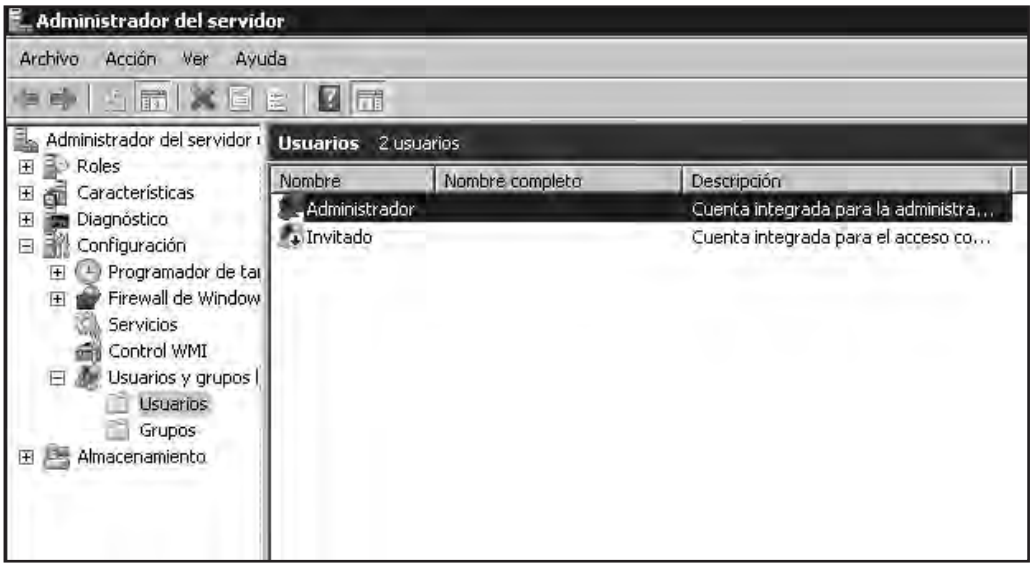
Este procedimiento de creación de cuentas de servicio se debe realizar para cada uno de los servicios que se ejecutan en el sistema. De este modo se cumple el requisito del ENS en lo que a identificación se refiere.

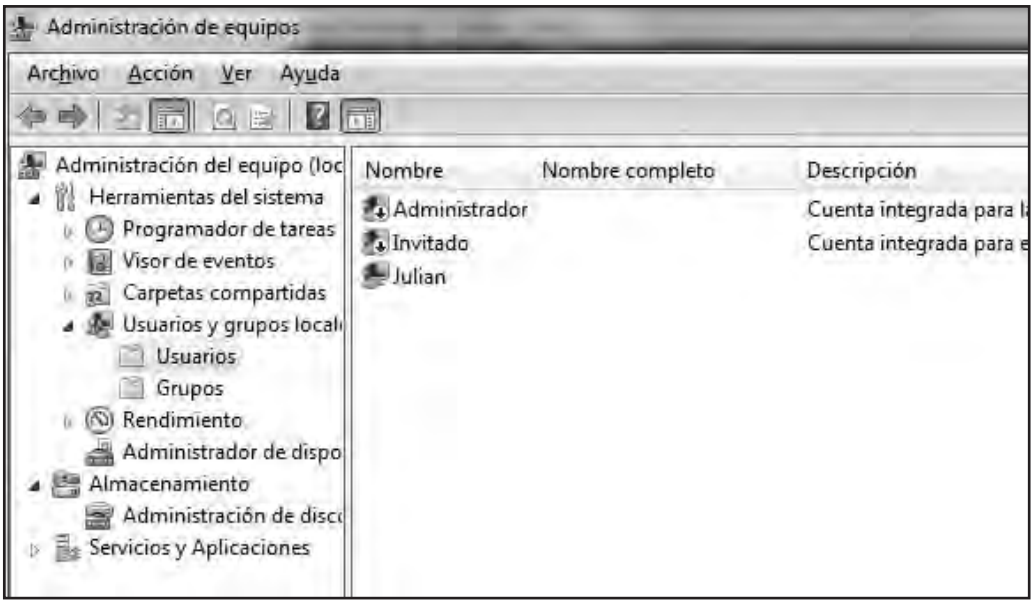
No es posible deshabilitar las cuentas de servicio del mismo modo que el resto de las cuentas de Active Directory. Con este tipo de cuentas la operación se debe realizar a través de PowerShell (Set-ADServiceAccount) o mediante la herramienta de Editor ADSI. En ambos casos se puede cambiar el atributo Enabled de las cuentas de servicio a valor False, consiguiendo así su deshabilitación.

Identificación local

El Esquema Nacional de Seguridad también exige que los equipos que no son miembros de un dominio o que requieran de la creación de cuentas locales de usuario cumplan con las exigencias de la normativa. Windows Server 2008 R2 y Windows 7 son aptos para el cumplimiento de los requisitos de identificación de las cuentas.

Para la creación local de cuentas de usuario es necesario utilizar la herramienta de administrador en Windows Server 2008 R2 o la herramienta de Administración de equipos en Windows 7. En ambos casos, la creación de la cuentas permiten cumplir el requisito de autenticación inequívoca de todos los usuarios y servicios del sistema.

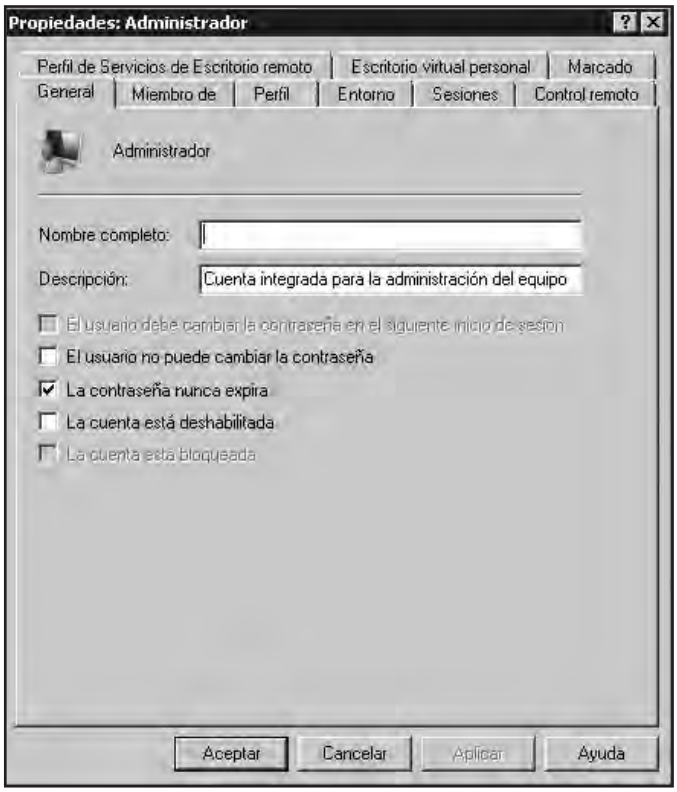




Al igual que en Active Directory, es necesario un alto grado de concienciación de los responsables de la creación de las cuentas, ya que serán los encargados de hacer cumplir el ENS en lo que a identificación única se refiere.

El otro requisito del ENS para el proceso de identificación es la capacidad de bloquear las cuentas sin necesidad de eliminarlas para ello. Este requisito es soportado por Windows, ya que una de las propiedades de las cuentas permite deshabilitarlas sin eliminarlas del sistema.

(Consulte la figura de la derecha.)



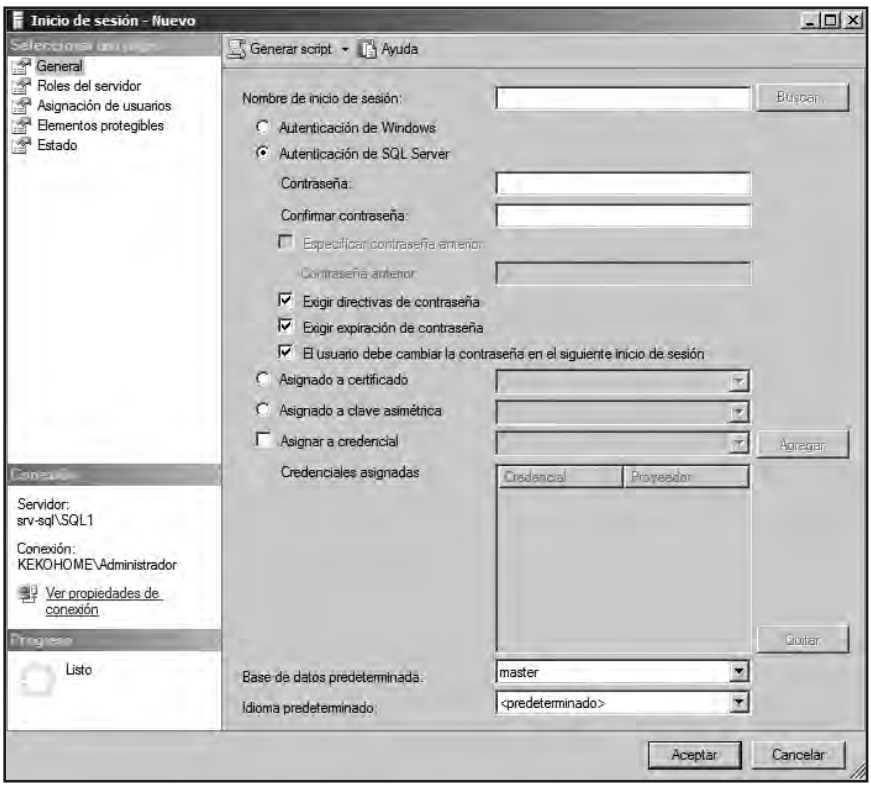
Identificación de Aplicación Servidor

Algunos de los sistemas servidores Microsoft, como puede ser MS SQL Server, proporcionan capacidades de gestión de identificación independientes al sistema operativo y Active Directory. En estos casos es necesario que el sistema servidor cumpla también con lo establecido en el Esquema Nacional de Seguridad siempre que se emplee dicho mecanismo de identificación.

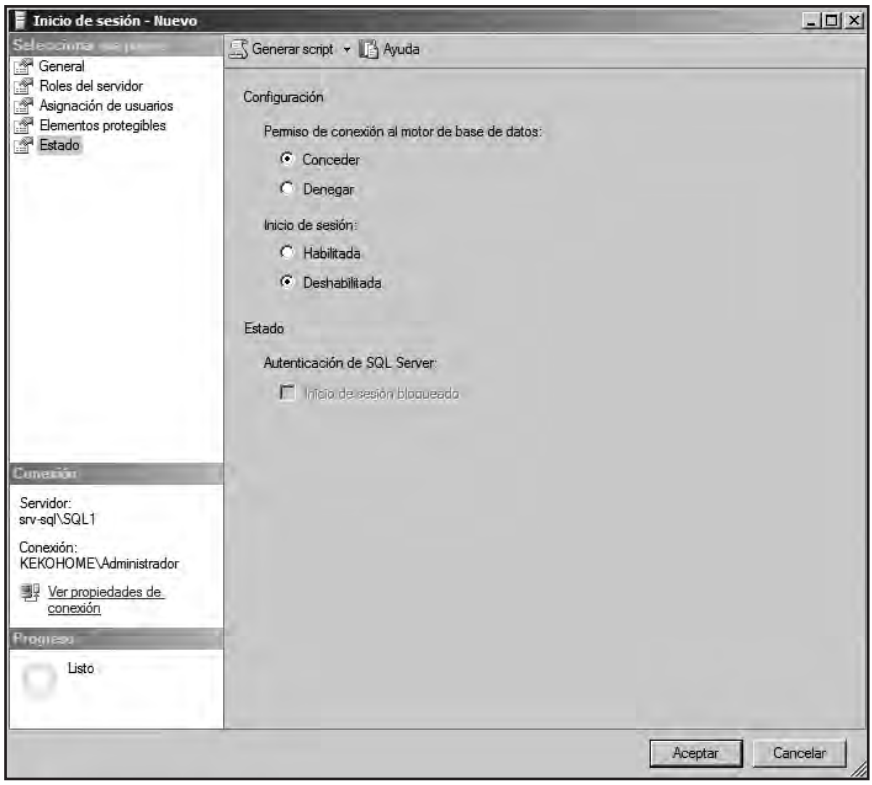
La totalidad de los sistemas servidor de Microsoft que presentan mecanismos alternativos de identificación de los usuarios cumple los requisitos del ENS. Por su extensibilidad se utilizará, en esta publicación, Microsoft SQL Server como ejemplo de cómo estos sistemas permiten el cumplimiento de los mencionados requisitos.

MS SQL Server soporta la capacidad de identificación única de los usuarios y aplicaciones que accedan en este caso concreto al sistema gestor de base de datos. Para la identificación se utilizan los inicios de sesión, objetos que identifican a usuarios y aplicaciones en cualquiera de los servicios de MS SQL Server: Motor de base de datos, Analysis Services, Reporting Services e Integration Servicies.

Los inicios de sesión en MS SQL Server 2008 R2 soportan dos tipos de autenticación: Integrada en Windows y propia de MS SQL Server. En ambos casos se permite la identificación inequívoca de quién accede, cuándo lo hace y a qué información.



También MS SQL Server 2008 R2 soporta la capacidad de deshabilitar los inicios de sesión prohibiendo así el acceso a la información y, al mismo tiempo, permitiendo la auditoria de dichas cuentas en el sistema, como exige el Esquema Nacional de Seguridad.



6.1.2. Requisitos de acceso

"Los requisitos de acceso atenderán a lo que a continuación se indica:

a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.

b) Los derechos de acceso de cada recurso se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.

c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración."

El Esquema Nacional de Seguridad establece que el procedimiento de requisitos de acceso debe aplicarse en los tres niveles de seguridad, como se indica en los siguientes párrafos.

El ENS exige que los requisitos de acceso en los sistemas deban cumplir los siguientes aspectos:

- Todos los recursos del sistema se protegerán impidiendo el acceso a todo el mundo, salvo a la entidades que cuenten con los derechos de acceso necesarios.
- Los derechos de acceso a cada recurso se establecen según los criterios de la persona responsable del recurso, siguiendo en todo momento la normativa de seguridad del sistema.
- Se debe controlar el acceso a los componentes del sistema y sus ficheros o registros de configuración.

Microsoft proporciona en todos sus sistemas las listas de control de acceso que nos permiten controlar el mismo a cada uno de los recursos del sistema. Una lista de control de acceso o ACL es una lista de entidades donde se establecen los derechos de acceso para permitir, denegar o auditar la actividad de dicha entidad sobre cada recurso.

Por tanto, el proceso de securización de los recursos de sistema, en cuanto a requisitos de acceso se refiere, recae principalmente sobre las ACLs del sistema. En los entornos Microsoft, las ACLs se presentan en diversos entornos, desde el sistema operativo hasta el sistema de ficheros, pasando por las aplicaciones.

A continuación se detalla cómo los sistemas de Microsoft permiten establecer restricciones de acceso a través de los distintos mecanismos existentes.

Acceso al sistema operativo

Al hablar de restricciones de acceso siempre se piensa en primer lugar en el sistema operativo. Windows Server 2008 R2 presenta la opción de proteger el acceso al sistema mediante una lista de control de acceso, impidiendo el acceso total al sistema y posteriormente estableciendo acceso total o parcial al mismo, atendiendo a lo establecido en el ENS.

Al igual que en configuraciones abordadas con anterioridad, cuando se habla de aplicar restricciones sobre los sistemas operativos es necesario abordar la solución tanto desde el punto de vista de Active Directory como desde un sistema operativo independiente.

El ENS establece como requisito que la totalidad de los recursos del sistema estarán protegidos por defecto ante el acceso por parte de cualquier entidad, es decir, en este caso las cuentas de usuario deberían tener prohibido el acceso a la totalidad de los equipos.

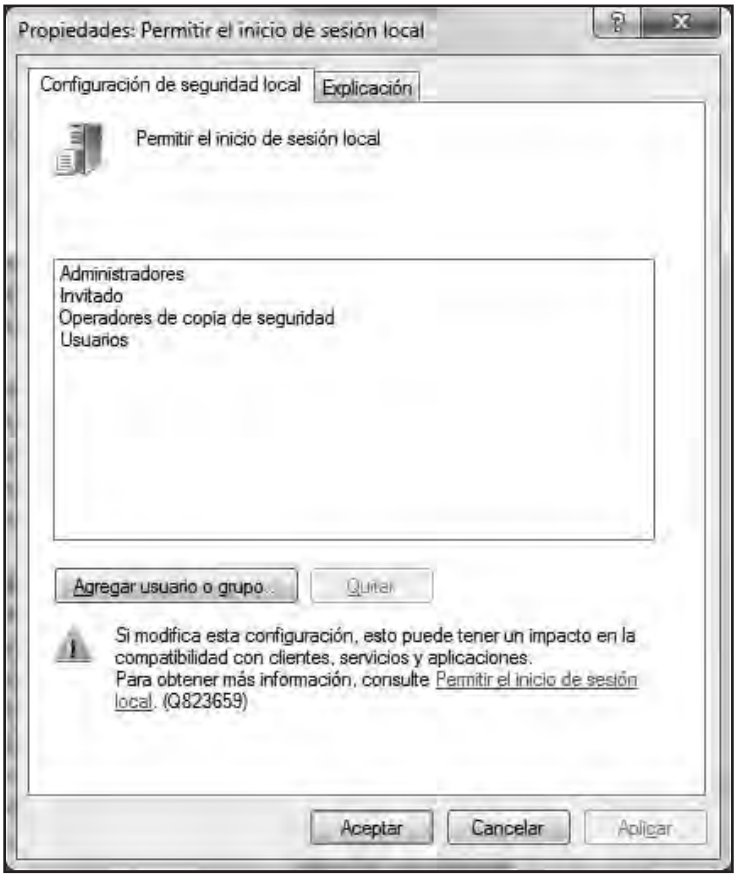
El cumplimiento de este requisito desde una solución de Active Directory es factible. Para ello se proporciona una característica a las cuentas de usuario que establece sobre qué máquinas pueden iniciar sesión, como se puede apreciar en la ilustración que aparece a continuación.

Si dicha lista o ACL se encuentra vacía, la cuenta de usuario no puede iniciar sesión en ninguna máquina del dominio, prohibiendo el acceso de forma predeterminada a los recursos del sistema. Por consiguiente, si se agregasen cuentas de equipos a la lista, esto significaría la posibilidad de iniciar sesión en dichos equipos. Este último procedimiento se debe realizar de forma controlada y autorizada por parte del responsable del sistema.

Por el contrario, en un escenario no Active Directory o para cuentas de usuario locales de máquina, el cumplimento de dicho requisito de debe establecer de forma local en cada uno de los sistemas. El procedimiento consistiría en establecer una directiva de seguridad que se encuentra en las políticas locales de la máquina.

Para acceder a la directiva de seguridad referenciada es necesario acceder al editor de políticas de la máquina local y configurar la directiva que se encuentra en la siguiente ruta: Configuración de Equipo > Configuración de Windows > Configuración de Seguridad > Directivas locales > Asignación de derechos de usuario. En dicha ubicación existe una directiva con el nombre Permitir el inicio de sesión local que establece las cuentas de usuario que pueden iniciar sesión en el sistema (véase la figura de la siguiente página).

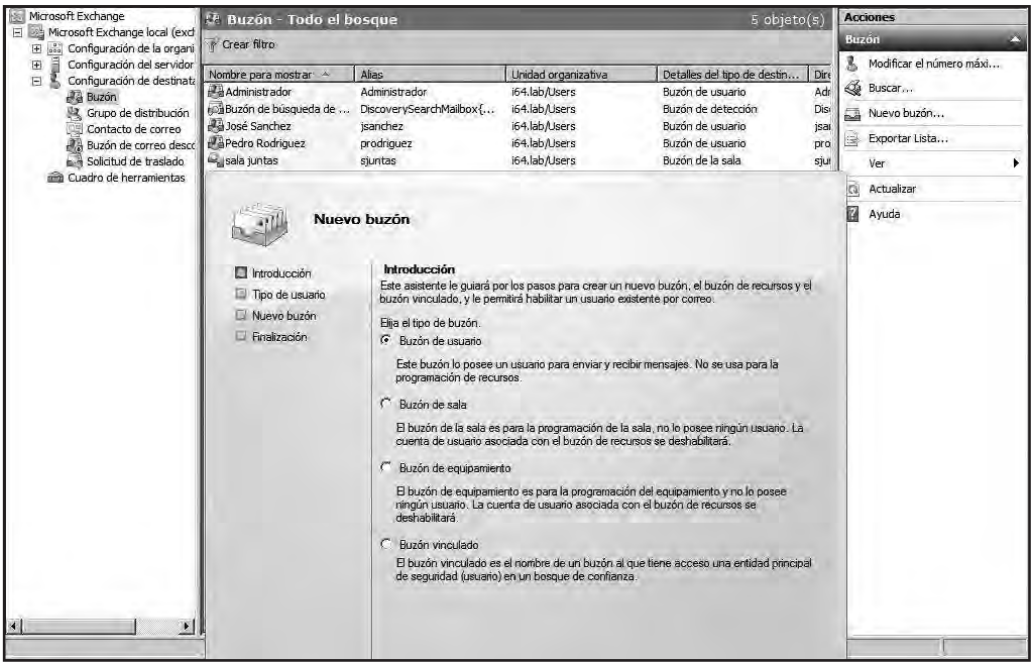
Eliminando de la ACL de la directiva todas las cuentas, a excepción del administrador para garantizar el acceso necesario para la administración del sistema, se cumpliría el requisito establecido por el ENS. Para conceder permiso de acceso a una entidad, bastaría con agregar dicha cuenta a la ACL de la directiva, pero siempre de un modo autorizado por parte de los responsables del sistema en cuestión.



Aplicaciones de servidor

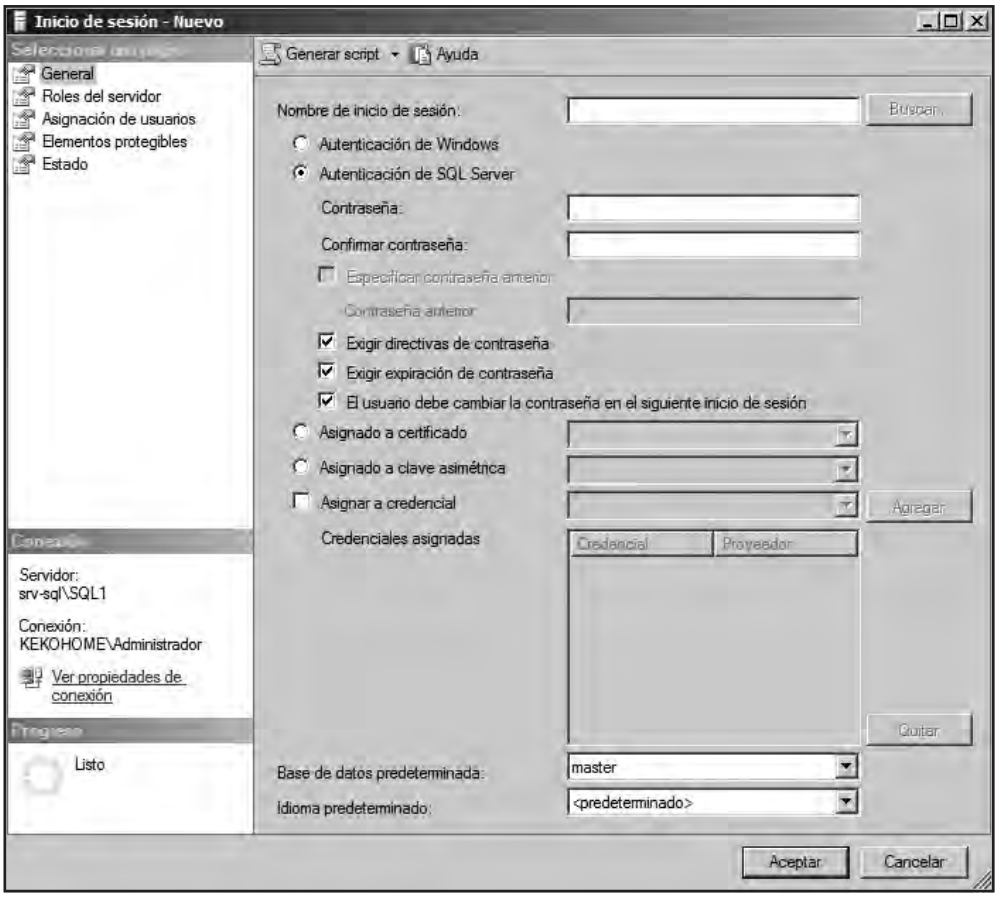
La extensa familia de aplicaciones de servidor con la que cuenta Microsoft, principalmente las últimas versiones de producto, ya cumplen por defecto este requisito. Soluciones como MS Exchange Server 2010, MS SharePoint Server 2010 o MS SQL Server 2008 R2 implementan de forma nativa la prohibición de acceso de cualquier entidad a sus sistemas. En cualquier aplicativo servidor sería necesario establecer acceso al sistema para cada entidad. Por ejemplo, en soluciones MS Exchange Server 2010 es necesario establecer la creación del buzón de correo electrónico para cada usuario, el cual tiene acceso único al mismo, e incluso si fuese requerido se podría establecer acceso para una cuenta de usuario sobre el buzón de correo electrónico de otro usuario (véase la figura superior de la siguiente página).

En el caso de MS SharePoint Server 2010, se deben agregar en la ACL del sitio las cuentas de usuario a las que se desee conceder acceso y la ubicación concreta donde el mismo tenga que acceder. Toda la concesión de permisos siempre debe estar supervisada y autorizada por el responsable del sistema (véase la figura inferior de la siguiente página).



Finalmente, en MS SQL Server 2008 R2, las cuentas de usuario del sistema o de Active Directory al cual pertenece el servidor donde se encuentra instalado el aplicativo, tienen prohibido el acceso al sistema de forma nativa. Si se desea conceder acceso al mismo es necesario crear un inicio de sesión asociado a dicha cuenta (véase la fiura de la siguiente página).

Cualquier sistema servidor de Microsoft requiere de acciones posteriores a la instalación para poder conceder acceso total o parcial al sistema por parte de cualquier tipo de entidad, cumpliendo así los requisitos establecidos a nivel de derechos de acceso por parte del Esquema Nacional de Seguridad.

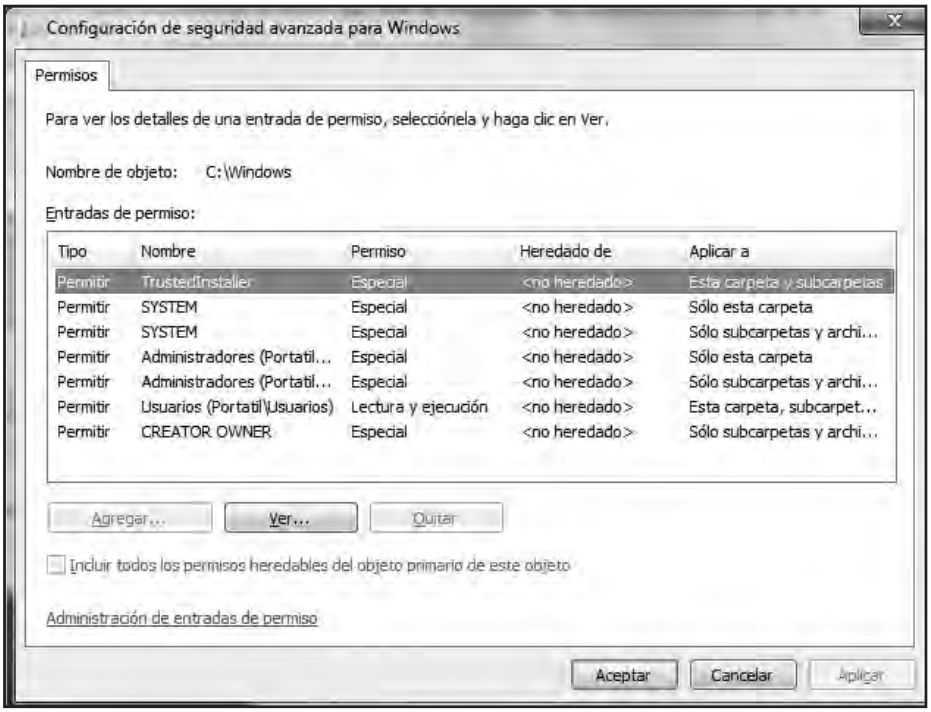


Sistema de ficheros

El sistema de ficheros es otro elemento que proporciona control de acceso en los sistemas informáticos. Concretamente, el requisito de acceso lo establece el sistema de ficheros NTFS a través de su modelo de seguridad. Este sistema de archivos proporciona una lista de control de acceso a cada uno de los objetos que quedan almacenados en el disco, como puede observsar en la imagen superior de la siguiente página.

A través de la ACL se puede establecer un control de acceso granular al sistema e, incluso, impedir de partida el acceso a cualquier elemento como establece el ENS. Posteriormente, siempre bajo el control y la responsabilidad del propietario del sistema, se establecerán los permisos concretos mínimos de acceso a la información.

Este control detallado lo proporcionan los permisos avanzados de NTFS como se puede observar en la ilustración que aparece a continuación (véase la imagen inferior de la siguiente página).


Configuración de seguridad avanzada para Windows
Permisos
Para ver los detalles de una entrada de permiso, selecciónela y haga clic en Ver.
Nombre de objeto: C:\Windows
Entradas de permiso:
Tipo Nombre Permiso Heredado de Aplicar a
Permitir TrustedInstaller Especial <no heredado> Esta carpeta y subcarpetas
Permitir SYSTEM Especial <no heredado> Sólo esta carpeta
Permitir SYSTEM Especial <no heredado> Sólo subcarpetas y archi...
Permitir Administradores (Portatil... Especial <no heredado> Sólo esta carpeta
Permitir Administradores (Portatil... Especial <no heredado> Sólo subcarpetas y archi...
Permitir Usuarios (Portatil\Usuarios) Lectura y ejecución <no heredado> Esta carpeta, subcarpet...
Permitir CREATOR OWNER Especial <no heredado> Sólo subcarpetas y archi...
Agregar... Ver... Quitar
Incluir todos los permisos heredables del objeto primario de este objeto
Administración de entradas de permiso
Aceptar Cancelar Aplicar


Entrada de permiso para Windows
Objeto
Nombre: CREATOR OWNER
Cambiar...
Aplicar a: Sólo subcarpetas y archivos
Permisos: Permitir Denegar
Control total
Atravesar carpeta / ejecutar archivo
Mostrar carpeta / leer datos
Leer atributos
Leer atributos extendidos
Crear archivos / escribir datos
Crear carpetas / anexar datos
Escribir atributos
Escribir atributos extendidos
Eliminar subcarpetas y archivos
Eliminar
Aplicar estos permisos sólo a objetos y/o contenedores dentro de este contenedor
Borrar todo
Administración de permisos
Aceptar Cancelar

6.1.3. Segregación de funciones y tareas

"El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita.

En concreto, se separarán al menos las siguientes funciones:

a) Desarrollo de operación.

b) Configuración y mantenimiento del sistema de operación.

c) Auditoría o supervisión de cualquier otra función."

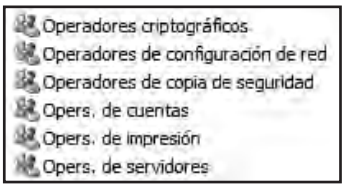
El Esquema Nacional de Seguridad establece que el procedimiento de segregación de funciones y tareas no se debe establecer ante un nivel bajo de seguridad de información, pero por el contrario sí es necesario en los niveles medio y alto, como se puede observar en la indicado en los siguientes párrafos.

El ENS exige que los requisitos de segregación de funciones y tareas en los sistemas de seguridad de nivel medio o alto deban cumplir un único aspecto, que consiste en exigir la concurrencia de dos o más personas para la realización de tareas críticas, para evitar abusos de derechos sobre algún tipo de acción ilícita. En concreto se deben separar al menos las funciones de:

- Desarrollo de operación.
- Configuración y mantenimiento del sistema.
- Auditoría y supervisión de cualquier otra función.

Las últimas versiones de sistemas operativos Windows Server 2008 R2 y Windows 7 proporcionan todo lo necesario para el correcto cumplimiento de este requisito del ENS. Concretamente, estas versiones de sistema operativo disponen de grupos de usuarios específicos para los tres niveles de control.

El sistema proporciona una colección de grupos destinados al desarrollo de determinadas funcionalidades. Un caso ilustrativo pueden ser los operadores de cuentas que proporcionan el permiso para poder realizar tareas de creación o eliminación de cuentas de usuario en sistemas locales o en Active Directory.



Por otro lado, para la configuración y el mantenimiento del sistema, también se proporcionan grupos de usuarios capacitados para configurar y mantener cualquier

funcionalidad ya instalada en el sistema. Un ejemplo puede ser DNSAdmin, que permite configurar y mantener todo lo relacionado con el servidor de resolución de nombres.

Finalmente, para la auditoría y la supervisión existen unos determinados grupos de usuarios que proporcionan la capacidad de ver los registros de eventos y monitorizar el sistema. Por ejemplo, el Lector del registro de eventos proporciona el privilegio de acceder únicamente al visor de sucesos del sistema y conocer qué acciones y qué ha ocurrido sobre el mismo.

Los sistemas operativos, como se acaba de ver, proporcionan ayudas para poder cumplir los requisitos establecidos por el ENS en materia de segregación de funciones. Pero si estos grupos no fueran suficientes, el sistema soporta la creación de nuevo, y siguiendo los mecanismos de requisitos de acceso detallados en el apartado anterior,

se suministran a dichos grupos los privilegios necesarios para la realización de sus objetivos.

En cualquiera de los casos, simplemente agregando las entidades encargadas de realizar cada una de las tareas a los respectivos grupos se conseguiría resolver el objetivo.

6.1.4. Proceso de gestión de derechos de acceso

"Los derechos de acceso de cada usuario se limitarán atendiendo a los siguientes principios:

a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario."

El Esquema Nacional de Seguridad establece que el proceso de gestión de derechos de acceso se encuentre regulado independientemente del nivel de seguridad requerido. El ENS establece que los derechos de acceso de cada usuario se ajustarán estrictamente a los siguientes principios:

- Mínimo privilegio para acotar los daños que pudiera causar una entidad de forma accidental o intencionada.
- Necesidad de conocer. Los privilegios permitirán únicamente a los usuarios acceder al conocimiento necesario para el cumplimiento de sus obligaciones.
- Capacidad de autorizar. Únicamente el personal con competencia para ello podrá conceder, alterar o simplemente anular la autorización de acceso a los recursos.

Para el cumplimiento de estos requisitos Microsoft proporciona en su nuevos sistemas operativos, Windows Server 2008 R2 y Windows 7, componentes que ayudan a simplificar dichas tareas. Se trata del control de cuentas de usuario y la delegación de funciones.

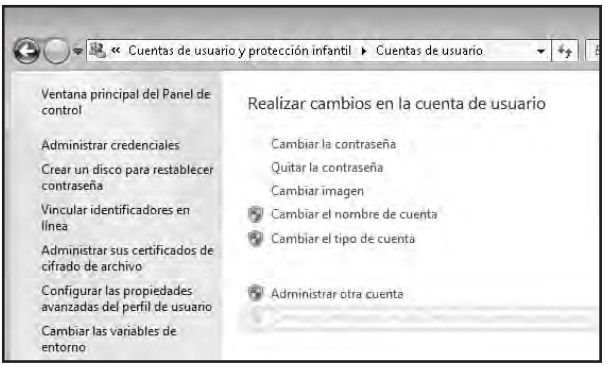
Control de cuentas de usuario

Cumplir con el mínimo privilegio posible para todas las cuentas es una tarea realmente compleja. Existen cuentas de usuario que requieren privilegios elevados en el sistema para una determinada tarea, pero no para el resto. En este momento es cuando interviene el control de cuentas de usuario.

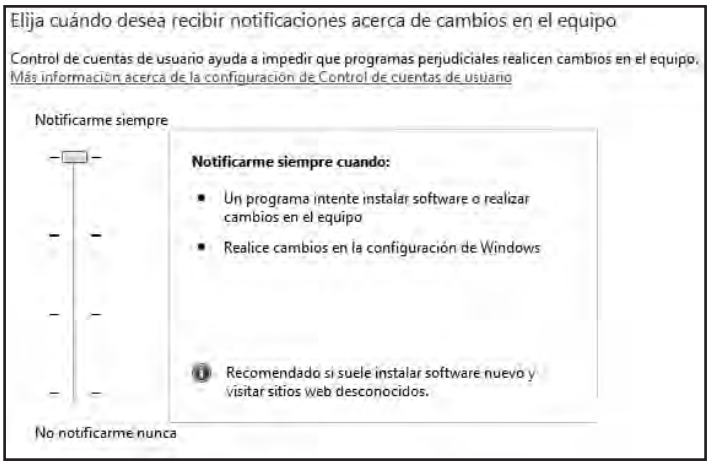
El control de cuentas de usuario o UAC es una funcionalidad de los sistemas operativos Microsoft de nueva generación que obliga al cumplimiento del menor privilegio posible para la realización de cada tarea. Todos los usuarios, ya sean de un dominio o locales, se tratan como usuarios básicos independientemente de los derechos que le hayan sido asignados con anterioridad. Sólo utilizará los derechos en aquellas acciones que lo requieran solicitando previamente al usuario su elevación.

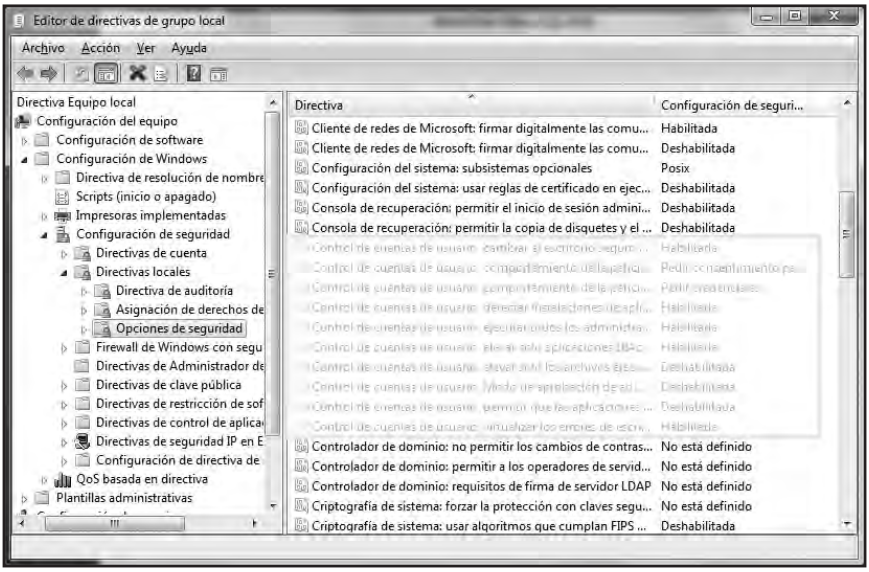
El Control de cuentas de usuario está activado y configurado por defecto en Windows 7 y Windows Server 2008 R2. De este modo, cualquier acción que realice un usuario dentro del sistema contará con los privilegios mínimos, cumpliendo así los requisitos del ENS.

Este nuevo componente de sistema operativo se puede personalizar en cualquier escenario, con el objetivo de adecuarlo a los requisitos de entorno de trabajo de cada usuario. Presenta dos modos de personalización, uno básico y otro avanzado. El básico se realiza desde la herramienta de configuración de cuentas de usuarios, en el Panel de control de los equipos.



Desde esta herramienta se configura el nivel de notificación de elevación de credenciales manteniendo el requisito de mínimo privilegio, aunque en alguna de las opciones de notificación se puede incurrir en otros problemas de seguridad (véase la primera figura de la siguiente página). La configuración avanzada del control de cuentas de usuario permite un control más elevado, y no sólo en lo referente a la notificación. Este otro modo de configuración se realiza a través de políticas, permitiendo una gestión centralizada de dicha funcionalidad.





La configuración de las directivas del control de cuentas de usuario es muy importante realizarla con sumo control para evitar incumplir el ESN en términos de derechos de usuario, ya que permite deshabilitar UAC para determinados tipos de cuentas.

Delegación de funciones

La delegación de funciones es otra de las características de los sistemas operativos que facilita el cumplimiento de las restricciones del ENS en términos de derechos de usuarios. Los sistemas de una organización tienen multitud de funcionalidades cuya administración recae sobre distintas personas.

En muchos casos, este tipo de situaciones se resuelve en las organizaciones estableciendo un nivel de privilegios muy excesivo sobre las personas que intervienen en la administración de los sistemas; son los administradores de los servidores. Este modo de operar incumple lo establecido en el Esquema Nacional de Seguridad.

Para evitar incurrir en el error de conceder un exceso de privilegio a los usuarios encargados de gestionar partes concretas de los sistemas, Windows Server 2008 R2 proporciona modos de delegación de funciones concretas sobre los usuarios o grupos que lo requieran para su posterior administración.

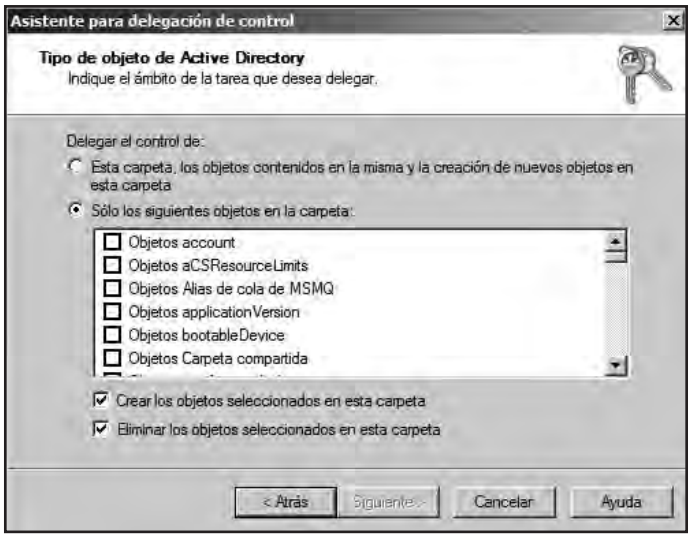
A continuación se abordarán tres ejemplos de delegación de funciones, para conocer las distintas posibilidades que existen en los sistemas operativos.

Active Directory

En la solución de Active Directory, la delegación de funciones es una tarea muy común, ya que existen funcionalidades muy diversas gestionadas por personas distintas. El proceso de delegación de un dominio permite conceder permisos a un usuario estándar para cualquier tipo de acción concreta e, incluso, acumular varios derechos sobre funciones, si el usuario así lo requiere.

El proceso de delegación en Active Directory se basa en un asistente que permite seleccionar la acción o acciones a delegar. Por un lado, el asistente permite seleccionar las acciones más comunes a delegar, como pueden ser crear y administrar cuentas, restablecer contraseñas o, simplemente, unir equipos al dominio.

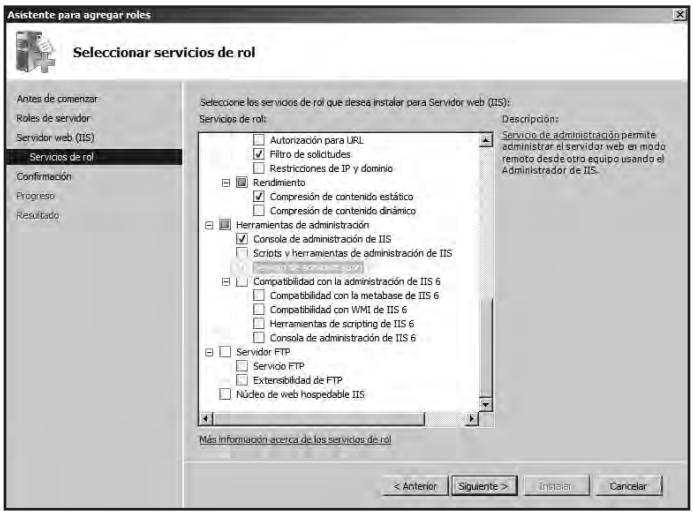
Por otra parte, el asistente también permite establecer un proceso de delegación más detallado sobre los objetos del dominio que se desee. De este modo se podría delegar el control sobre un tipo de objeto concreto que se encuentre en un determinado contenedor.



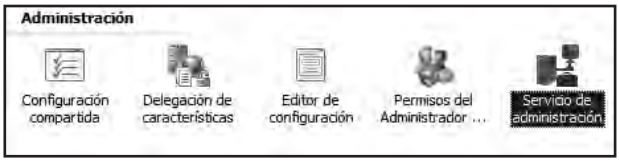
La delegación se puede realizar sobre usuarios individuales o grupos, ambos pertenecientes al dominio a configurar o a otro de confianza.

Internet Information Server (IIS)

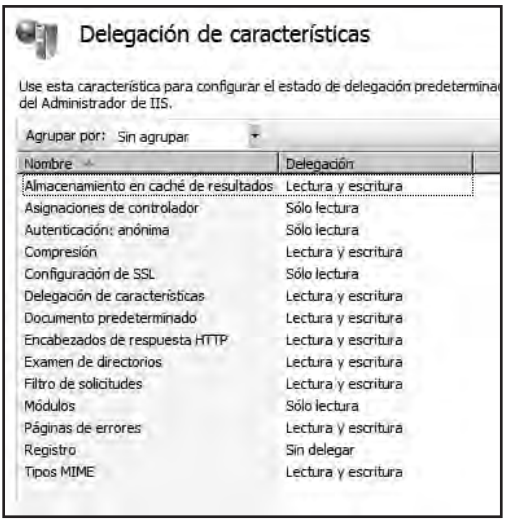
El rol de servidor web en Windows Server 2008 R2 también proporciona la capacidad de delegar la gestión de determinados sitios o aplicaciones web, en el nivel de detalle que se desee. Con esta nueva funcionalidad, se puede plantear la posibilidad de administración delegada de un servidor web con Internet Information Server (IIS). Para habilitar la delegación en el servidor web es necesario contar previamente con el Servicio de Administración instalado. Este se puede instalar a posteriori en el servidor Web, siempre a través del administrador del servidor.



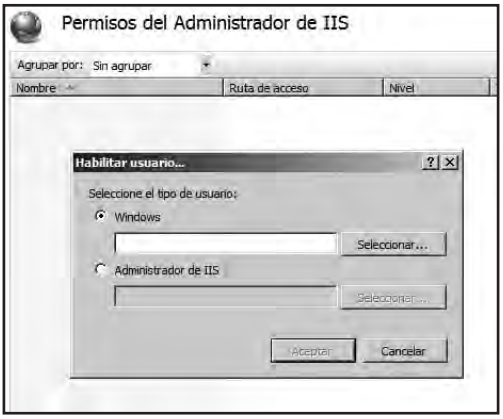
Tras la instalación del servicio, es necesario activar la administración remota del servidor web, ya que la administración delegada sólo es posible de forma remota. La administración remota se habilita, según los requisitos de la organización, desde la consola de administración de IIS a través de la herramienta servidor Servicio de administración.



Una vez configurada la administración remota, ya se pueden delegar la tareas administrativas. Uno de los aspectos más importantes cuando se habla de delegación es determinar las funcionalidades que se van a permitir administrar. Para ello, IIS permite gestionarlas a nivel de servidor o de forma independiente, para cada uno de los sitios web o aplicaciones virtuales alojados en el servidor. Esto lo realiza a través del componente Delegación de características a nivel de servidor, que puede ver en la figura de la derecha.



Finalmente, bastaría con agregar al usuario o usuarios que tienen derecho a la administración del sitio web o aplicación virtual a través del componente Permisos del Administrador de IIS de cada elemento que se desee delegar (véase la figura de la derecha).



Hyper-V

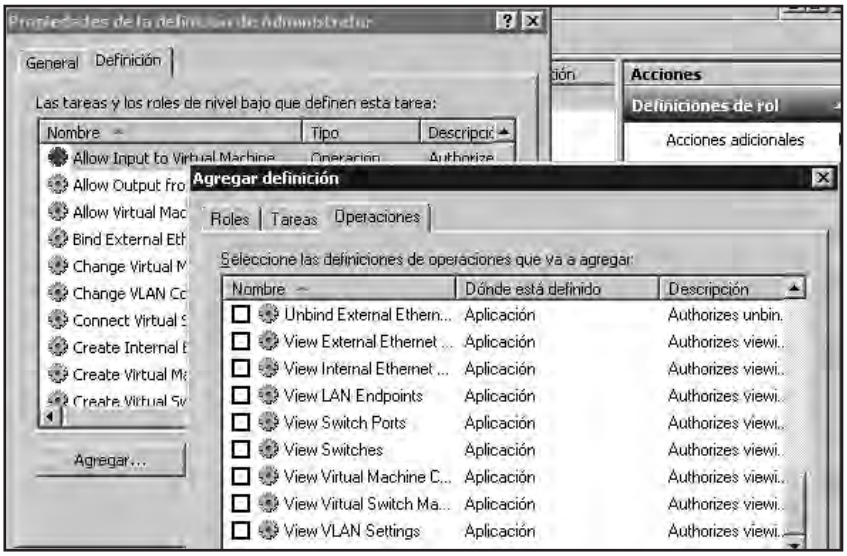
En los sistemas operativos existen diversos componentes cuya delegación no se realiza de forma tradicional o a través de asistentes de configuración destinados a

ello. Un caso concreto de este tipo de componentes es el rol Hyper-V, característica de virtualización que permite la delegación de funcionalidades a usuarios, pero utilizando para ello un archivo de configuración xml.

Con este tipo de procedimientos de delegación es necesario utilizar la herramienta administrativa Administrador de autorización, que permite configurar la delegación basada en archivos de configuración.

Para la delegación de Hyper-V es necesario trabajar con el archivo C:\ProgramData\Microsoft\Windows\Hyper-V\InitialStore.xml para la concesión de credenciales a los distintos usuarios.

Para la personalización de los privilegios que se desean conceder a los distintos usuarios es necesario crear una definición de rol y asignarle las tareas que se desea poder realizar, como se puede observar en la siguiente ilustración.



Finalmente, una vez personalizada la Definición de rol, ya se pueden delegar las tareas configuradas sobre los usuarios que se desee. Para ello, es necesario crear una Asignación de rol que permita asociar la Definición de rol con los usuarios o grupos que se desea disfruten de los privilegios configurados.

6.1.5. Mecanismos de autenticación

"Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados a cada nivel.

Nivel BAJO

a) Se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, o dispositivos físicos (en expresión inglesa «tokens») o componentes lógicos tales como certificados software u otros equivalentes o mecanismos biométricos.

b) En el caso de usar contraseñas se aplicarán reglas básicas de calidad de las mismas.

c) Se atenderá a la seguridad de los autenticadores de forma que:

1.º Los autenticadores se activarán una vez estén bajo el control efectivo del usuario.

2.º Los autenticadores estarán bajo el control exclusivo del usuario.

3.º El usuario reconocerá que los ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.

4.º Los autenticadores se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.

5.º Los autenticadores se retirarán y serán deshabilitados cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) No se recomendará el uso de claves concertadas.

b) Se recomendará el uso de otro tipo de mecanismos del tipo dispositivos físicos (tokens) o componentes lógicos tales como certificados software u otros equivalentes o biométricos.

c) En el caso de usar contraseñas se aplicarán políticas rigurosas de calidad de la contraseña y renovación frecuente.

Nivel ALTO

a) Los autenticadores se suspenderán tras un periodo definido de no utilización.

b) No se admitirá el uso de claves concertadas.

c) Se exigirá el uso de dispositivos físicos (tokens) personalizados o biometría.

d) En el caso de utilización de dispositivos físicos (tokens) se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

e) Se emplearán, preferentemente, productos certificados [op.pl.5]."

El Esquema Nacional de Seguridad establece que el mecanismo de autenticación de los sistemas debe estar regulado con exigencias distintas para los tres niveles de seguridad. Debido a que el Esquema Nacional de Seguridad exige restricciones distintas para cada uno de los niveles de seguridad existentes de la información, se desarrollará por separado cada nivel a lo largo de este apartado.

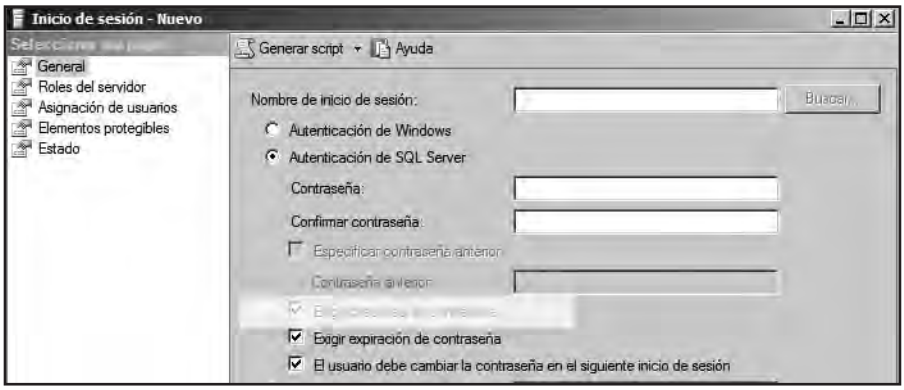
Nivel bajo

El ENS establece que en sistemas con nivel de seguridad de la información bajo, es válido cualquier mecanismo de autenticación, ya sean claves concertadas, certificados, mecanismos biométricos o cualquier otro tipo de autenticación basada en software o hardware.

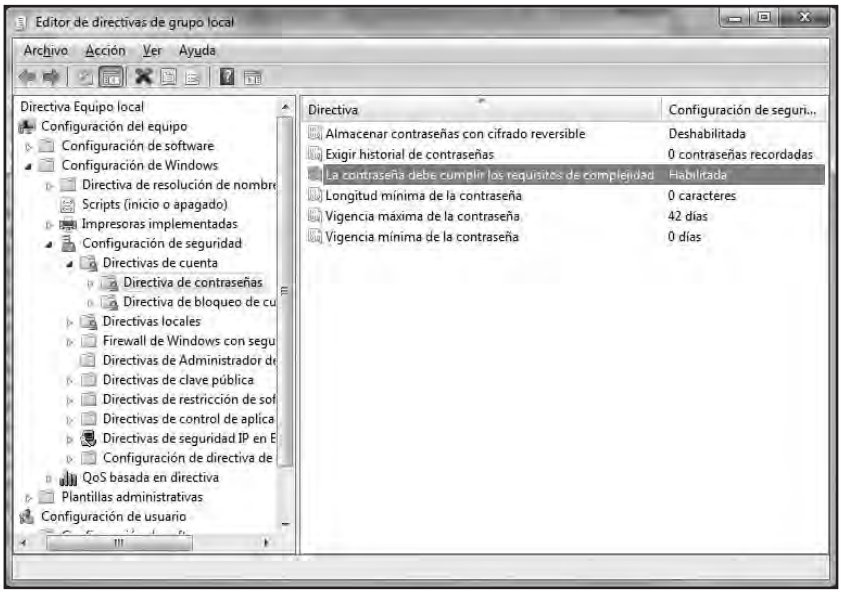
El Esquema Nacional de Seguridad establece unas restricciones mínimas en este nivel, independientemente del mecanismo de autenticación utilizado. Para un mejor entendimiento del cumplimiento de las restricciones se abordará uno de los mecanismos de autenticación, la clave concertada, para comprobar cómo los sistemas de Microsoft facilitan su cumplimiento.

El primer requisito que establece el ENS se refiere únicamente al mecanismo de clave concertada, ya que exige que las contraseñas cumplan reglas básicas de calidad. En este punto, es necesario diferenciar las credenciales, usuario y contraseña, de dominio, locales o de aplicación. Pero en cualquiera de los tres tipos de credencial los sistemas de Microsoft permiten el cumplimiento de esta restricción.

Todos los sistemas de Microsoft que permitan una gestión local de cuentas se integran con el sistema operativo para poder gestionar las restricciones a nivel de contraseñas de forma unificada.

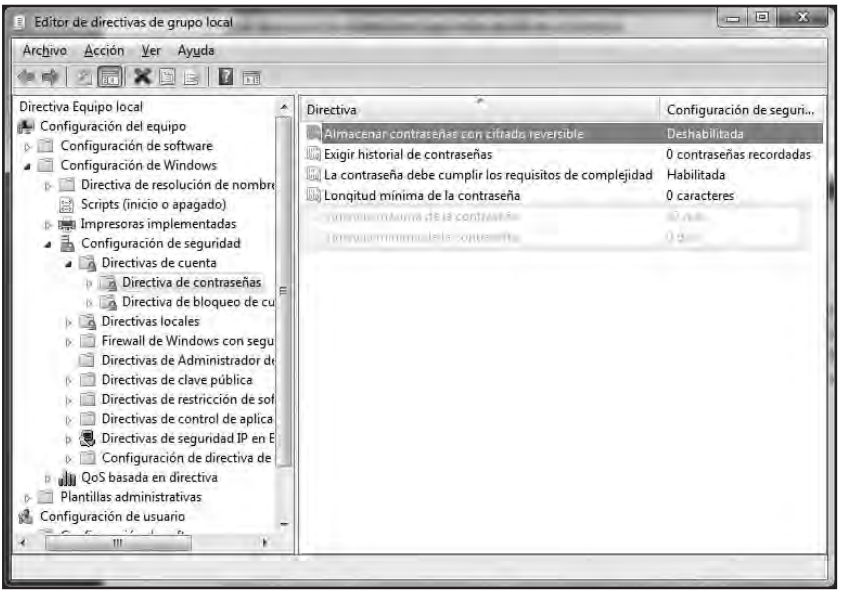


La configuración del sistema operativo para la restricción a nivel de contraseñas se realiza a través de directivas de seguridad, permitiendo su configuración desde las políticas locales o mediante políticas de grupo. Dentro de las directivas de seguridad se encuentra aquella que exige que las contraseñas cumplan determinados requisitos de complejidad ante cualquier cambio de contraseña, según exige el ENS.



El resto de restricciones son comunes a cualquier mecanismo de autenticación que se utilice. El Esquema Nacional de Seguridad exige que los autenticadores, es decir, las cuentas de usuario, se deban crear desactivados y los usuarios serán los únicos conocedores de las contraseñas. Las cuentas de usuario en los sistemas Windows deben ser creadas con la configuración que se muestra en la siguiente ilustración. La cuenta permanece deshabilitada hasta que el usuario la vaya a utilizar por primera vez, y tiene que cambiar la contraseña por una que sólo conozca él la primera vez que inicie una sesión en el sistema.

Las contraseñas deberán ser modificadas de forma obligatoria con una determinada periodicidad, que estará especificada por la política de la organización en función de la categoría del sistema. Para este objetivo los sistemas de Microsoft proporcionan unas directivas de seguridad que permiten configurar la vigencia mínima y máxima de las contraseñas, como se puede observar en la ilustración que aparece a continuación.



Cuando una cuenta de usuario deje de utilizarse, deberá ser deshabilitada pero no eliminada, por si fuese necesaria su posterior auditoría, tal y como se establece en el apartado de Identificación del Esquema Nacional de Seguridad.

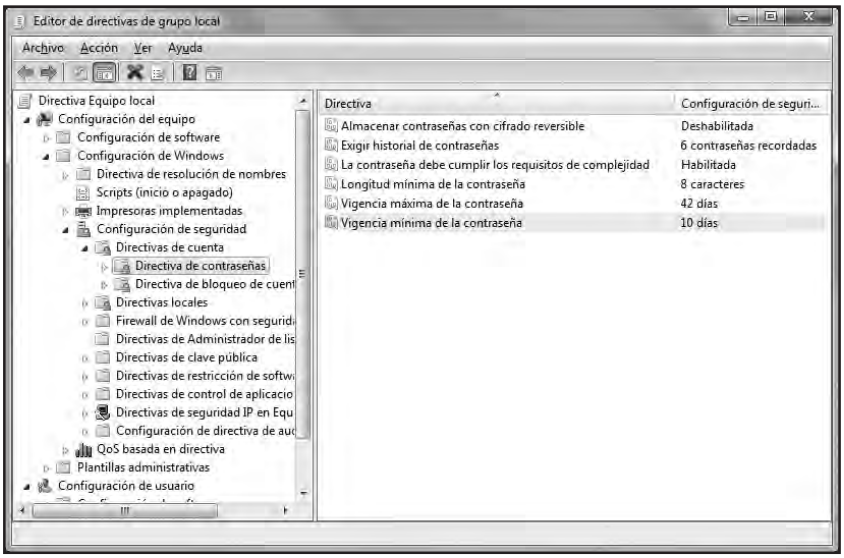
Nivel medio

A diferencia del nivel bajo, el ENS recomienda prescindir del uso de claves concertadas como mecanismo de autenticación en este nivel, pero en ningún caso queda prohibido. Si se decide hacer uso de claves concertadas, es estrictamente necesaria la utilización de políticas rigurosas de calidad y renovación de contraseñas. Dichas restricciones van dirigidas a utilizar:

- Contraseñas de longitud elevada, para evitar obtenerlas mediante mecanismos de fuerza bruta durante la vigencia de las mismas.
- Periodos no muy largos de renovación de las contraseñas. Se recomienda ajustar este tiempo en función de la longitud de la contraseña.
- Recordar las últimas contraseñas utilizadas por cada usuario para no poder volver a usarlas en un tiempo determinado.
- Establecer una vigencia mínima de la contraseña para evitar realizar cambios sucesivos hasta poder utilizar de nuevo la misma contraseña.

- Complejidad de la contraseña. Por supuesto, es necesario que las contraseñas de los usuarios cumplan unos mínimos de seguridad para así evitar descubrimientos no deseados de las mismas.

Todas estas opciones de configuración se pueden poner en práctica a través de las políticas locales de los sistemas operativos de Microsoft o a través de las políticas de grupo en Active Directory.



Los mecanismos de autenticación aconsejados para este tipo de nivel de seguridad de la información serían los siguientes:

- Dispositivos físicos (Tokens).
- Certificados.
- Biometría.

En este nivel se centrará la atención únicamente en el mecanismo de autenticación basado en certificados, ya que los otros mecanismos se abordarán en el siguiente nivel de seguridad, el alto. El uso de certificados ya se encuentra completamente integrado en los procesos de autenticación de los sistemas de Microsoft. A continuación se detallarán algunos ejemplos de los entornos donde usar certificados para la autenticación de los usuarios, Active Directory y Servidor Web.

Active Directory

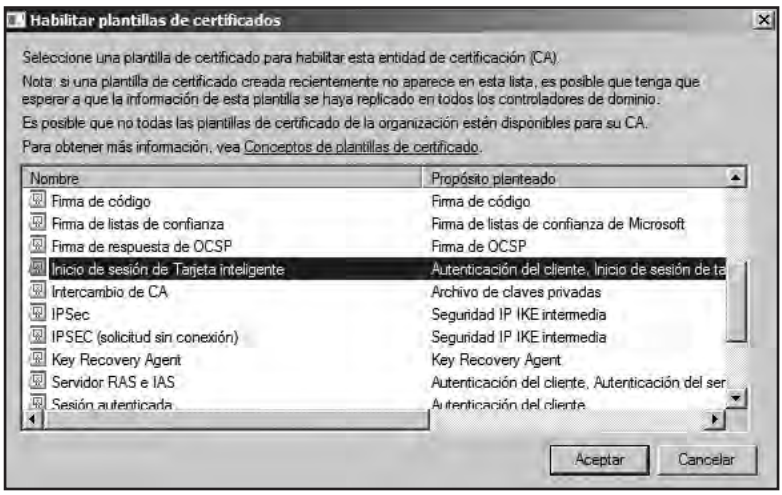
Windows Server 2008 R2 y Windows 7 son compatibles con el mecanismo de autenticación basado en certificados. En un entorno de dominio se puede autenticar a las entidades ante un proceso de inicio de sesión mediante certificados, pero siempre que estos estén almacenados en una tarjeta inteligente.

Este mecanismo también queda encuadrado en el método de autenticación basado en dispositivo físico.

A continuación se detallan los pasos más importantes para la puesta en marcha del mecanismos de autenticación basado en certificados en un entorno de Active Directory. Microsoft proporciona con Windows Server 2008 R2 la infraestructura completa para la puesta en marcha de la autenticación mediante tarjeta inteligente.

En primer lugar, es necesario contar con una colección de certificados que pueden ser generados a partir de una entidad de certificación externa a la compañía o una propia de la organización. Es posible utilizar el DNI-e para la autenticación de los usuarios. Para llevar a cabo este modo de autenticación se deben utilizar herramientas como SmartID Corporate Logon de SmartAccess.

La entidad de certificación de Windows Server 2008 R2, Active Directory Certificate Server, soporta la generación de los tipos de certificados necesarios para la autenticación. La entidad de certificación debe ser de empresa y la plantilla de certificado necesaria para la validación de entidades es Inicio de Sesión de Tarjeta Inteligente. Dicha plantilla no se encuentra operativa de forma predeterminada en las entidades de certificación, por lo que es necesario habilitarla.



La plantilla Inicio de sesión de Tarjeta Inteligente ya se encuentra operativa; por tanto, es el momento de emitir los certificados para cada uno de los usuarios que lo requieran. El procedimiento de emisión es muy sencillo, ya que nos permite emitir y almacenar el certificado sobre la tarjeta inteligente al mismo tiempo.

Para la emisión del certificado, el usuario debe acceder a la página web de inscripción de certificados, normalmente https://<nombre_servidor>/certsrv y realizar los siguientes pasos:

1. Acceder a la URL del portal web de inscripción de certificados.

2. Seleccionar la tarea Solicitar un certificado.
3. A continuación seleccionar Solicitud de certificado avanzada.
4. Y, finalmente, seleccionar Crear y enviar una solicitud a esta CA.
5. En la página de emisión de certificados, establecer la plantilla de certificado a Inicio de sesión de Tarjeta Inteligente.
6. Y establecer el valor del campo Proveedor de servicios de cifrado (CSP) a Microsoft Base Smart Card Crypto Provider.

7. Para la emisión del certificado pulsar enviar al final de la página
8. El sistema nos solicitará que se inserte la tarjeta donde se almacenará el certificado. Tras insertarla, el certificado se emite y almacena en la tarjeta inteligente.

Llegados a este punto, el usuario en cuestión ya posee el certificado necesario para un inicio de sesión basado en tarjeta inteligente. Ahora es el momento de configurar el entorno de trabajo del usuario, es decir, el equipo y la cuenta, para establecer el método de autenticación.

Los nuevos sistemas operativos de Microsoft, Windows Server 2008 R2 y Windows 7, soportan de forma predeterminada doble autenticación, método de clave concertada y certificados, al mismo tiempo. De este modo, se permite al usuario decidir el mecanismo de autenticación a utilizar cada vez que desee acceder al sistema.

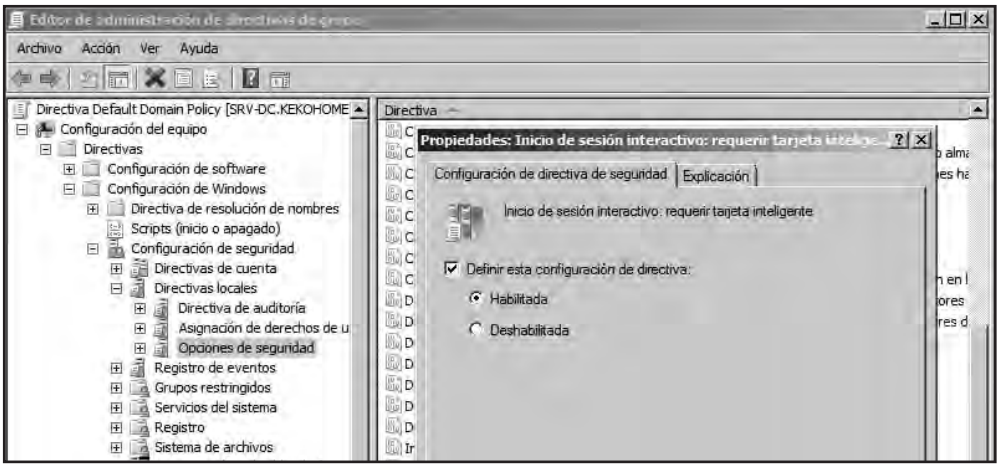
El comportamiento del sistema operativo se puede modificar para establecer el mecanismo de autenticación basado en tarjeta inteligente como único, para un usuario o equipo.

Para establecer que un usuario concreto debe iniciar siempre sesión a través de tarjeta inteligente, es necesario configurar su objeto de cuenta de usuario. Las cuentas de usuario de dominio tienen en sus propiedades un atributo que obliga a ello.

De este modo, el usuario, cuando vaya a iniciar sesión en cualquier equipo de la organización, necesitará presentar su tarjeta inteligente, ya que con su nombre de usuario y contraseña no será validado por un controlador de dominio.

Otra alternativa de configuración es establecer que a un equipo o equipos determinados sólo puedan acceder los usuarios que dispongan de una tarjeta inteligente con un certificado válido. Esta configuración se puede realizar a través de las políticas locales de la máquina o mediante las políticas de grupo.

En cualquiera de los casos, existe una directiva de seguridad con el nombre Inicio de sesión interactivo: requerir tarjeta inteligente en la Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad, que permite establecer como único mecanismo de inicio de sesión en el equipo la tarjeta inteligente.

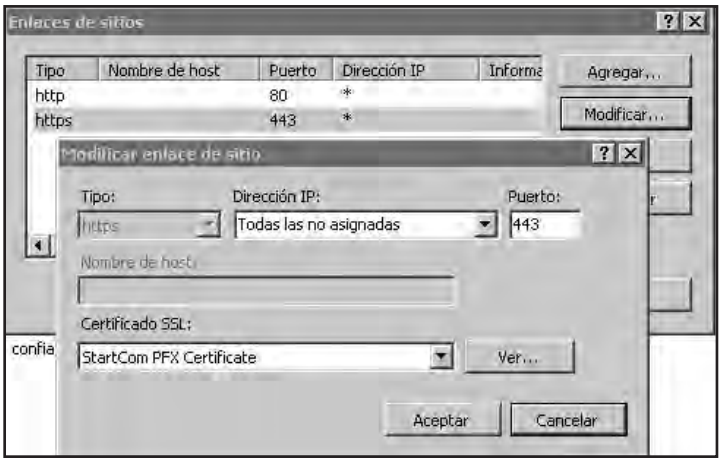


Servidor Web

Otro de los entornos más comunes en las organizaciones que requieren un inicio de sesión controlado porque manejan información confidencial son los servidores web. Windows Server 2008 R2 y Windows 7 cuentan con la capacidad de implementar una solución de servidor web basada en Internet Information Server (IIS), y ambos con la funcionalidad de autenticar a los usuarios basándose en certificados de cliente.

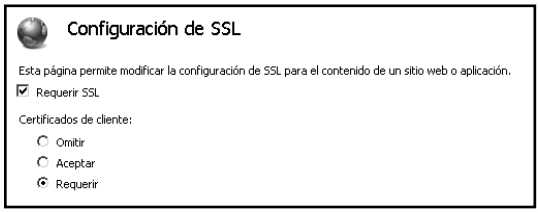
El mecanismo de autenticación que presenta IIS a nivel de certificados es un tanto peculiar, ya que va relacionado directamente con el protocolo de acceso HTTPS. Sólo cuando un sitio web está configurado para requerir el protocolo de acceso seguro basado en certificado, como se puede observar en la ilustración, es posible establecer la necesidad de presentar un certificado válido por parte del cliente (véase la figura superior de la página siguiente).

Este proceso de autenticación, o mejor dicho de validación del cliente, puede ser integrado con cualquier otro método de autenticación que soporte y requiera la



aplicación web. Los certificados en esta infraestructura se utilizan como un elemento más de autenticación, pero perfectamente válidos para el nivel de seguridad requerido por el ENS en cuanto al acceso a los servicios web de la organización.

Para habilitar el requisito de utilizar por parte del cliente un certificado de autenticación, es necesario configurar en el sitio web, aplicación virtual o directorio virtual la validación de cliente a través de SSL (*Secure Socket Layer*).



Una vez configurado el entorno web que requiere de la autenticación del cliente mediante certificados, cuando el cliente intenta acceder a dicho sitio web, el navegador solicita al usuario la selección de un certificado, almacenado en la máquina o en una tarjeta inteligente, para su validación en el servidor, como se puede observar en la siguiente ilustración

Nivel alto

El Esquema Nacional de Seguridad establece que los mecanismos de autenticación en los sistemas con información de nivel alto deben ser dispositivos físicos o biométricos. Además de esto, recomienda preferentemente la utilización de productos certificados por el Centro Criptológico Nacional.

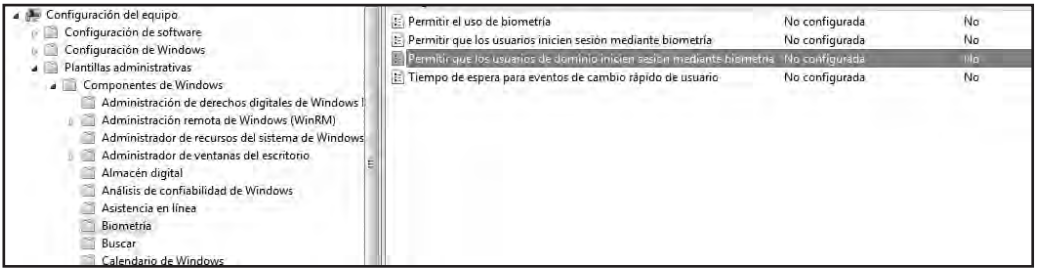
Para este nivel, Microsoft también proporciona funcionalidades que permiten dar cobertura a los requisitos establecidos por el ENS. Por ejemplo, los sistemas operativos de última generación, Windows Server 2008 R2 y Windows 7, proporcionan soporte nativo para dispositivos biométricos e incluyen un servicio de proveedor de credenciales.

A pesar de haberse abordado en el nivel anterior, el mecanismo de inicio de sesión mediante tarjeta inteligente es válido en este nivel, ya que proporciona un doble factor de autenticación solicitando un PIN, tras la inserción de la tarjeta.

Biometría

Con respecto a los dispositivos biométricos, Microsoft proporciona soporte nativo para la autenticación de usuarios a través de este tipo de dispositivos. Anteriores sistemas operativos de Microsoft ya soportaban la capacidad de iniciar sesión en ellos a través de dispositivos biométricos, como lectores de huella. Pero esto sólo era posible para inicios de usuario local, impidiendo la capacidad de utilizar este tipo de mecanismos de autenticación en entornos corporativos de Active Directory.

Windows 7 y Windows Server 2008 R2 proporcionan la capacidad de autenticar no sólo a usuarios locales de la máquina, sino que también a usuarios de dominio. Para la configuración del mecanismo de autenticación biométrico para cuentas de dominio, simplemente es necesario configurar, a través de políticas, una directiva como se puede observar en la ilustración que aparece a continuación. Esta directiva permite simplemente habilitar o deshabilitar la capacidad de autenticar cuentas de usuario de Active Directory a través de la biometría.



Los identificadores utilizados para la autenticación biométrica de los usuarios son gestionados por el software o el hardware utilizado para la lectura, por ejemplo la huella digital. Normalmente, dicho identificador queda almacenado en el equipo local, no permitiéndose su utilización en cualquier equipo del dominio. Para este fin

sería necesario utilizar dispositivos biométricos que usasen software que centralizase esos identificadores.

Proveedor de credenciales

Los proveedores de credenciales son la tecnología que extiende los mecanismos de autenticación de Microsoft. Se trata de la evolución de la antigua GINA o MSGINA (Microsoft Graphic Identification and Authentication). La nueva familia de sistemas operativos de Microsoft incorpora de forma nativa los proveedores de credenciales.

Los proveedores de credenciales proporcionan la capacidad de introducir a los sistemas operativos mecanismos de autenticación que se adapten a cualquiera de las necesidades que puedan existir ahora y en el futuro. Tiene la capacidad incluso de admitir fácilmente una autenticación multifactor, como puede ser sumar una autenticación biométrica a otra de tarjeta inteligente. Con ello se permite cumplir las exigencias del ENS en las situaciones más críticas.

Windows proporciona un servicio con el que interactúan estos proveedores de credenciales personalizados. El servicio se denomina Servicio de proveedor de credenciales. La existencia de éste permite a los desarrolladores del proveedor de credenciales preocuparse únicamente del mecanismo de autenticación, ya que del aspecto visual se encarga el propio sistema operativo. De este modo se facilita el uso de las nuevas credenciales a los usuarios, ya que el entorno de inicio de sesión no se verá alterado.

Con el objetivo de simplificar la tarea de elección del mecanismo de autenticación idóneo según el nivel de seguridad exigido por el Esquema Nacional de Seguridad, se introduce a continuación una tabla resumen con los mecanismos de autenticación admisibles.

		Nivel		
		Bajo	**Medio**	**Alto**
Algo se sabe	Clave	Sí	Con cautela	No
Algo que se tiene	Tokens	Sí	Sí	Criptográficos
Algo que se es	Biometría	Sí	Sí	Doble factor

6.1.6. Acceso local

"Se considera acceso local al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización. Estos accesos tendrán en cuenta el nivel de las dimensiones de seguridad:

Nivel BAJO

a) Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo. La información revelada a quien intenta acceder debe ser la mínima imprescindible (los diálogos de acceso proporcionarán solamente la información indispensable).

b) El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.

c) Se registrarán los accesos con éxito, y los fallidos.

d) El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

Nivel MEDIO

Se informará al usuario del último acceso efectuado con su identidad.

Nivel ALTO

a) El acceso estará limitado por horario, fechas y lugar desde donde se accede.

b) Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida."

El Esquema Nacional de Seguridad regula el nivel de seguridad a establecer ante cualquier tipo de acceso que se pueda producir dentro de las propias instalaciones de la organización. Para ello, el ENS establece exigencias diferentes para cada uno de los tres posibles niveles en que se pueden encontrar los sistemas.

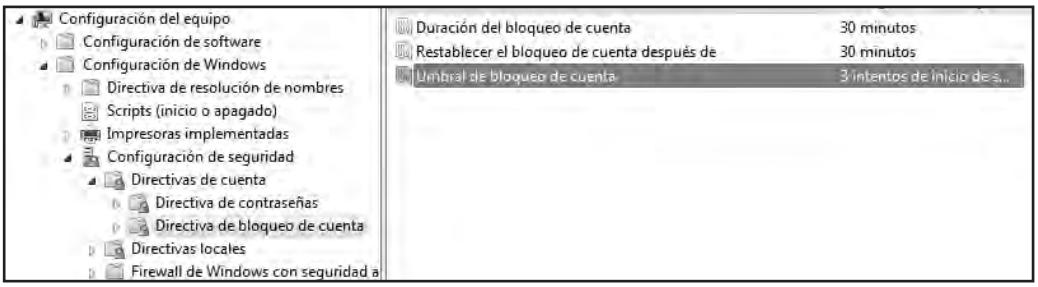
Nivel bajo

El primer requisito que se establece en este nivel es evitar en todo momento el acceso a la información sin un inicio previo. Este es uno de los grandes retos de la seguridad informática, porque los sistemas operativos proporcionan infinidad de mecanismos de seguridad, pero cuando éstos se encuentran iniciados. Pero, ¿podemos proteger la información cuando dicho sistema se encuentra en modo offline?

Este reto es posible resolverlo con los nuevos sistemas operativos de Microsoft y el nuevo hardware disponible. Por un lado, y gracias al avance del hardware, podemos controlar quién enciende físicamente un equipo a través de la tecnología TPM (*Trusted Platform Module*). Esta impide el arranque de la BIOS y, por tanto, del resto del hardware hasta introducir una clave, por teclado o dispositivo extraíble, desbloqueando tras ello el arranque de la BIOS.

Pero también tenemos otro tipo de funcionalidad, en este caso por parte del sistema operativo que impide la manipulación o acceso a la información mientras el sistema operativo se encuentra parado. Esta funcionalidad es Bitlocker, que permite el cifrado del disco impidiendo el acceso si no se proporciona previamente una clave, independientemente del estado del sistema operativo o si se estuviese accediendo a través de otro equipo. Esta tecnología se detalla más adelante en el apartado de protección de los soportes.

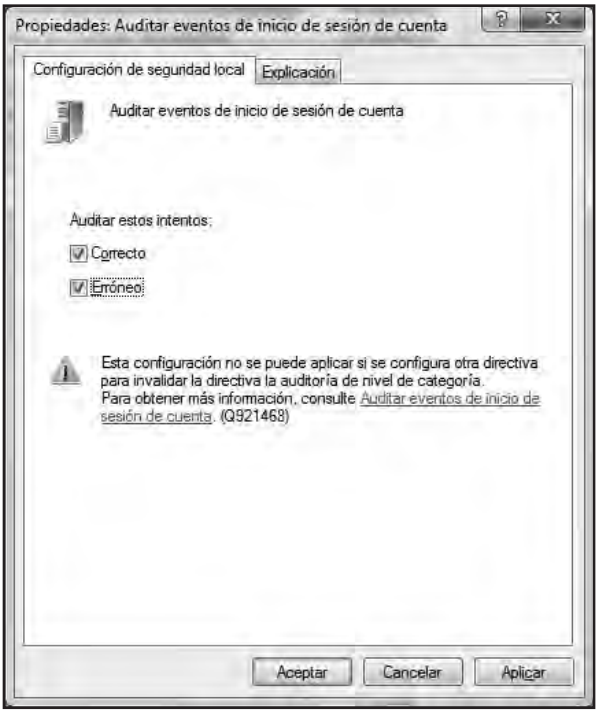
Otro de los requisitos del nivel bajo es la protección ante ataques de las cuentas de usuario. Para ello, se requiere que éstas se bloqueen tras un intento limitado de accesos erróneos. Windows 7 y Windows Server 2008 proporcionan, mediante directivas locales o políticas de grupo, la capacidad de bloqueo de cuentas por intentos erróneos de acceso.



La configuración de estas directivas se debe establecer en función de lo indicado por la política de la organización, aunque no se debería en ningún caso permitir más de 5 intentos erróneos.

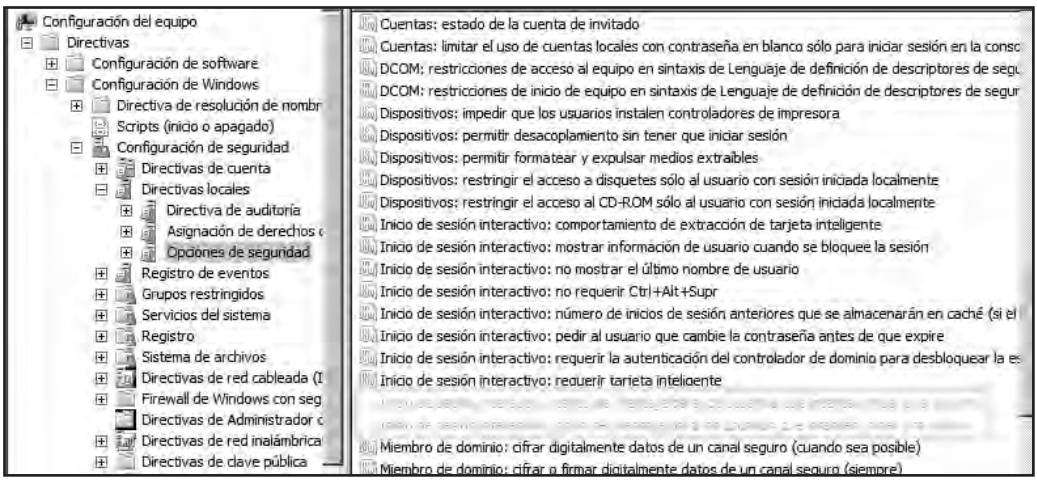
También otros sistemas servidor de Microsoft, como MS SQL Server, permiten la configuración de directivas que establezcan bloqueos de cuentas ante intentos de inicio de sesión erróneos. En este caso, MS SQL Server 2008 R2 proporciona la capacidad de establecer las mismas políticas de bloqueo de contraseña para sus inicios de sesión que las definidas en el sistema operativo.

El ENS también establece que el sistema deberá registrar todos los intentos de inicios de sesión, tanto los correctos como los erróneos. Para ello, Windows 7 y Windows Server 2008 R2 proporcionan la capacidad de auditarlos. Como se puede ver en la siguiente ilustración, mediante directivas locales o políticas de grupo, existe una directiva que se puede configurar para permitir la auditoria correcta y errónea de los inicios de sesión (véase la figura de la derecha).



Finalmente, el último requisito para el nivel bajo de acceso local es que se debe informar a los usuarios de sus obligaciones, inmediatamente después de obtener el acceso. Para este cometido Microsoft no proporciona una funcionalidad ya implementada, sino que suministra a través del proveedor de credenciales la capacidad de realizar este tipo de acciones.

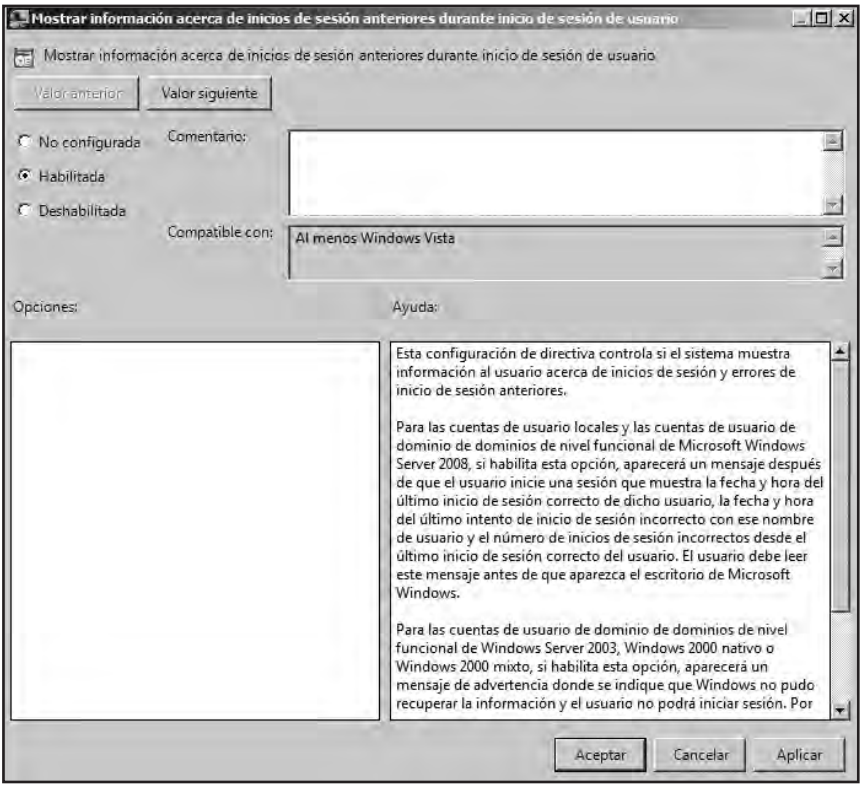
Existe una alternativa de forma directa, aunque no cumple al pie de la letra la norma del ENS, ya que la notificación se realiza al usuario antes de iniciar sesión. Para llevar a cabo esta configuración, se actúa en las directivas locales o políticas de grupo que se presentan en la siguiente ilustración.



Nivel medio

El nivel medio del Esquema Nacional de Seguridad establece que los usuarios deben ser informados tras su inicio de sesión de cuál fue el último inicio realizado con esa cuenta.

Windows 7 y Windows Server 2008 R2 proporcionan la capacidad de notificar a toda cuenta de usuario el último inicio de sesión correcto y el último erróneo.



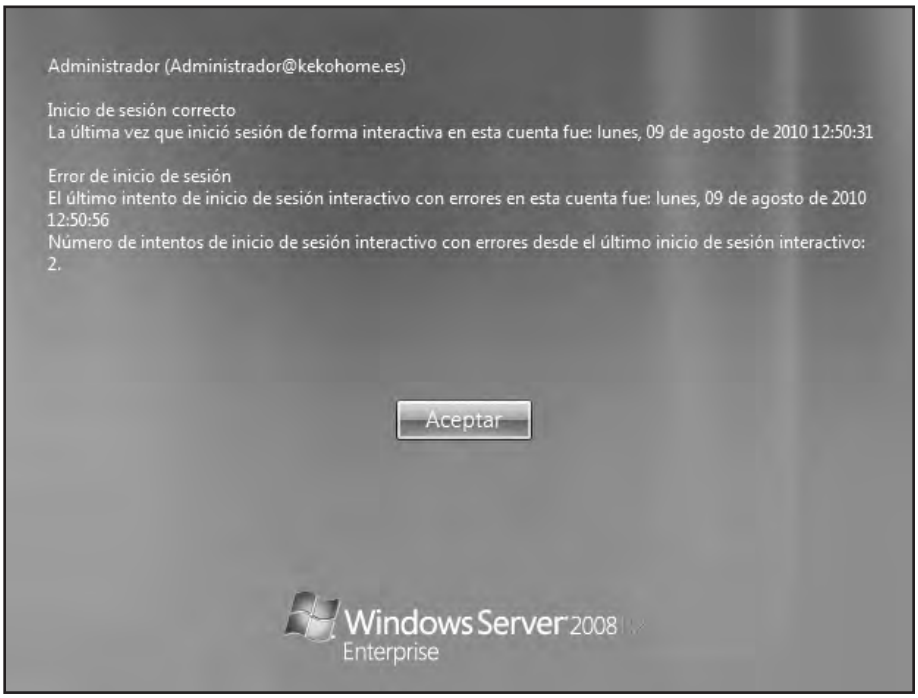
Tras la configuración de la directiva, cada vez que el usuario inicie sesión de forma correcta el resultado que éste verá es el que aparece en la primera ilustración de la siguiente página.

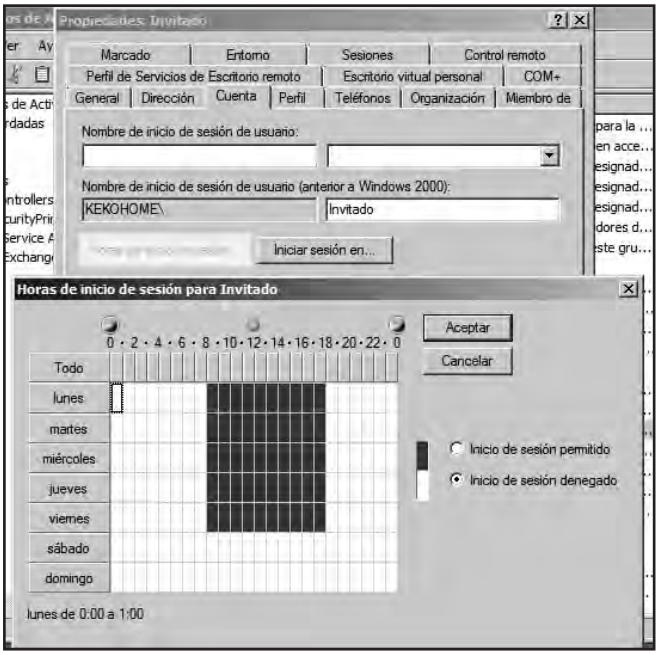
Nivel alto

En el nivel más alto que se establece en el ENS se requiere cumplir todos los requisitos de los niveles anteriores, más el cumplimiento que todos los usuarios tengan limitado el horario, fechas y lugar desde donde acceden a los sistemas.

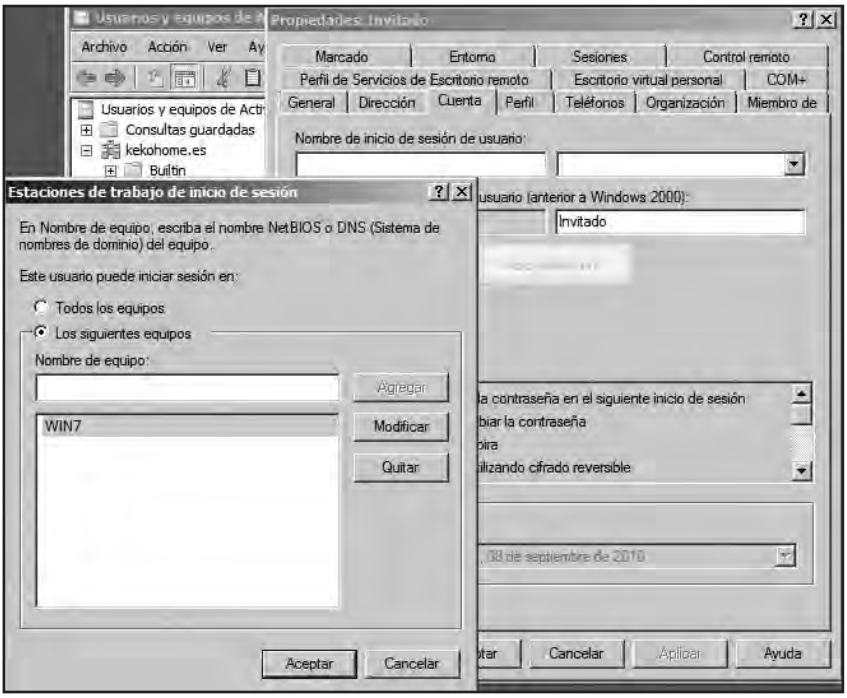
Para este cumplimiento es estrictamente necesario trabajar bajo el control de Active Directory, ya que en Windows Server 2008 R2 proporciona la capacidad de

establecer el horario de la semana en que cada usuario tendrá acceso al sistema. Esta configuración se establece a través de las propiedades de cada cuenta de usuario.





A través de las propiedades de cada cuenta de usuario, Active Directory también permite determinar en qué equipos miembros del dominio el usuario podrá acceder al sistema. Simplemente basta con agregar los equipos a los que tendrá acceso a la lista que aparece en la siguiente ilustración.



6.1.7. Acceso remoto

"Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros.

Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo (como [op.acc.6]) como el canal de acceso remoto (como en [mp.com.2] y [mp.com.3]).

Nivel MEDIO

Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva."

También quedan regulados por el Esquema Nacional de Seguridad los accesos que se realicen de forma remota sobre el sistema a través de redes de terceros. Para ellos el ENS diferencia las exigencias para cada uno de los dos niveles en que se pueden encontrar los sistemas.

Nivel bajo

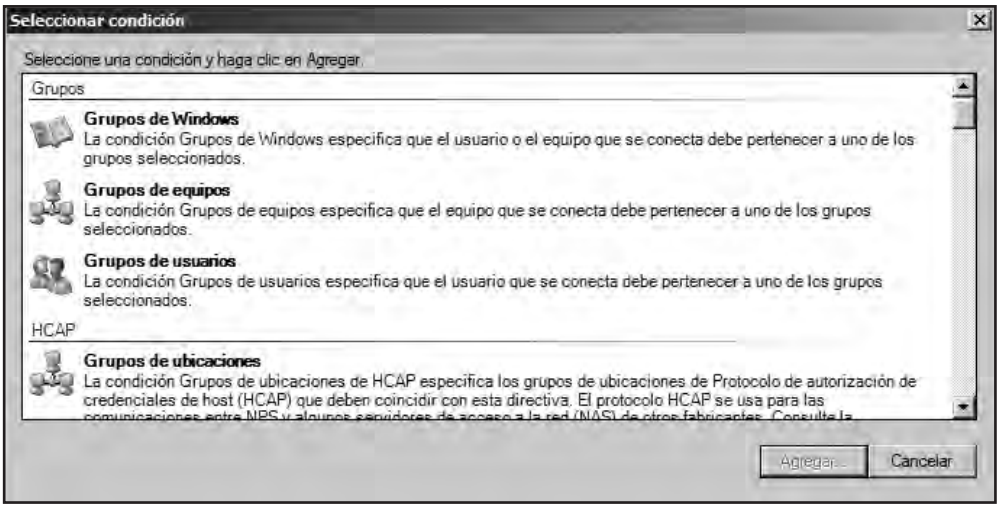
El cumplimiento del ENS en materia de acceso remoto implica la protección del acceso tal y como se establece también para el acceso local planteado en el apartado anterior. Se debe observar por otra parte lo establecido para el canal de acceso remoto en los términos de protección de confidencialidad y de la autenticidad e integridad, tratado en el apartado "Protección de las comunicaciones" de este manual.

Niveles medio y alto

Ante sistemas que requieran un nivel medio o alto en materia de acceso remoto, deberán cumplirse los requisitos establecidos en el nivel bajo, además de definir políticas específicas de acceso.

Para la generación de políticas específicas de acceso remoto de los usuarios, Microsoft incorpora una nueva funcionalidad en Windows Server 2008 R2 que es el Servidor de directivas de redes o NPS.

El servicio de acceso y políticas de redes se usa para administrar de forma centralizada el acceso a la red mediante varios servidores de acceso, como puntos de acceso inalámbricos, servidores VPN, servidores de escritorio remoto y conmutadores de autenticación 802.1x. Todo ello mediante la generación de políticas de red que proporcionan un control granular del acceso al sistema.



6.2. Explotación

Pertenecientes al marco operaciones, se incluyen entre las medidas las designadas para la explotación de los servicios. El Esquema Nacional de Seguridad define en ellas una serie de procesos tanto de control como de gestión que deberán llevarse a cabo por parte de todas las administraciones. Estas medidas son de diferente índole y se clasifican en los siguientes apartados:

- Inventario de activos.
- Configuración de la seguridad.
- Gestión de la configuración.
- Mantenimiento.
- Gestión de cambios.
- Protección frente a código dañino.
- Gestión de incidencias.
- Registro de la actividad de los usuarios.
- Registro de la gestión de incidencias.
- Protección de los registros de actividad.
- Protección de claves criptográficas.

Dichas medidas atienden a diferentes tareas que deben ser efectuadas por un departamento informático. Para su entendimiento y aplicación, en este libro se agrupan en función de sus objetivos: gestión y configuración de activos, protección y prevención frente a incidencias, y sistemas de registros y gestión de logs.

6.2.1. Gestión y configuración de activos

Uno de los problemas que se relacionan indirectamente con el de la seguridad, y no siempre es adecuadamente tratado por las organizaciones, es el del inventario de activos. Conocer lo que se posee es una necesidad de toda organización. Si no se realiza un inventario adecuado, difícilmente podrán proponerse medidas de seguridad proporcionales. Aunque se piensa normalmente en los servidores como parte fundamental de la prestación de un servicio, no es el único elemento que participa en la seguridad, tal y como se entiende en el ENS. Una estación de trabajo donde opera un trabajador de cualquier administración y pueda acceder a una base datos con información de ciudadanos, participa también en la seguridad general.

El Esquema Nacional de Seguridad exige medidas que permitan trabajar y conocer los activos de la entidad:

"Inventario de activos [op.exp.1].

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo."

Una brecha de seguridad en un sistema no controlado constituye un fallo significativo en la seguridad general. Un sistema de la organización que no cuente con antivirus o cortafuegos activos para el equipo puede poner en riesgo las infraestructuras a título general. Para la realización del inventario de activos la organización podría apoyarse en MS System Center Configuration Manager 2007 R2 (SCCM 2007). Tradicionalmente, dentro de las características aportadas por esta solución y sus antecesoras, las del inventariado de hardware y software son algunas de las fundamentales. Sirven además como parte de procedimientos posteriores, como el de análisis y gestión de licenciamiento o la distribución de software.

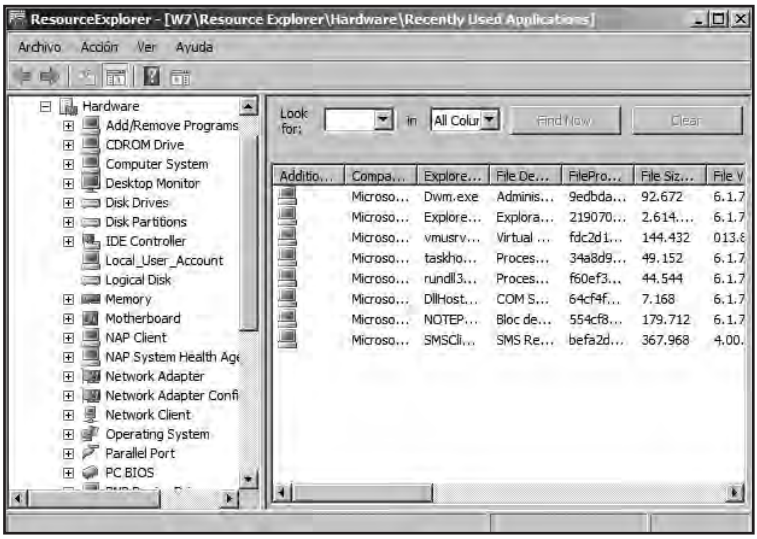


Figura 6.2.1. Explorador de recursos de SCCM 2007.

Sin embargo, con el paso del tiempo a esta solución se le han agregado otras características que pueden ser explotadas para el cumplimiento del Esquema Nacional de Seguridad. Los componentes de configuración deseada y Assest Intelligent que proporciona SCCM 2007 R2, permitirían una evaluación continua del estado de seguridad de los servidores y las estaciones de trabajo, marcando las pautas necesarias de qué es o no seguro, y estableciendo una métrica para ello. La seguridad desde este punto de vista podrá ser cuantificada.

Para ello, lo único que se requiere es definir los parámetros en cuanto a configuración deseada de seguridad: antivirus activo, configuraciones automáticas habilitadas, determinados servicios parados, cuentas administrativas controladas, etcétera. Formalmente, será la política de seguridad la que lo establezca. SCCM 2007 R2 aporta el resto de elementos necesarios para su funcionamiento: agentes, controles, parámetros e informes. La siguiente imagen muestra una visión general de una organización, donde se evalúa el cumplimiento de una serie de medidas por parte de algunos equipos de la organización.

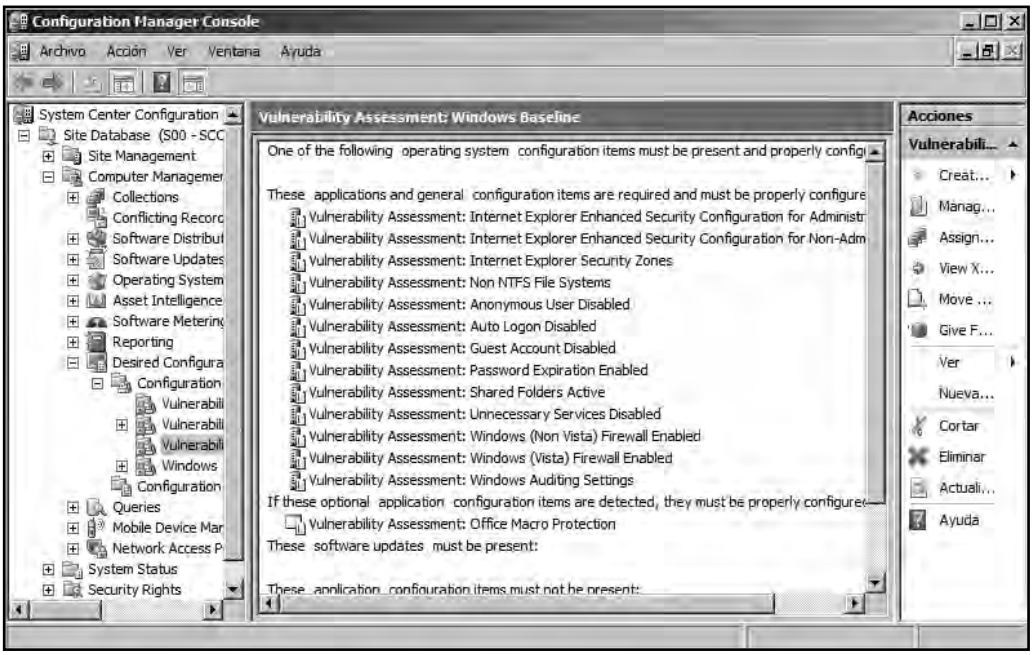


Figura 6.2.2. Análisis de configuración deseada en una organización.

La capacidad para dimensionar los roles en MS System Center Management Server 2010, permite el cumplimiento de segregación de funciones que marca el ENS. Los departamentos de explotación, con sus responsables correspondientes, podrían tener acceso a determinadas partes de la consola, mientras que el personal relacionado con la seguridad podría acceder a los elementos de configuración deseada y sus informes correspondientes. Las posibilidades que se aportan son múltiples y permiten un control absoluto del estado

de seguridad de una organización. De hecho, cubrirían perfectamente los objetivos previstos por otras de las medidas exigidas a nivel de operación.

"Configuración de la seguridad [op.exp.2].

Se configurarán los equipos previamente a su entrada en operación, de forma que:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplicará la regla de «mínima funcionalidad»:

1º El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad.

2º No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.

3º Se eliminarán o desactivarán mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.

c) Se aplicará la regla de «seguridad por defecto»:

1º Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.

2º Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.

3º El uso natural, en los casos en que el usuario no ha consultado el manual, será un uso seguro.

Gestión de la configuración [op.exp.3].

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

a) Se mantenga en todo momento la regla de «funcionalidad mínima» ([op.exp.2]).

b) Se mantenga en todo momento la regla de «seguridad por defecto» ([op.exp.2]).

c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).

d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).

e) El sistema reaccione a incidencias (ver [op.exp.7]).”

Las medidas anteriormente definidas tienen bastante relación con el primer elemento del inventariado. Si en primera instancia se necesita conocer qué hay, en una segunda se requiere su mantenimiento, tanto en configuración como en seguridad. Para ello, nuevamente MS System Center Configuration Manager ofrece funcionalidades para que estas tareas puedan ser llevadas a cabo con relativa comodidad.

Nuevamente, los sistemas de inventario, más la característica de configuración deseada, permitirían conocer el estado de seguridad de un sistema: analizando el estado

de los servidores, evaluando el número de administradores existentes, comprobando si ciertos servicios críticos se encuentran caídos o, por el contrario, si otros, que son potencialmente peligrosos, siguen desactivados. Para evaluar las posibilidades de uso con respecto a este componente, Microsoft desarrolló un paquete de funciones orientadas a la evaluación de criterios y seguridad, atendiendo a las normas de uso en materia de protección de datos que se establecen desde Europa. MS Windows Server 2003 Assessment Configuration Pack for European Union Data Protection Directive (EUDPD) proporciona una buena base para que los administradores de SCCM 2007 R2 puedan hacer uso de los mecanismos de configuración deseada, pudiendo ser ésta adaptada al cumplimiento del ENS.

Además, por las capacidades reactivas de esta suite, determinadas condiciones de seguridad que se hayan visto mermadas podrían ser reparadas, lanzando scripts a través de su plataforma de distribución de software. Para detener servicios determinados o para eliminar o crear usuarios, las posibilidades que se ofrecen son numerosas.

Las tareas de diseño y distribución de sistemas operativos a los sistemas clientes ocupan también un tiempo muy significativo de las tareas de un departamento de explotación. Dimensionar y mantener un importante número de estaciones de trabajo no es fácil, máxime cuando se tienen que plataformar muchas concurrentemente, preparando imágenes para su despliegue. Sin embargo, esta tarea de realizar instalaciones múltiples constituye una necesidad, puesto que si la labor a menudo rutinaria se realizara individualmente, los riesgos de seguridad planteados serían numerosos. Es preferible desviar muchos esfuerzos iniciales en crear una imagen de sistema operativo, con sus aplicaciones correspondientes, que sea segura y sólidamente probada, que no realizar instalaciones individuales que permiten incurrir en mayores fallos de seguridad.

Nuevamente, SCCM 2007 R2 presenta funcionalidades para el despliegue y gestión de nuevos sistemas operativos. A través de su módulo OSD (Operating System Deployment), se podrán crear imágenes generando secuenciaciones adaptativas, que podrán ser alteradas con el paso del tiempo. Por ejemplo, se genera de forma inicial una imagen, pero tras un tiempo en producción, se evalúa que ésta debe ser reajustada por unos fallos de seguridad que no fueron advertidos inicialmente. MS System Center Configuration Manager 2007 R2 proporciona mecanismos tanto para alterar el estado de la imagen y que sea desplegada en los nuevos sistemas ya reajustados, como para interactuar haciendo los cambios oportunos en los sistemas que ya se hubieran desplegado.

Para que las tareas de explotación puedan ser más dinámicas, Microsoft ha proporcionado una consola de gestión de datos de MS SCCM 2007 R2 integrada en MS SharePoint Server. Se trata de Configuration Manager Dashboard. De esta forma, los responsables correspondientes podrían acceder a la información reportada a nivel de seguridad tales como la gestión de actualizaciones, estado de salud y cumplimiento de normas de seguridad estipuladas por la organización. El acceso se realizaría a través de una interfaz web totalmente personalizada, con la disponibilidad de información en tiempo real.

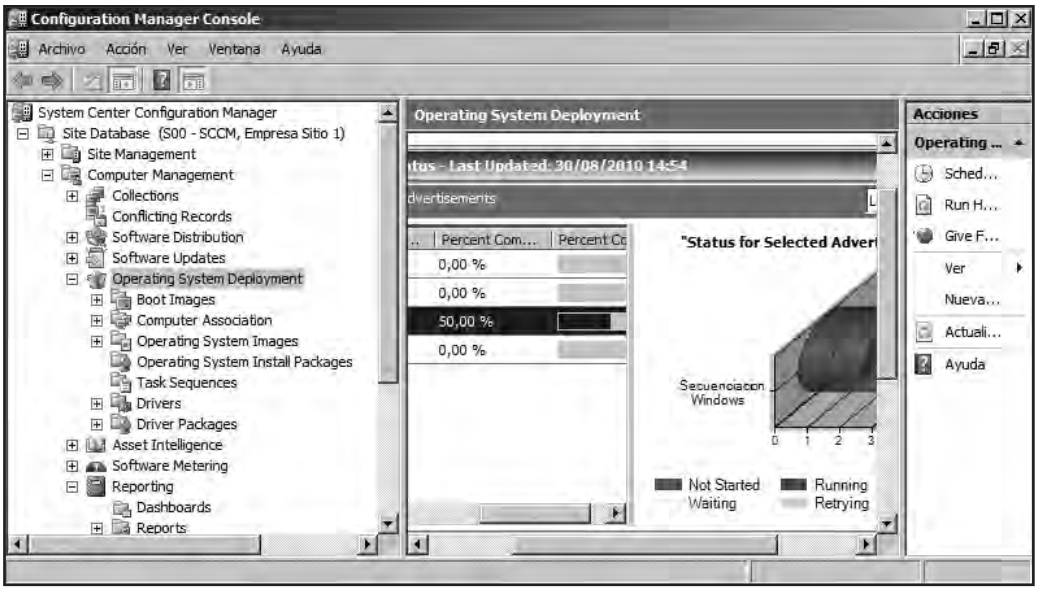


Figura 6.2.3. Módulo de despliegue de sistema operativo en SCCM 2007 R2.

Otro de los productos de reciente aparición y que ayudará al control y cumplimiento de las diferentes tareas de control es MS System Center Service Manager 2010. El objetivo fundamental de este servicio es minimizar los riesgos provocados por errores de configuración, ayudando a resolver incidencias rápidamente. Proporciona procesos integrados para el control de cambios y la resolución de incidentes y problemas. A través de su base de datos de administración de configuración (CMDB) e integración de procesos, conecta de manera automática conocimiento e información desde MS System Center Operations Manager, MS System Center Configuration Manager y los servicios de dominio de Directorio Activo.

Dentro de las tareas fundamentales que consigna el ENS para el mantenimiento evolutivo de la seguridad, la definición de procesos de mantenimiento es importante. Estos establecen todas aquellas tareas enfocadas a mantener la seguridad o la funcionalidad mediante la adopción de actualizaciones que debidamente haya comunicado el fabricante.

"Mantenimiento [op.exp.4].

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.

b) Se efectuará un seguimiento continuo de los anuncios de defectos.

c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización."

La gestión de actualizaciones atiende a dos naturalezas diferentes, la seguridad y la mejora de funcionalidades. A veces van de forma pareja, pero no necesariamente. La administración de actualizaciones es el proceso de control de la implementación y mantenimiento de las versiones de software provisionales en los entornos de producción. Ayuda a mantener la eficacia operativa, solucionar las vulnerabilidades de seguridad y mantener la estabilidad de un entorno de producción. Si una organización no puede determinar ni mantener un nivel conocido de confianza en sus sistemas operativos y software de aplicación, puede presentar varias vulnerabilidades de seguridad. Si se aprovechan, se puede producir la pérdida de beneficios y de propiedad intelectual. Para reducir esta amenaza, se debe disponer de sistemas configurados correctamente, usar el software más reciente e instalar las actualizaciones de software recomendadas.

Cuando Microsoft pone en marcha su iniciativa Trustworthy Computing (TC), uno de los efectos que se quería conseguir de forma más inmediata consistía en la reducción del tiempo en que una amenaza era efectiva por la existencia de una vulnerabilidad. El problema que se planteaba no era solamente que la solución existiera, sino que el canal de comunicación con el personal de TI y la gestión de las actualizaciones pudiera ser eficiente.

Años antes de la aparición de TC se había puesto en marcha un centro de sistemas de respuesta de seguridad denominado Microsoft Security Response Center (MSRC). Los esfuerzos conjuntos de este centro de respuestas, más las iniciativas que en materia de seguridad ha puesto en marcha Microsoft, han hecho posible a día de hoy reducir significativamente los expedientes de seguridad que afectan a los productos de Microsoft. El MSRC presenta dos objetivos fundamentales. En primer lugar, busca información de forma proactiva acerca de las vulnerabilidades del software, y luego proporciona avisos y actualizaciones de seguridad que abordan específicamente estas vulnerabilidades. En segundo lugar, monitoriza de forma constante un incidente de seguridad y responde rápidamente para ayudar a sus clientes a protegerse de las amenazas de seguridad cuando estas surgen. Una parte fundamental en esta misión consiste en la evaluación de los informes que los clientes proporcionan sobre posibles vulnerabilidades en los productos de Microsoft, y si fuera necesario, garantizar la preparación y divulgación de revisiones y boletines de seguridad que respondan a estos informes.

El MSRC publica un boletín para cada vulnerabilidad que pudiera, a juicio de Microsoft, afectar a los sistemas de múltiples clientes, independientemente de su alcance o probabilidad. No todas las vulnerabilidades afectan de igual modo a todos los usuarios y sistemas, pero en la medida de lo posible se ha generado un sistema de clasificación de gravedad denominado SRS (Severity Rating System). La clasificación establece los siguientes niveles:

- **Crítica.** Vulnerabilidad que puede permitir la propagación de un gusano de Internet sin la acción del usuario.
- **Importante.** Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
- **Moderada.** El abuso podría reducirse en gran medida mediante factores como una configuración predeterminada, auditoría o dificultad de abuso.
- **Baja.** Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Atendiendo a la gravedad de la vulnerabilidad, el personal de TI podrá identificar en qué medida un sistema presenta más o menos riesgo de seguridad, en caso de no estar correctamente actualizado. Cuando una vulnerabilidad es puesta en conocimiento del MSRC, independientemente de cuál sea su procedencia, se desencadena un proceso reglado para intentar determinar su gravedad y la solución a la misma. Todos los grupos de productos de Microsoft cuentan con un equipo de ingeniería de apoyo, que desarrolla las actualizaciones de software para los problemas localizados cuando el producto ya se ha lanzado. Una vez localizada una vulnerabilidad de seguridad, MSRC y los grupos de productos correspondientes evalúan y comprueban el problema. A continuación, el equipo de ingeniería de apoyo del grupo de productos crea y prueba una revisión de seguridad para solucionar el problema, mientras MSRC trabaja con quien detectó la vulnerabilidad para coordinar la publicación de información pública por medio de un boletín de seguridad que incluye los detalles de la revisión de seguridad.

Cuando la solución se encuentra disponible, hace público el expediente y proporciona la solución que en la mayoría de los casos corresponderá a una actualización de seguridad. Si por alguna circunstancia la publicación de un fallo se hace público sin el conocimiento de Microsoft, el proceso de investigación sigue procesos similares. No obstante, se podrían en estos casos recomendar soluciones temporales hasta que se ofrezca una solución final.

Pero en el ENS, no se habla solamente de seguridad en lo concerniente a mantenimiento. También es parte del proceso la evaluación continua para la mejora evolutiva en productos. En este sentido, Microsoft también hace un esfuerzo constante. Las revisiones de producto llevan habitualmente no sólo mejoras en rendimiento o soluciones de fallos descubiertos, sino que aportan nuevas funcionalidades para un producto determinado.

Adicionalmente a las actualizaciones de seguridad, los sistemas de gestión proporcionan otros tipos de actualizaciones:

- **Revisión de seguridad.** Corrección muy extendida para un producto específico, dirigida a una vulnerabilidad de seguridad. Con frecuencia se considera que una revisión de seguridad tiene una gravedad, que en realidad hace referencia a la clasificación de gravedad de MSRC de la vulnerabilidad a la que va dirigida la revisión de seguridad.

- **Actualización crítica.** Corrección ampliamente extendida para un problema específico, dirigida a un error crítico relacionado con la falta de seguridad.
- **Actualización.** Corrección muy extendida para un problema específico, dirigida a un error que no es crítico pero que está relacionado con la falta de seguridad.
- **Reparación.** Paquete simple que incluye uno o varios archivos utilizados para solucionar un problema de producto. Las reparaciones tratan situaciones específicas del cliente; sólo están disponibles a través de una relación de asistencia con Microsoft y puede que no se distribuyan fuera de la organización del cliente sin la autorización legal por escrito de Microsoft. Anteriormente se utilizaban los términos QFE (actualización de ingeniería de corrección rápida), revisión y actualización como sinónimos de reparación.
- **Conjunto de actualizaciones.** Conjunto de revisiones de seguridad, actualizaciones críticas, actualizaciones y reparaciones que se publican como una propuesta acumulativa o dirigida a un componente del producto. Permite la fácil implementación de varias actualizaciones de software.
- **Service Pack.** Conjunto acumulado de reparaciones, revisiones de seguridad, actualizaciones críticas y actualizaciones desde la publicación del producto y que incluye varios problemas resueltos que no se han puesto a disposición por medio de ninguna otra actualización de software. Los Service Pack también pueden incluir una cantidad limitada de características o cambios de diseño a solicitud de los clientes. Su distribución es muy amplia y Microsoft los prueba con más rigurosidad que cualquier otra actualización de software.
- **Service Pack integrado.** Combinación de un producto con un Service Pack en un único paquete.
- **Feature pack.** Nueva característica publicada para un producto que agrega una funcionalidad. Por lo general, se integra en el producto en su siguiente versión.

Para una mejor gestión de todo tipo de actualizaciones, Microsoft ha proporcionado por un lado herramientas, y por otro procedimientos de uso. Estos procedimientos permiten que los administradores de TI puedan planificar agendas de cara a la gestión de actualizaciones. Microsoft hace públicos sus expedientes y las actualizaciones los segundos martes de cada mes. Esto no es óbice para que en determinada circunstancia, y atendiendo a razones de criticidad, determinados expedientes puedan hacerse públicos fuera del ciclo habitual.

Para la gestión de las actualizaciones de todos los productos de Microsoft las organizaciones cuenta con dos soluciones en función del tipo de empresa y de las estrategias a plantear: MS Windows Server Update Services (WSUS) y MS System Center Configuration Manager. WSUS constituye la solución gratuita para la gestión estructurada de actualizaciones. Representa una solución perfecta para pequeñas y medianas organizaciones. Las grandes organizaciones ,sin embargo, requieren una

mayor flexibilidad que puede ser aportada por MS System Center Configuration Manager 2007 R2.

MS SCCM 2007 R2 proporciona un rol que se integra dentro de todas las funcionalidades que se proporcionan con la suite. Desde un punto de vista integral del análisis constituye la mejor referencia, máxime cuando se encuentra integrado con las soluciones de despliegue de los sistemas operativos, inventarios o configuración deseada entre otras.

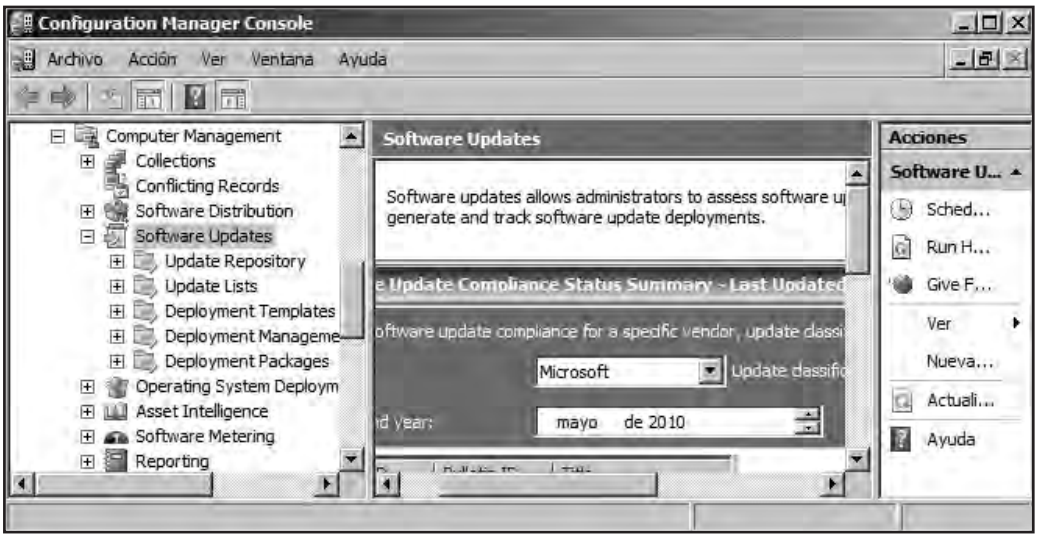


Figura 6.2.4. Gestión de actualizaciones con SCCM 2007.

Apoyado en el servicio de informes de MS SCCM R2 proporciona una completa información de estado y gestión de cambios de los equipos. Permite conocer el estado evolutivo de los equipos, manteniendo soluciones para deshacer un posible estado en caso de que no hubiera resultado conveniente. Esta medida constituye desde el punto de vista del ENS otra de las normas de seguridad a contemplar a partir del nivel de categoría media.

La plataforma de distribución de software de MS SCCM R2, independiente del módulo de gestión propio de actualizaciones, permitiría el despliegue de mejoras de cualquier producto existente en el mercado. Aunque para esta situación no ofrece el mismo control y requiere una intervención más manual, permitiría la homogeneización en los criterios de despliegue.

"Gestión de cambios [op.exp.5].

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.

b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.

c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.

d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación"

A veces, la aplicación de una actualización podría implicar que algún componente del servicio prestado pudiera fallar o perder parte de su funcionalidad. Con objeto de minimizar este impacto, deberá plantearse un sistema de control o pruebas que determine la eficacia de la aplicación de una actualización. Aunque las aplicaciones de Microsoft se presentan altamente testeadas, no se pueden evaluar todos los escenarios tan heterogéneos que es posible presentar con productos de terceros. Como plataforma de pruebas, los sistemas de virtualización constituyen el entorno ideal para la realización de los diferentes test. MS System Center Virtual Machine Manager constituye un sistema ideal en la integración de Hyper-V para la creación de escenarios de pruebas. La presentación a través del portal de autogestión con la asignación de roles, permite que diferentes departamentos o administradores puedan realizar los tests oportunos sobre entornos virtuales que emulen los escenarios reales. Para crear esta representación se pueden utilizar los mecanismos de virtualización de sistemas físicos. Esta solución permite no tener un sistema de pruebas similar al de producción, sino el mismo sistema de producción que virtualizado podrá ser utilizado como referencia para evaluar la funcionalidad de las diferentes actualizaciones.

6.2.2. Protección y prevención frente a incidencias

Dentro de las amenazas a las que se enfrenta una organización, las correspondientes al malware constituyen una de las más conocidas. Sin embargo, no siempre se plantean los mecanismos de protección más eficientes contra ella. El ENS es consciente de este hecho y plantea como obligatorio desde el nivel más básico contar con sistemas para bloquear sus acciones maliciosas.

"Protección frente a código dañino [op.exp.6].

Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como « spyware», y en general, todo lo conocido como «malware».

Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante."

La adquisición por parte de Microsoft de las compañías GeCAD Software Srly Sybaria tendía a una estrategia para asumir soluciones líderes en la lucha contra el

malware. La solución de GeCAD desembocó finalmente en las soluciones Security Essentials para entornos domésticos y MS Forefront Client Security (FCS) para empresas, que en el año 2010 evolucionó en MS Forefront Endpoint Protection 2010. El motor que incorporan estos productos ostenta unos grandes resultados en diferentes tests que realizan diferentes organizaciones.

En Av-comparatives, los estudios basados en análisis de heurística de comportamiento presentan este motor como uno de los mejores entre los analizados. En este análisis se utiliza una misma máquina en las mismas condiciones para todos los antivirus. Se provee a las soluciones de una firma correspondiente a un mismo día, pasando a ejecutar posteriormente diferentes tipos de malware que han hecho su aparición 10 días después de la firma a testear. Puesto que los diferentes antimalware no contarán con la firma para detectar los virus, deberán contar únicamente con sus sistemas basados en análisis de comportamiento para detectar la presencia del malware. El test persigue dos objetivos concretos, determinar el índice de acierto en detección y evaluar el número de falsos positivos que puede llegar a dar el antivirus. En el análisis de mayo de 2010 el motor obtenía la calificación más alta asignable en el cómputo final de los tests, con unos números altos en la detección proactiva sumados a un número muy bajo de falsos positivos.

Sin embargo, no todos son números y a estos hay que acompañarlos de un sistema de gestión coherente y proporcionado. Además, la gestión de alertas y la gestión de la seguridad frente a incidencias también cuenta para el ENS a partir del nivel medio.

"Gestión de incidencias [op.exp.7].

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

a) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y la protección de los registros según convenga al caso.

c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimientos para informar a las partes interesadas, internas y externas.

e) Procedimientos para:

1º Prevenir que se repita el incidente.

2º Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

3º Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias. La gestión de incidentes que afecten a datos de carácter personal

tendrá en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto."

A través de la consola de MS Forefront Client Security y la que vendrá integrada con System Center Configuration Manager 2007 R2 de MS Forefront Endpoint Protection 2010, los administradores de seguridad tendrán información en tiempo real de las incidencias que se den en sus sistemas. No sólo en lo relativo a problemas de malware, sino también de otras incidencias relacionadas con la seguridad. MS FCS y FEP incluyen también un componente para el control de la seguridad en los equipos y permite evaluar fallos existentes en los mismos que puedan provocar brechas de seguridad en las organizaciones.

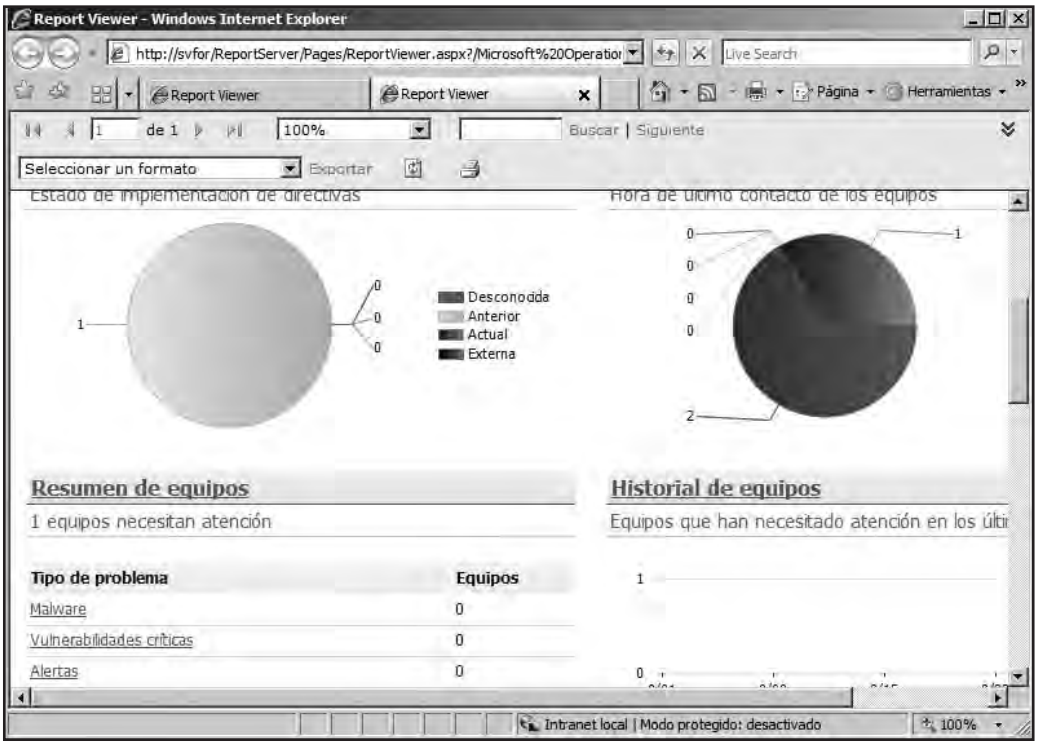


Figura 6.2.5. Gestión de riesgos con MS Forefront Cliente Security.

A través de la consola de administración puede implementarse un sistema de gestión de alertas eficiente. Podrán conocerse los riesgos a los que se enfrenta la organización y notificarlos adecuadamente al personal correspondiente.

Sin embargo, las soluciones antimalware que pueden disponer las organizaciones, van más allá de las que se disponen sobre los sistemas operativos. A través de las soluciones de protección para correo electrónico, de gestión de contenido o de

defensa perimetral, la organización puede expandir los mecanismos de protección contra el malware. MS Forefront Protection for Exchange 2010, MS Forefront Protection for SharePoint 2010 y MS Forefront Threat Management Gateway 2010, aportan funcionalidades para la protección en múltiples escenarios. La labor combinada de todos proporciona cotas de defensa altísimas, sumando las capacidades multimotor de los sistemas MS Forefront Protection a la gestión, segmentación y control de tráfico que aporta MS Forefront TMG 2010.

La centralización de toda la información a través de MS System Center Operation Manager, con los Management Pack correspondientes para cada producto, permite una visión global de la seguridad. De esta forma, se entiende la seguridad centralizada de productos, y una capacidad para ofrecer reacciones ante amenazas e incidencias.

6.2.3. Sistemas de registros y gestión de logs

La trazabilidad de un sistema constituye una necesidad para evaluar las potenciales incidencias que ha sufrido una entidad. Pero también la facultan como defensa en un caso judicial, donde se requieran unas evidencias que demuestren un potencial ataque o acto malintencionado efectuado por alguno de sus empleados. Los registros son esenciales para la resolución de conflictos y aportan datos suficientes para arrojar luz sobre situaciones de difícil solución. Sin embargo, los sistemas de registro no son exigidos en todos los escenarios de servicios de la Administración Pública. Sólo serán preceptivos en la categorización alta o media. Las dos primeras medidas que se citan a continuación sólo se deberán tener en cuenta en servicios categorizados con el nivel más alto.

"Registro de la actividad de los usuarios [op.exp.8].

Se registrarán todas las actividades de los usuarios en el sistema, de forma que:

a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.

b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.

c) Deben registrarse las actividades realizadas con éxito y los intentos fracasados.

d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se determinará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1])."

"Protección de los registros de actividad [op.exp.10].

Se protegerán los registros del sistema, de forma que:

a) Se determinará el periodo de retención de los registros.

b) Se asegurará la fecha y hora. Véase [mp.info.5].

c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.

d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos."

Los sistemas operativos que proporciona Microsoft cuentan con un sistema de registro de actividades. Recogen diferentes tipos de eventos relativos al registro de Windows accesibles a través del Visor de Sucesos en formato de auditoría. El establecimiento de estas auditorías se lleva a efecto a través de las directivas de seguridad. Las auditorías que se realizan a nivel de sistema presentan dos posibilidades:

- Una auditoría correcta es aquella que emite resultados satisfactorios cuando se han cumplido todas las condiciones para que el hecho se pudiera dar. Por ejemplo, un usuario que elimina un fichero puesto que tenía los permisos correspondientes para poder hacerlo.
- Una auditoría errónea es aquella que emite resultados cuando no se dan las condiciones establecidas. Por ejemplo, se producirá una auditoría errónea cuando un usuario intente eliminar un fichero para el cual no tenía permiso.

Los últimos sistemas operativos incorporan el nuevo sistema de eventos, MS Windows Eventing 6.0, que permite una mejora para la gestión de eventos de seguridad y establecer mecanismos de correlación para los mismos. Entre los elementos destacados, MS Windows Eventing presenta una nueva consola, permitiendo la generación de vistas personalizadas y un texto descriptivo mejorado. El sistema de MS Windows Eventing 6.0 basa su funcionalidad en un motor de xml, lo que permite una mayor escalabilidad y accesibilidad. Almacenar la información en formato xml permite que soluciones particulares puedan acceder a dicha información aprovechando las características y la potencia del sistema en xml.

Al establecer las auditorías a través de las directivas, se especifican una serie de categorías para determinar diferentes evaluadores en lo referente a la seguridad, de tal forma que se debe plantear si necesitamos o no habilitar las auditorías correctas y erróneas para cada una de las circunstancias que se pudiesen producir. Estas son las diferentes categorías que referencian auditorías:

- Inicio de sesión.
- Inicio de sesión de cuenta.
- Administración de cuentas.
- Acceso a objetos.
- Accesos del servicio de directorio.
- Usos de privilegios.
- Seguimiento de procesos.
- Sucesos del sistema.
- Cambio de directivas.

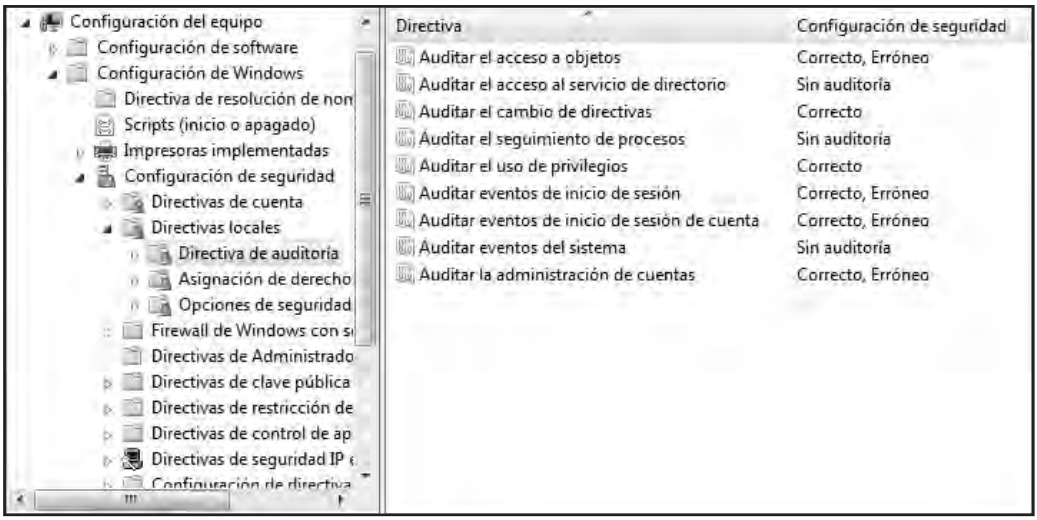


Figura 6.2.6. Configuración de auditoría de seguridad.

Sin embargo, estas auditorías presentan un sistema de granularidad que permite subdividir y activar diferentes subcategorías. Se trata de las directivas de auditoría granular (GAP). Este sistema permite sobre todo filtrar la información importante de la que no lo es limitando la cantidad de información recibida a la estrictamente necesaria. Las diferente subcategorías en las que han quedado definidas las categorías principales son:

- Sistema.
  - Cambio de estado de seguridad.
  - Extensión del sistema de seguridad.
  - Integridad del sistema.
  - Controlador IPsec.
  - Otros eventos de sistema.
- Inicio/cierre de sesión.
  - Inicio de sesión.
  - Cerrar sesión.
  - Bloqueo de cuenta.
  - Modo principal de IPsec.
  - Modo rápido de IPsec.
  - Modo extendido de IPsec.

- Inicio de sesión especial.
- Otros eventos de inicio y cierre de sesión.
- Servidor de directivas de redes.

- Acceso de objetos.
  - Sistema de archivos.
  - Registro.
  - Objeto de Kernel.
  - SAM.
  - Servicios de certificación.
  - Aplicación generada.
  - Manipulación de identificadores.
  - Recurso compartido de archivos.
  - Filtrado de paquetes.
  - Filtrados de conexión.
  - Otros eventos de acceso a objetos.
- Uso de privilegios.
  - Uso de privilegio confidencial.
  - Uso de privilegio no confidencial.
  - Otros eventos de uso de privilegio.
- Seguimiento detallado.
  - Creación del proceso.
  - Finalización del proceso.
  - Actividad DPAPI.
  - Eventos de RPC.
- Cambio de plan.
  - Cambio en la directiva de auditoría.
  - Cambio de la directiva de autenticación.
  - Cambio de la directiva de autorización.
  - Cambio de la directiva del nivel de reglas de MPSSVC.

    - Cambio de la directiva de Filtering Platform.
    - Otros eventos de cambio de directivas.
- Administración de cuentas.
    - Administración de cuentas de usuario.
    - Administración de cuentas de equipo.
    - Administración de grupos de seguridad.
    - Administración de grupos de distribución.
    - Administración de grupos de aplicaciones.
    - Otros eventos de administración de cuentas.
- Acceso Servicio de Directorio.
    - Acceso del servicio de directorio.
    - Cambios de servicio de directorio.
    - Replicación del servicio de directorio.
    - Replicación del servicio de directorio detallada.
    - Inicio de sesión de la cuenta.
    - Validación de credenciales.
    - Operaciones de vales de servicio Kerberos.
    - Otros eventos de inicio de sesión de cuentas.
    - Servicio de autenticación Kerberos.

Atendiendo a las necesidades del ENS, de la auditoría de usuarios y especialmente de los operadores y administradores del sistema, se estima como necesaria la activación de las auditorías sobre los siguientes elementos:

- Inicio de sesión.
- Inicio de sesión de cuenta.
- Administración de cuentas.
- Acceso a objetos.
- Usos de privilegios.
- Cambio de directivas.

¿Qué sistemas deberían verse afectados por las mismas? Esto dependerá de las condiciones y escenarios planteados por la organización. En el caso de contar con una

infraestructura de Active Directory, deberían establecerse en todos los controladores de dominio. Pero también los de inicio de sesión y uso de privilegios en todos aquellos servidores que proporcionen soporte a los servicios. En el caso de los servidores de ficheros deberían establecerse también las relativas al acceso a objetos.

Para una información más detallada de todos los registros podrá remitirse a la información que con respecto al mismo puede encontrar en el artículo referenciado en la siguiente dirección URL.

http://support.microsoft.com/kb/947226/es

Pero no solamente el sistema operativo presenta sistemas de registro. Los diferentes servicios que aportan la infraestructura Microsoft cuentan con sus propios sistemas de registro: MS Internet Information Server, MS SQL Server, MS Exchange Server, MS SharePoint Server o los productos MS Forefront proporcionan registros que arrojarán información de interés sobre situaciones críticas.

Toda esta información podrá ser utilizada en casos forenses, permitiendo dilucidar problemas que puedan derivar en acciones judiciales o administrativas, tal y como determina otra de las medidas establecidas en el ENS.

"Registro de la gestión de incidencias [op.exp.9].

Se registrarán todas las actuaciones relacionadas con la gestión de incidencias, de forma que:

a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

b) Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

c) Como consecuencia del análisis de las incidencias, se revisará la determinación de los eventos auditables."

El problema al que se enfrentará la organización es cómo consolidar y catalizar cada uno de ellos. Para ello, el rol de Auditor Colector System (ACS) de MS System Center Operation Manager 2007 R2 podría ser de una ayuda significativa. ACS servirá a las organizaciones para consolidar registros de seguridad individuales en una base de datos administrada centralmente. Permite también filtrar los eventos generados. Pero también proporciona la capacidad para la correlación de logs al permitir el análisis de datos y proporcionar herramientas para la generación de informes a través del servicio de reporting de MS SQL Server. La seguridad que proporciona ACS faculta que sólo un usuario que haya recibido específicamente el derecho para tener acceso a la base de datos de ACS, puede ejecutar consultas y crear informes sobre los datos recopilados. Esto permite la segregación de funciones y la protección de los registros, manteniendo altos períodos de retención de los registros.

Para la implementación y funcionalidades de ACS intervienen tres componentes:

- **Reenviadores de ACS.** Incluido en el agente de Operation Manager de los servidores sujetos a recopilación de información, recogerá los diferentes eventos locales que se hayan establecido.
- **Recopilador de ACS.** Este servicio será el encargado de recibir y procesar todos los eventos que remitan los diferentes reenviadores. Tras procesarlos se enviarán los datos a la base de datos de ACS. Este proceso incluye el desensamblado de los mismos con el fin de incluirlos en varias tablas en la base de datos de ACS. Con ello, se consigue minimizar la redundancia de datos, así como aplicar filtros para que no se almacenen eventos innecesarios.
- **Base de datos de ACS.** La base de datos de ACS es el repositorio central para eventos que se generan a partir de una directiva de auditorías en una implantación de ACS.

La idea fundamental de trabajo es que los agentes en los servidores o estaciones de trabajo correspondientes recuperarán los registros del sistema. Estos serán enviados a los recopiladores correspondientes. Este hecho marca un proceso transcendental puesto que desde este momento, éstos quedan totalmente aislados de la persona que administra el servidor, y aunque éste los eliminara intencionadamente se mantendría una copia de los mismos en el servidor de recopilación. Se desvía de esta forma el procedimiento de retención de logs de los servidores al servicio de ACS, que al ser manejados en una base de datos permite que se haga de forma más eficiente.

Los recopiladores serán los encargados de tratar la información recibida. Podrán cribar o tratar adecuadamente los registros en base a los parámetros que se establezcan, por ejemplo dimensionarlos más adecuadamente de cómo se originan en sus sistemas respectivos. Para ello se realiza un tratamiento de normalización para su almacenamiento en la base de datos. El objetivo es que al emplear mecanismos de correlación y generación de informes, éstos sean adecuados y no generen discrepancias en su tratamiento.

Las últimas de las medidas que se exigen a nivel de explotación corresponden a la protección de claves criptográficas. Aunque se enuncia a continuación lo que se expresa en lo concerniente a explotación, los sistemas de cifrado se tratarán específicamente en páginas posteriores del libro. Solamente tener en cuenta de forma preceptiva los procedimientos exigidos en la siguiente medida para categorías baja y media o alta.

"Protección de claves criptográficas [op.exp.11].

Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.

Categoría BÁSICA

a) Los medios de generación estarán aislados de los medios de explotación.

b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Categoría MEDIA

a) Se usarán programas evaluados o dispositivos criptográficos certificados.

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional."

6.3. Protección de los equipos

Tal y como se ha expresado a lo largo del libro, la seguridad en su concepto general afecta a la totalidad de los sistemas. El Esquema de Seguridad Nacional recoge, a través de sus medidas, la necesidad de proteger de igual forma servicios e información. También las estaciones de trabajo y los puestos de trabajo se encuentran supeditadas a la norma y son atendidos por ésta de forma expresa.

No hay que olvidar que muchas de las acciones enfocadas al tratamiento de los datos y los servicios se realizan desde estaciones de trabajo. La administración de los servidores, el acceso a bases de datos o la gestión de usuarios, entre otras, son acciones habituales que se realizan desde ellas. Son frecuentemente un punto vulnerable dentro de la escena de seguridad, por lo que merecen un tratamiento especial y así se recoge en el ENS.

Es cierto que determinados aspectos fundamentales, como los procesos de autenticación o las comunicaciones, son acciones importantes que se inician desde los equipos. En las medidas previstas como marco de protección en el Esquema Nacional de Seguridad, las relativas a equipos son las siguientes:

- Puesto de trabajo despejado.
- Bloqueo del puesto de trabajo.
- Protección de portátiles.
- Medios alternativos.

La primera de las medidas persigue dos objetivos fundamentales: garantizar un uso eficiente de los medios disponibles y proteger frente a incidencias el material físico utilizado para el cumplimiento de las funciones del personal. Las medidas previstas en el Esquema Nacional de Seguridad para la protección de equipos desde este punto de vista, difieren en función del nivel de criticidad de la organización, y son las siguientes:

"5.3.1 Puesto de trabajo despejado [mp.eq.1].

Categoría BÁSICA

Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento

Categoría MEDIA

Este material se guardará en lugar cerrado cuando no se esté utilizando."

Sin embargo, las medidas de protección van más allá de lo puramente físico. La protección del equipo se debe extender más allá del momento en que el usuario se encuentra sentado en su puesto de trabajo y operando con el equipo. Cuando una persona deja su equipo y éste tiene su sesión iniciada, almacena y mantiene de forma activa mecanismos que pueden permitir que otra persona acceda a datos que de otra forma no estarían a su alcance. Bien mediante los mecanismos de Single Sign On o de autenticación integrada, las credenciales almacenadas en un equipo permitirían el acceso a portales o aplicaciones internas, servicios de ficheros, y otros elementos críticos.

Eso sin contar con el hecho habitual de que los usuarios de los equipos, por cuestiones de comodidad, hayan almacenado o hagan uso de la función recordar credenciales proporcionada por el sistema. Abandonar el equipo sin la debida protección podría implicar un acto de imprudencia y, por ello, el ENS exige el cumplimiento de medidas. Si el usuario no tiene capacidad de previsión, el sistema deberá hacer dicha tarea automáticamente en aquellos sistemas de categoría media o alta.

"Bloqueo de puesto de trabajo [mp.eq.2].

Nivel MEDIO

El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Nivel ALTO

Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo."

Los sistemas operativos a través de las directivas de seguridad de Windows proporcionan mecanismos para el cumplimiento de estas medidas. Como ya se ha comentado, cuando se habla de sesiones hay que tener en cuenta que éstas pueden ser de dos tipos:

- Autenticación local.
- Autenticación en red.

En ambas circunstancias, el abandono del equipo sin haber cerrado la sesión permitiría que ésta, bien sea local o iniciada en red, permaneciera abierta. Las siguientes directivas permiten bloquear o suspender sesiones de ambos tipos.

Para poder bloquear una sesión local, se habilita el protector de pantalla del escritorio. Cuando se activa el salvapantallas, la sesión se bloquea automáticamente y su recuperación exige la introducción de credenciales para que se desbloquee. La Figura 6.3.1 muestra el lugar donde localizar dicha directiva.

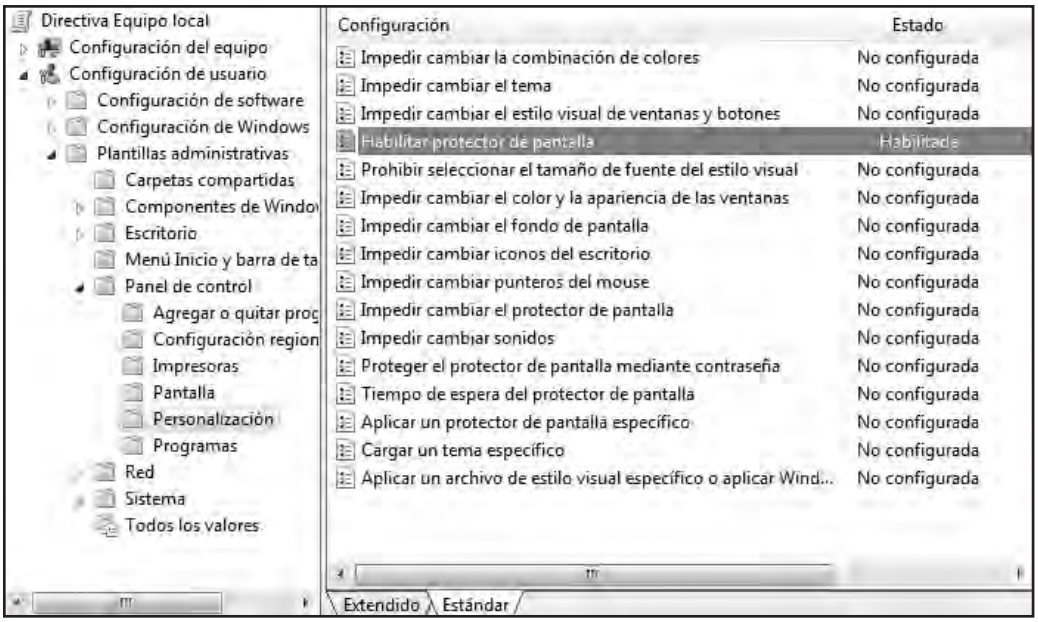


Figura 6.3.1. Directiva para habilitar el protector de pantalla.

Si se deshabilita esta configuración, no se podrán establecer contraseñas para los protectores de pantalla y se deshabilita la sección Protector de pantalla del cuadro de diálogo Configuración del protector de pantalla. En consecuencia, los usuarios no podrán cambiar las opciones establecidas para el protector de pantalla.

Si se habilita, se ejecutará un protector, siempre que se cumplan dos condiciones:

- Que un protector de pantalla válido en el cliente se establezca mediante la opción Nombre del archivo ejecutable del protector de pantalla o mediante el Panel de control en el equipo cliente.
- Que el tiempo de espera del protector de pantalla se establece en un valor diferente de cero mediante la configuración o a través del Panel de control.

Para impedir que esta acción pueda ser alterada localmente, se podrá activar también la opción de Impedir cambiar el protector de pantalla. En el caso de la sesiones de red, podrán activarse las siguientes directivas correspondientes al equipo.

Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión. Esta configuración de seguridad, determina si se va a desconectar a los usuarios conectados al equipo local fuera de las horas de inicio de sesión establecidas para su cuenta de usuario. Afecta al componente Bloque de mensajes del servidor (SMB).

Cuando se habilita esta directiva, fuerza la desconexión de las sesiones de cliente con el servicio SMB cuando las horas de inicio de sesión del cliente expiren. Si se deshabilita esta directiva, se permite mantener una sesión de cliente establecida una

vez expiradas las horas de inicio de sesión del cliente. La Figura 6.3.2 muestra el lugar donde se encuentra dicha directiva.

Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión. Esta configuración de seguridad determina el período de tiempo de inactividad continuo que debe transcurrir en una sesión del Bloque de mensajes del servidor (SMB) para que ésta se suspenda por falta de actividad.

Los administradores pueden usar esta directiva para controlar cuándo suspende el equipo una sesión SMB inactiva. Si la actividad del cliente se reanuda, la sesión se restablecerá automáticamente. En la configuración de esta directiva, el valor 0 equivale a desconectar la sesión inactiva tan pronto como sea razonablemente posible. El valor máximo es 99999, que equivale a 208 días. En la práctica, este valor deshabilita la directiva. De forma predeterminada, los valores especificados son de 15 minutos para los servidores y sin definir para las estaciones de trabajo.

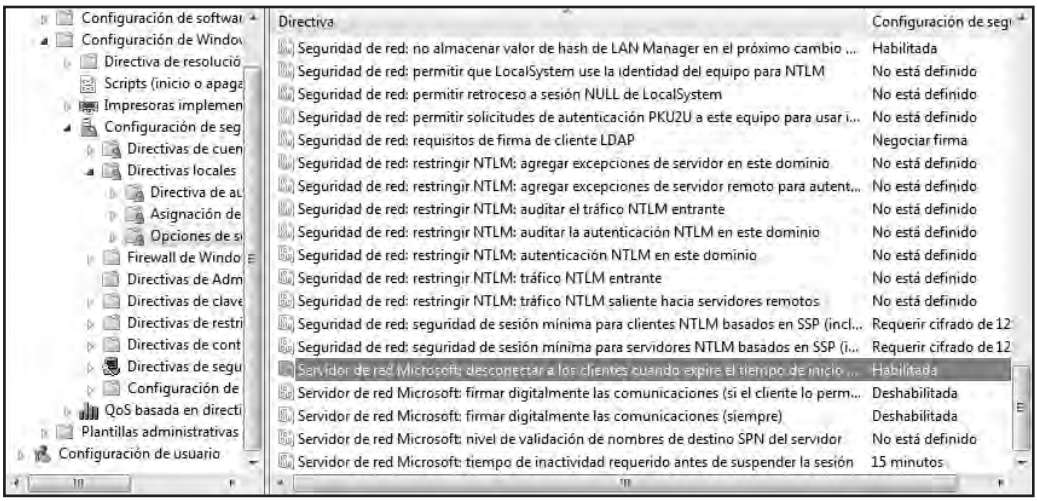


Figura 6.3.2. Directiva para la desconexión de clientes cuando expire la hora de inicio de sesión.

Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión. Esta configuración de seguridad determina si se desconecta a los usuarios conectados al equipo local fuera de las horas de inicio de sesión válidas de la cuenta de usuario. Esta configuración afecta al componente Bloque de mensajes del servidor (SMB). Cuando se habilita esta directiva, fuerza la desconexión de las sesiones de cliente con el servidor SMB cuando las horas de inicio de sesión del cliente expiren. Si se deshabilita esta directiva, se permite mantener una sesión de cliente establecida una vez expiradas las horas de inicio de sesión del cliente.

La seguridad establecida a través de esta directiva funciona como una de tipo cuenta. Para las cuentas de dominio, sólo podrá existir una directiva de tipo cuenta. Ésta se debe definir por lo tanto a través de la directiva de dominio predeterminada y la exigen los controladores de dominio que forman el dominio. Los controladores de

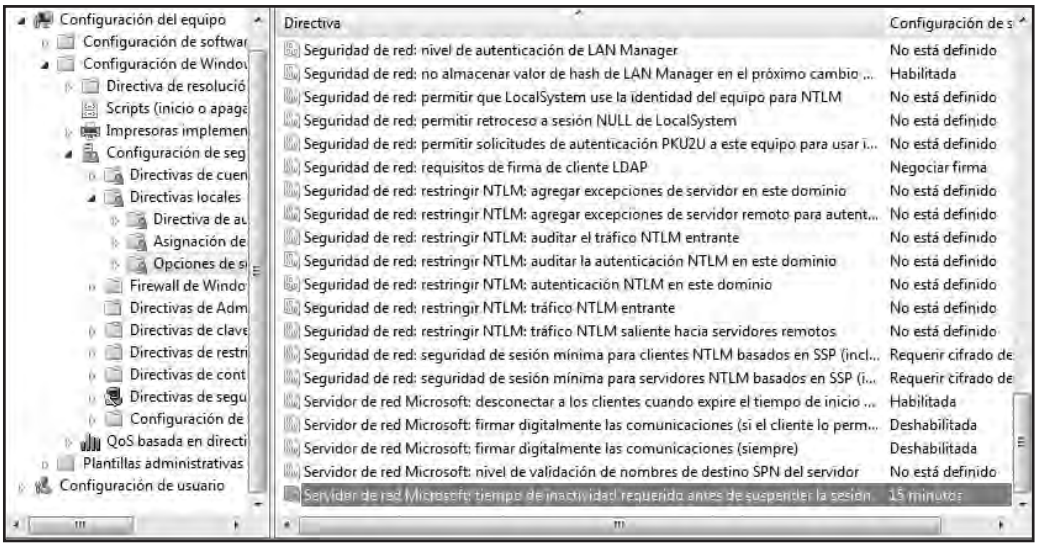


Figura 6.3.3. Directiva que establece el tiempo de inactividad antes de suspender una sesión.

dominio siempre extraen la directiva de cuenta del objeto de directiva de grupo (GPO) de la directiva de dominio predeterminada, incluso si hay una directiva de cuenta diferente aplicada a la unidad organizativa que contiene el controlador de dominio. De manera predeterminada, las estaciones de trabajo y los servidores unidos a un dominio, por ejemplo equipos miembros, también reciben la misma directiva de cuenta para sus cuentas locales. La configuración de Kerberos no se aplica a los equipos miembros.

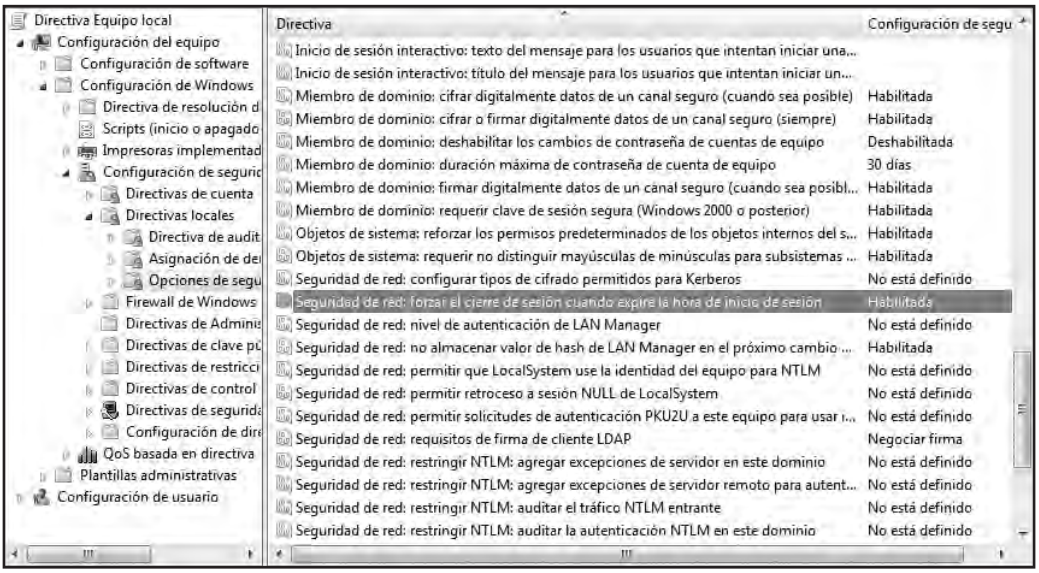


Figura 6.3.4. Directiva para forzar el cierre de sesión cuando expire la hora de inicio de sesión.

En relación con los sistemas de uso de servicios integrados en Directorio Activo, hay que tener también presente lo relativo al uso de Tickets Kerberos. Estos se utilizan para acceder a los servicios de la organización que utilicen Kerberos como mecanismo de identificación. Deberán establecerse también valores para limitar su uso más allá de un tiempo establecido para las siguientes circunstancias:

- Vigencia máxima de Tickets de usuario.
- Vigencia máxima de renovación para Tickets de usuario.
- Vigencia máxima de Tickets de servicio.

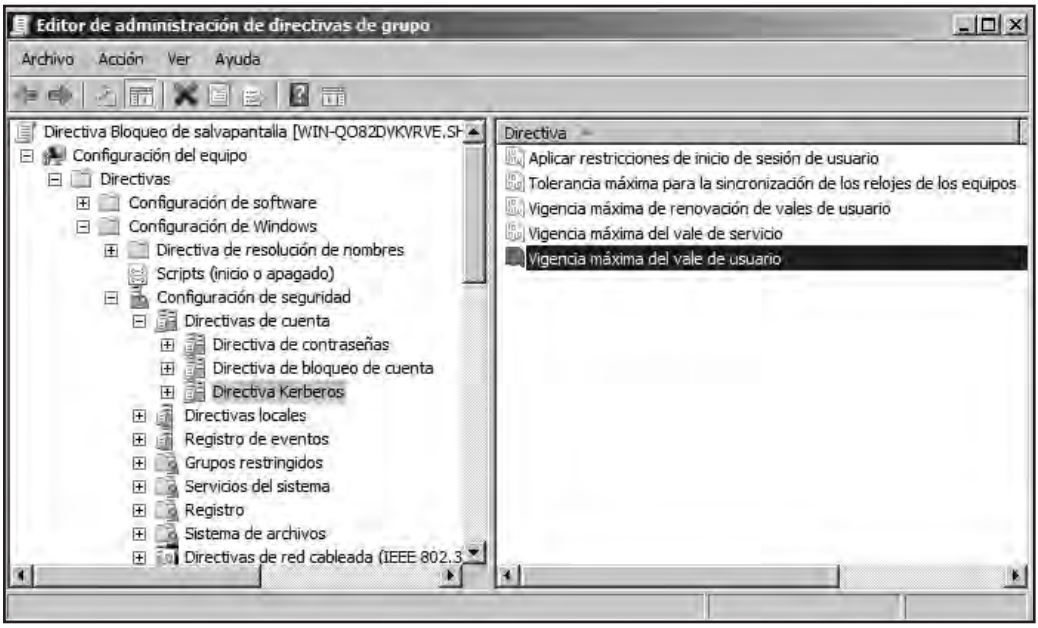


Figura 6.3.5. Gestión de las vigencias máximas de uso de los Tickets Kerberos.

Para una mejor aplicación de las directivas en infraestructura de Directorio activo, podrá hacerse uso de los objetos de política de grupo. Esto permitirá un mejor control a la hora de aplicarlas, permitiendo configuraciones diferentes en función de las necesidades y las políticas estipuladas por la organización. No todos los equipos y usuarios seguramente cuenten con las mismas prerrogativas, y aplicar las políticas desde el dominio, a través de su estructura lógica, permitirá una mayor eficacia en la gestión.

En lo que respecta a la protección de los equipos un aspecto crítico es aquel que afecta a los equipos portátiles. Aunque la seguridad involucra a todos los elementos de una organización, deberán cuidarse especialmente aquellos dispositivos que salgan fuera de sus instalaciones. Los equipos portátiles han aportado una movilidad necesaria, pero hace imprescindible extender la seguridad más allá del área de administración típica de una organización.

No hay más que fijarse en la posibilidad de que un equipo pueda ser extraviado, robado, o bien que sea utilizado en entornos de dudosa confianza. Si este equipo contuviese información crítica de una organización, ésta se encontraría expuesta a ataques alternativos que de otra forma no hubieran sido factibles: por ejemplo, si el usuario mantiene un fichero de uso de claves de acceso a la organización en su escritorio. Aunque no se conociesen las credenciales de acceso al equipo, un arranque de tipo offline con un Live-CD permitiría acceder a la información existente en el mismo.

Puesto que no se puede garantizar una seguridad física, se promueve el uso de medidas alternativas para garantizar la seguridad de los datos.

"Protección de portátiles [mp.eq.3].

Categoría BÁSICA

Los equipos que abandonen las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

a) Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

b) Se establecerá un canal de comunicación para informar, al servicio de gestión de incidencias, de pérdidas o sustracciones.

c) Se establecerá un sistema de protección perimetral que minimice la visibilidad exterior y controle las opciones de acceso al interior cuando el equipo se conecte a redes, en particular si el equipo se conecta a redes públicas.

d) Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

Categoría ALTA

a) Se dotará al dispositivo de detectores de violación que permitan saber si el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incidente.

b) La información de nivel alto almacenada en el disco se protegerá mediante cifrado."

Para garantizar la seguridad de los sistemas internos, se requieren procedimientos y medidas que pongan en conocimiento las incidencias que afecten a los dispositivos móviles. Entre ellos, mecanismos de notificación que permitan que una persona que sufra un incidente relacionado con la pérdida o robo de un equipo portátil pueda comunicarlo oportunamente.

En las conexiones en lugares tales como hoteles, aeropuertos o zonas Wi-Fi, la conexión a la sede implica la implantación de mecanismos que garanticen una conexión cifrada. Los medios que a menudo se ofrecen en estos escenarios son inalámbricos. Aun cuando se proporcionen sistemas basados en clave para su acceso, WEP (Wired Equivalent Privacy) o WPA (Wi-Fi Protected Access), éstos no ofrecen la seguridad oportuna. Un potencial atacante que se encontrara en la misma red Wi-Fi, y que conozca la clave correspondiente de acceso a ella, podría robar información de los datos en tránsito.

Para evitar este hecho podrían emplearse mecanismos de acceso basados en redes virtuales privadas (VPN) o portales seguros de gestión de acceso. En el caso de las redes VPN, las premisas son:

- **Conexión que establezca un tunneling.** Para ello, se realizará un túnel lógico, entre el origen y el destino. Esto permite una comunicación segura entre redes privadas a través de redes públicas como Internet. El establecimiento de dicho túnel puede realizarse en diferentes capas de la conexión.
- **Conexión encapsulada.** El encapsulamiento va a permitir que diferentes tipos de protocolos y servicios puedan ser encaminados a través de una red pública como puede ser Internet.
- **Conexión cifrada.** El intercambio de datos entre los extremos se cifrará garantizando la privacidad de los mismos.
- **Conexión autenticada.** Para impedir que la conexión sea realizada por cualquiera, la conexión podrá ser autenticada a nivel de usuario.

En el ámbito Microsoft, varios son los servicios que permiten proporcionar conexiones de tipo VPN:

- Sistema operativo servidor como Windows Server 2008 R2, a través de sus roles de acceso remoto y su servidor de políticas de red.
- Microsoft Forefront Threat Management Gateway 2010.
- Microsoft Forefront Unified Access Gateway 2010.

Aunque los tres mecanismos son válidos para establecer conexiones de tipo VPN, los dos últimos ofrecen garantías alternativas para el establecimiento de la conexión segura. Microsoft Forefront TMG 2010 integra la solución de VPN dentro de las características de firewall que proporciona. Entendida desde el soporte multired, garantiza el control de tráfico entre la red de VPN y las diferentes redes a las que da soporte de infraestructura. (Véase la Figura 6.3.6.)

No sólo se garantiza el acceso seguro, sino que éste, y en función del usuario, se permitirá o denegará el acceso al resto de redes y servicios de la organización. En esta circunstancia y de forma predeterminada, mientras el usuario tenga activa la conexión VPN, cualquier acceso a Internet se realizará a través de la misma. Esto garantiza un aislamiento de la conexión, impidiendo que de forma concurrente el cliente VPN esté

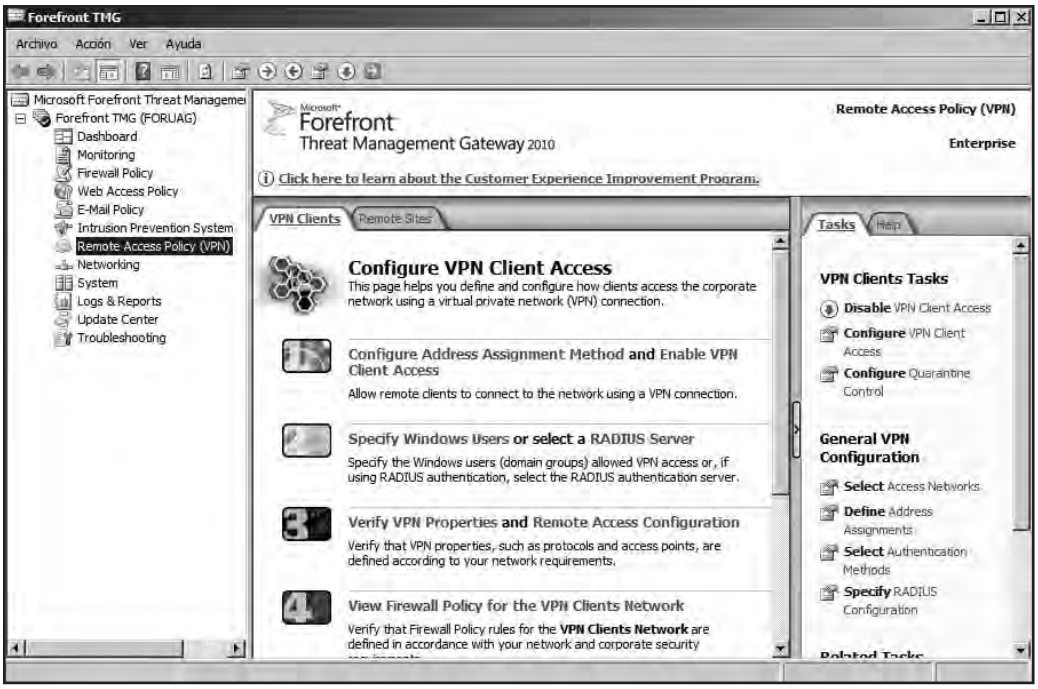


Figura 6.3.6. Configuración de la conexión de clientes VPN en MS Forefront TMG 2010.

conectado a la red del sistema interno e Internet. Se evita así que se convierta en un puente de conexión que no tendría por qué estar debidamente controlado.

MS Forefront UAG 2010 ofrece conectividad a través de un portal de acceso a servicios de la organización. Los mecanismos de seguridad adicionales ofrecen seguridad de tipo Endpoint. Esto permitirá marcar las condiciones de seguridad que deberá presentar un equipo remoto para el acceso a los diferentes servicios. Si un equipo no cuenta entre sus sistemas de defensa con un antivirus, un firewall, un nivel apropiado de actualización o incumple cualquier norma marcada por la organización a través de las políticas de seguridad, el acceso no se realizará, o bien será parcial. Esto permitiría acceder solamente a servicios no críticos de la organización. (Véase la Figura 6.3.7.)

Como se muestra en la imagen anterior, determinados servicios presentados a través del portal de acceso no se encuentran disponibles porque el equipo cliente no contaba con los requisitos de seguridad exigidos por la organización. También entre los servicios que se ofrecen en MS Forefront Unified Access Gateway 2010 se encuentran los de conexión de redes virtuales privadas (VPN). Los tipos de túneles que admiten tanto MS Forefront UAG, como los citados anteriormente son:

- PPTP (*Point To Point Tunneling Protocol*).
- L2TP (*Layer 2 Tunneling Protocol) sobre IPsec (IP Security*).
- SSTP (*Secure Socket Tunneling Protocol*).

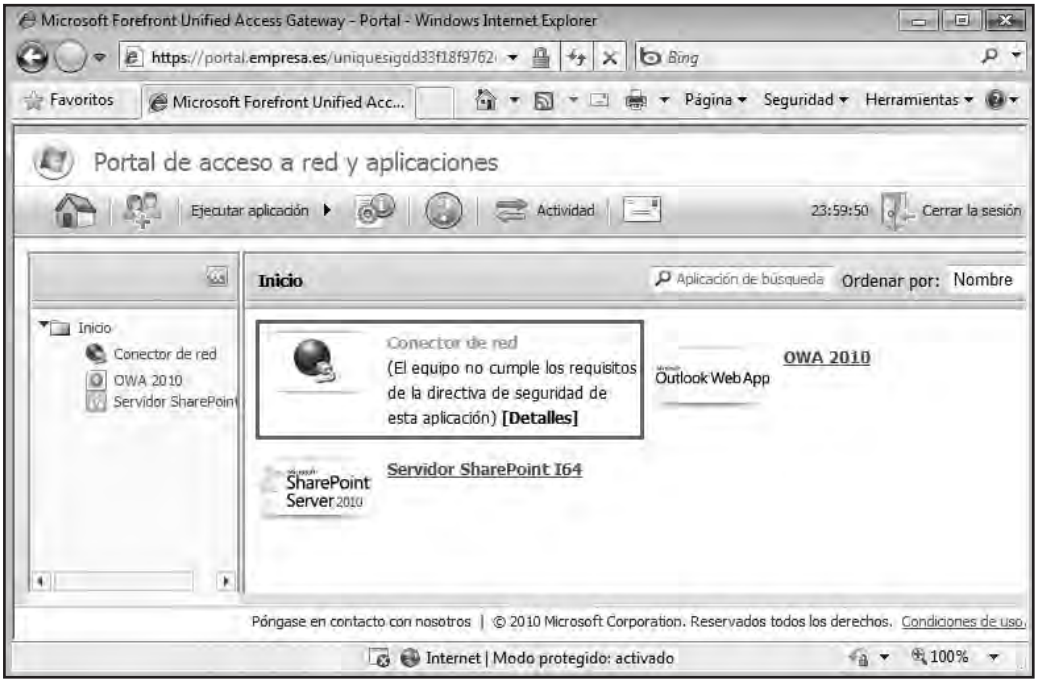


Figura 6.3.7. Acceso a la organización a través de la seguridad Endpoint.

En la comunicación VPN, y con el objeto de garantizar la seguridad de los datos, la información de forma convencional es cifrada y encapsulada en el protocolo PPP (*Point to Point Protocol*). Sin embargo, PPP no ofrece mecanismos por sí mismo para garantizar la seguridad en el proceso de autenticación, por lo que dependerá exclusivamente del protocolo utilizado para ello. Si éste es débil, como CHAP (*Challenge Handshake Authentication Protocol*) o MS-CHAPv1 (*Microsoft Challenge Handshake Authentication Protocol versión 1*), no se ofrecen garantías si se utiliza exclusivamente PPP para la seguridad de la autenticación. PPTP hace uso exclusivamente de PPP; los otros dos protocolos utilizan sistemas alternativos para garantizar la confidencialidad de los datos.

En el caso de L2TP, se hace uso de IPsec y los drivers del mismo para garantizar el cifrado de la comunicación. Para ello, se produce un proceso de negociación de la seguridad mediante el protocolo IKE (*Internet Key Exchange*). Dicha negciación se establece en dos fases:

- **1ª fase.** ISAKMP (Asociación de seguridad de protocolo de gestión de claves de asociaciones de seguridad en Internet). Es donde se lleva a efecto la autenticación de la conexión y, para ello, se pueden utilizar diferentes mecanismos. Los sistemas Microsoft utilizan PSK (Clave Previamente Compartida) o los Certificados X.509.

- **2ª fase.** Donde se va a negociar la seguridad y generar las claves de cifrado simétricas, a través del proceso de intercambio denominado Diffie Hellman.

La negociación de la seguridad establece los algoritmos que podrán utilizarse tanto para la protección de la integridad (HMAC-SHA-1 ó HMAC-MD5), como para la confidencialidad (AES-CRT, 3DES-CBC ó DES-CBC).

Una vez establecida la autenticación mutua de IPSec y cuando se haya producido el intercambio de claves para el cifrado, se establecerá el túnel PPP.

En el caso de SSTP se proporcionan mecanismos para encapsular tráfico tipo PPP, sobre un canal seguro SSL (*Secure Socket Layer*) tipo HTTPS. PPP (*Point to Point Protocol*) garantiza el uso del mecanismo de autentificación, mientras que SSL proporciona la seguridad en el nivel de transporte, con negociación de las claves, cifrado y comprobación de la integridad. Este último ofrece las mayores garantías de versatilidad, al establecerse el túnel a través de un puerto, el 443, que de manera habitual se encontrará abierto en cualquier escenario de uso externo. Frente a él, tanto PPTP como L2TP/IPSec utilizan puertos no convencionales que podrían encontrarse cerrados.

Dentro de las medidas también previstas para la seguridad de los equipos portátiles se encuentran las relativas al cifrado de los equipos. Utilizar EFS (*Encripted File System*) o *Biitlocker*, que serán tratados posteriormente en la protección de los soportes, aportarán las garantías necesarias para el cumplimiento de estas medidas.

La última de las medidas de protección en equipos se puede integrar dentro de la dimensión de disponibilidad; aunque no confiere ninguna medida técnica especial, requiere su estudio por parte de las organizaciones. Aquellas que hayan sido catalogadas como de nivel medio o superior, deberán disponer de medios adicionales para garantizar el tratamiento de la información. Para ello, se deberá contar con un parque de equipos alternativos para dar continuidad al servicio ante la aparición de incidencias.

"Medios alternativos [mp.eq.9].

Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información en el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección. Igualmente, se establecerá un tiempo máximo para que los equipos alternativos entren en funcionamiento."

6.4. Protección de los soportes de información

Uno de los problemas que presenta el trabajar con sistemas informáticos y pretender implementar un sistema de prevención de pérdida de información o evitar el robo de la misma, es la cantidad de formatos que de naturaleza extraíble o externa pueden ser utilizados: CD, DVD, discos o unidades USB son algunas de las múltiples posibilidades. Estas últimas, debido a su popularidad, difusión y miniaturización, están ampliamente extendidas y son utilizadas de forma habitual para el transporte de todo tipo de material informático.

El Esquema Nacional de Seguridad se hace eco de este hecho y promueve por igual el empleo de metodologías de catalogación y medidas técnicas para el control de

estos soportes. Solicitar permiso, su custodia o destrucción, requerirán procedimientos reglados para que puedan ser utilizados según los criterios de la norma.

"Etiquetado [mp.si.1].

Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.

Criptografía. [mp.si.2].

Esta medida se aplica, en particular, a todos los dispositivos removibles. Se entenderán por dispositivos removibles los CD, DVD, discos USB, u otros de naturaleza análoga.

Nivel MEDIO

Se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

Nivel ALTO

a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

b) Se emplearán, preferentemente, productos certificados [op.pl.5].

Custodia [mp.si.3].

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, mediante las siguientes actuaciones:

a) Garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) ó lógicas ([mp.si.2]), o ambas.

b) Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.

Transporte [mp.si.4].

El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.

Para ello:

- *Se dispondrá de un registro de salida que identifique al transportista que recibe el soporte para su traslado.*
- *Se dispondrá de un registro de entrada que identifique al transportista que lo entrega.*
- *Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.*

- *Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel.*
- *Se gestionarán las claves según [op.exp.11].*

Borrado y destrucción [mp.si.5].

Nivel MEDIO

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización, serán objeto de un borrado seguro de su anterior contenido.

b) Se destruirán de forma segura los soportes, en los siguientes casos:

1.º Cuando la naturaleza del soporte no permita un borrado seguro.

2.º Cuando así lo requiera el procedimiento asociado al tipo de la información contenida.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].”

Las normas en este caso son claras: control de los medios, procedimientos de uso, destrucción y cifrado cuando sea necesario, esta última especialmente para el transporte de la información cuando ésta salga fuera de las infraestructuras de la organización. Los procedimientos tales como la notificación y el etiquetado vendrán definidos a través de la política de seguridad, y podrán emplearse para ello mecanismos ya mencionados para el tratamiento de los mismos. MS SharePoint Server es nuevamente una clave estratégica para el cumplimiento de la normativa.

En el caso de los mecanismos de cifrado Microsoft ofrece varias alternativas. Aunque en esta parte de las medidas se recogen las específicas de soporte. Las soluciones que se citan a continuación podrán ser utilizadas por aquellas que requieran confidencialidad de los datos, tales como la protección del equipo o la privacidad de la información. Los tres mecanismos que se ofrecen para garantizar la confidencialidad de ficheros son:

- El Sistema de ficheros cifrados (EFS o *Encripted File System*).
- Bitlocker.
- Bitlocker To Go.

EFS es el mecanismo tradicional. Permite un sistema de cifrado totalmente transparente para el usuario, no ofrece integridad en los datos o autentificación, por lo que no deberán obviarse otros mecanismos de seguridad alternativos. Utiliza para la confidencialidad el sistema de certificados estándar X.509.

El cifrado se produce empleando una clave de encriptación de fichero (FEK) generada aleatoriamente mediante algoritmo AES (*Advance Encription Standard*). EFS

posteriormente utilizará mecanismos de clave pública para cifrar la clave FEK. Los diferentes usuarios que acceden a los ficheros que han sido protegidos mediante EFS contarán con una clave privada con la que obtener la clave FEK.

Al objeto de preservar los mecanismos de seguridad en las copias de respaldo, cuando se realice una copia de seguridad de ficheros cifrados mediante mecanismos de EFS, con herramientas certificadas por Microsoft se garantizará que estos ficheros de respaldo mantienen su condición de cifrado mediante EFS. Esto también sucederá con los sistemas de medios extraíbles que utilicen NTFS y que son gestionados por el sistema operativo. Como estos medios no migran ni las claves de cifrado ni la de los agentes de recuperación de datos cifrados, la garantía de seguridad es muy alta.

Sin embargo, aunque el sistema es idóneo para la protección de ficheros de datos, no sería válido su uso en el cifrado activo del sistema operativo. Bitlocker, que aparece a partir de Windows Vista, implementa mecanismos para el cifrado de disco. Frente a EFS, que se utilizaba para la confidencialidad de determinados ficheros, este se emplea para unidades completas. (Véase la Figura 6.4.1.)

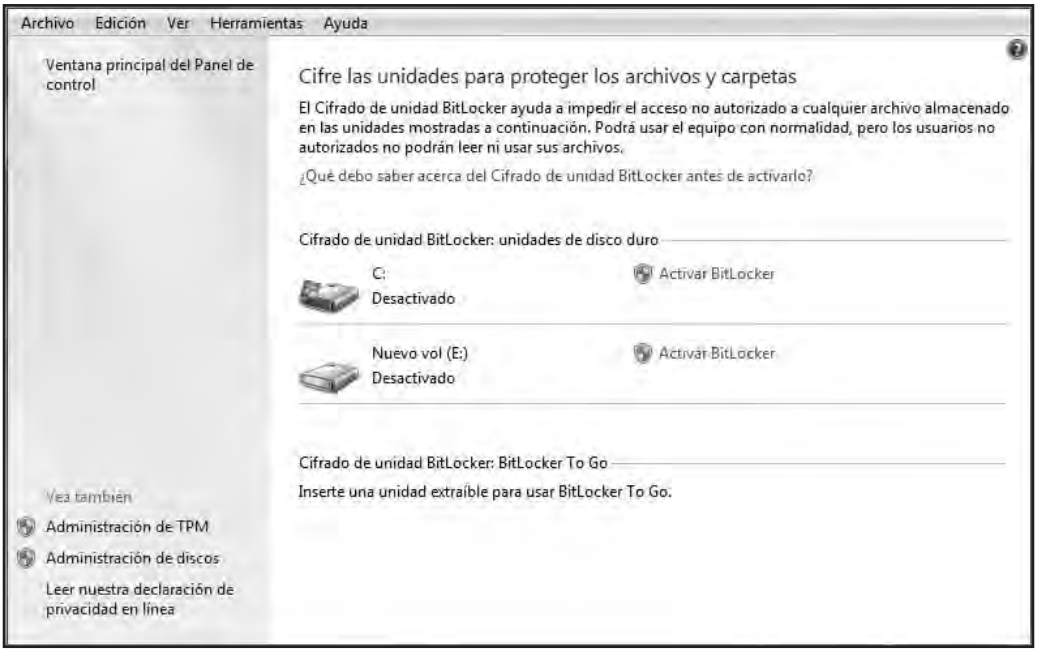


Figura 6.4.1. Activar cifrado de unidad con Bitlocker.

Para realizar su cometido, Bitlocker utiliza AES (*Advance Encription Standard*) como algoritmo de cifrado en modo CBC (*Cypher Block Chaining*). Por otra parte, con objeto de evitar los ataques por manipulación de datos cifrados, incorpora un difusor adicional independiente denominado Elephant. Para garantizar el almacenamiento de la clave de cifrado, Bitlocker puede utilizar las nuevas especificaciones de seguridad

hardware denominadas Trusted Platform Module (TPM). Este nuevo chip proporciona una plataforma segura para el almacenamiento de claves, passwords o certificados, haciendo más difícil el ataque contra los mismos. Aunque constituye el método ideal para el almacenamiento de la clave de cifrado, se pueden utilizar mecanismos alternativos como dispositivos USB para este almacenamiento. Sin embargo, de forma predeterminada se utiliza la tecnología de TPM.

Las funcionalidades de cifrado y descifrado de la información son totalmente transparentes para el usuario, yendo más allá del posible uso, puesto que previene al sistema de ataques basados en mecanismos offline. Cualquier intento de extraer la información sin la clave correspondiente será infructuoso.

La implementación inicial de Bitlocker en Windows Vista sólo admitía el cifrado de la partición donde estaba instalado el sistema operativo. La salida de Windows Vista SP1 permitió además el cifrado de otras particiones de datos, siempre y cuando no fuesen de arranque. Sin embargo, la implementación de confidencialidad mediante Bitlocker no se hace extensiva hacia las unidades extraíbles.

Esto se ha hecho posible con Windows 7 y la tecnología de Bitlocker To Go. La tecnología es bastante similar a la utilizada en Bitlocker y se basa en el uso de tres claves:

- El volumen se cifra con AES 128 con un difusor a través de una clave denominada FVEK (*Full volumen Encryption Key*).
- La clave FVEK se cifra mediante AES 256 bits con la clave VMK (*Volume Master Key*).
- Esta es cifrada y protegida por una clave protegida derivada de la password introducida por el usuario.

Las operaciones para el cifrado y descifrado de las unidades extraíbles son asequibles para su uso por parte de los usuarios, que sólo deberán conocer la última clave de cifrado del proceso. Cuando se inserta un dispositivo USB en un sistema MS Windows 7, se reconoce la posibilidad de utilizar Bitlocker To Go, solicitándose, si así se desea, la clave para iniciar el proceso de cifrado. Cuando se introduce una unidad cifrada, se solicitará la clave para iniciar el proceso de descifrado.

Con objeto de mantener la compatibilidad de estos dispositivos con sistemas operativos previos a MS Windows 7, Microsoft proporciona una herramienta que permite leer unidades cifradas en otros sistemas operativos cuando se proporcione la clave correspondiente. Su nombre es Bitlocker To Go Reader (véase la Figura 6.4.2).

En el caso de la eliminación segura de datos, Microsoft facilita la aplicación Sdelete, que utiliza como proceso la sobrescritura de los datos realizada con varias pasadas de ceros. Así se garantiza que los datos previos no podrán ser recuperados. Hay que recordar que las operaciones de formateo que acompañan al sistema operativo no son consideradas formalmente como procesos para el eliminación segura. La utilización de la aplicación es muy simple, debiendo especificarse únicamente el fichero o unidad sobre la que se trabajará y las opciones para la realización de dicha tarea (véase la Figura 6.4.3):

- - c Zero free space (good for virtual disk optimization).
- -p Specifies number of overwrite passes.
- -s Recurse subdirectories.
- -q Don't print errors (Quiet).
- -z Clean free space.

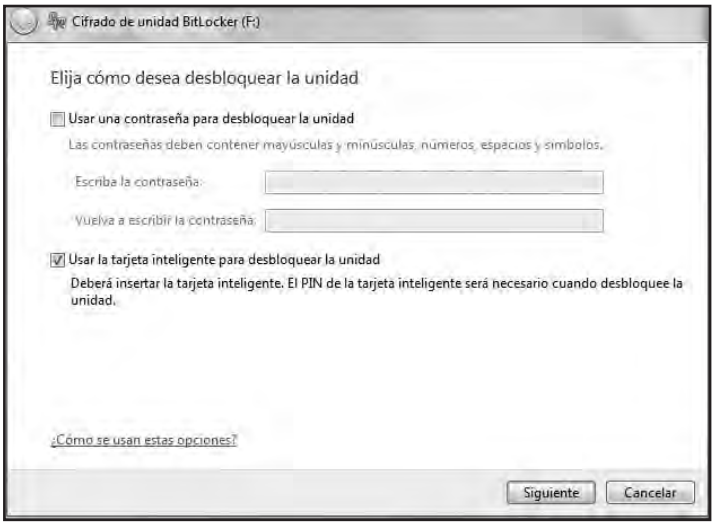


Figura 6.4.2. Cifrado de una unidad extraíble con Bitlocker To Go.

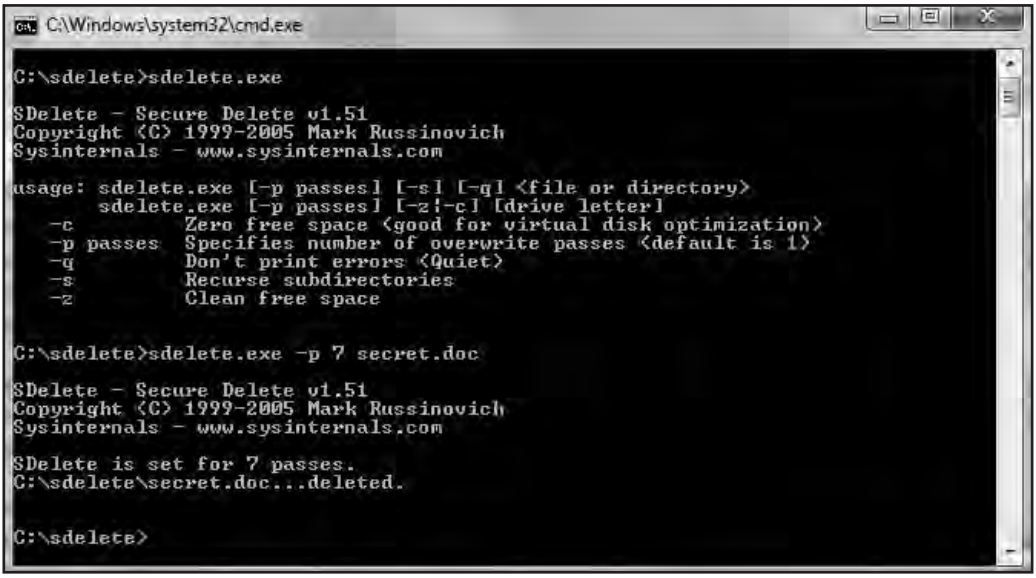


Figura 6.4.3. Uso de la herramienta SDelete.

6.5. Protección de las comunicaciones

La protección de las comunicaciones es uno de los aspectos más importantes en lo que a seguridad informática se refiere, ya que proporciona la garantía de privacidad y autenticidad de las comunicaciones que se realizan a través de la red. Por este motivo, era de esperar que el Esquema Nacional de Seguridad (ENS) dedicara un apartado (Anexo II, apartado 5.4) a definir el nivel de configuración de esta característica.

La protección de las comunicaciones, tanto externas como internas, debe establecer su privacidad en todo momento. El mecanismo de protección de las comunicaciones, según el ENS, es un punto de equilibrio donde intervienen la comodidad de uso y la protección de la información. Según el nivel de seguridad que requiera cada organismo se primará la comodidad frente a la protección en nivel bajo, mientras que en nivel alto se primará la protección frente a la comodidad de uso. Este concepto ya se ha presentado en otros apartados de este libro.

El ENS define claramente cómo se deben establecer condiciones adecuadas según el nivel de criticidad de la información a manejar y proteger. Por tanto, regula para cada uno de los aspectos relacionados con la protección de la comunicación las medidas a aplicar.

A continuación se detallarán cada uno de las medidas de seguridad a aplicar y cómo la tecnología de Microsoft ayuda a conseguir los requisitos exigidos.

6.5.1. Perímetro seguro

"Se dispondrá de un sistema de cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejará transitar los flujos previamente autorizados.

Categoría ALTA

a) El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.

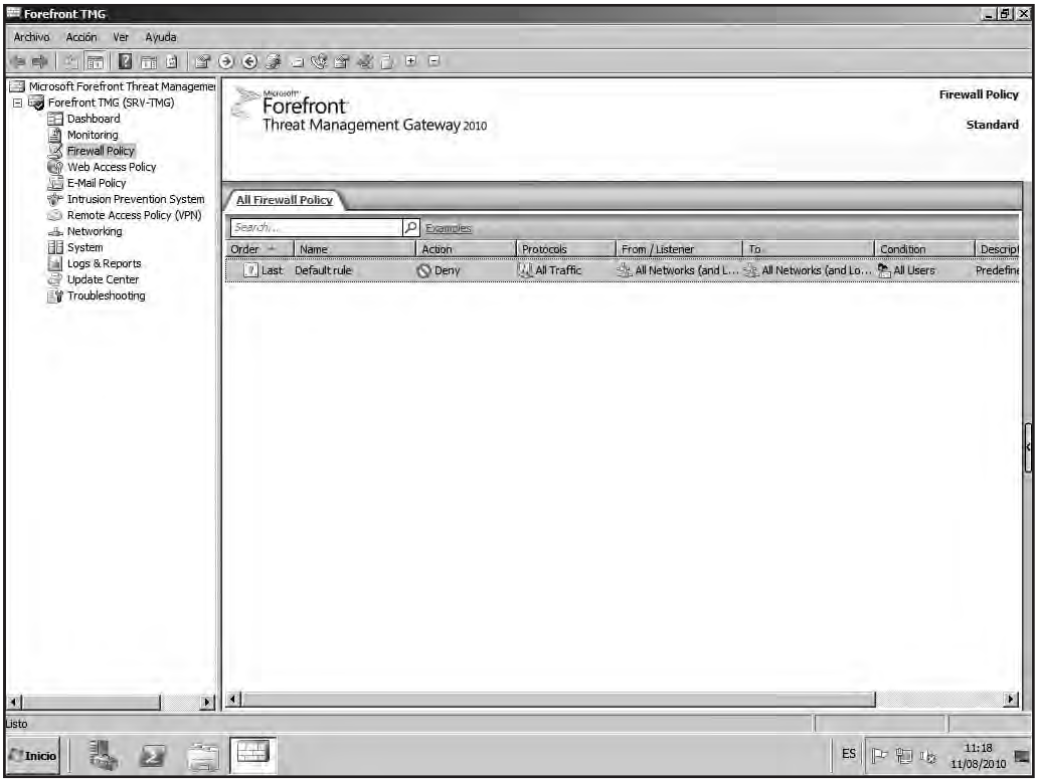
b) Se dispondrá de sistemas redundantes."

La seguridad en profundidad de un sistema empieza con la protección del perímetro, por lo que el Esquema Nacional de Seguridad establece pautas de configuración para este componente. Las exigencias establecidas son diferentes para los tres niveles de seguridad.

Para los dos niveles más bajos, el ENS exige la existencia de un sistema cortafuegos para separar los límites de la organización del exterior. Todo el tráfico deberá atravesar dicho cortafuegos y éste sólo dejará pasar los flujos previamente autorizados.

Microsoft proporciona una solución firewall basada en software a nivel de aplicación ya referida en esta publicación. Se trata de MS Forefront Threat Management

Gateway 2010, que cubre las necesidades establecidas por el ENS. Este producto no es únicamente una solución de cortafuegos, sino que presenta un módulo avanzado de sistema de prevención de intrusión (IPS) y una solución de servidor VPN, entre otras funcionalidades. MS Forefront TMG presenta una configuración predeterminada que bloquea cualquier tipo de tráfico que entre o salga de la red de la organización, como se observa en la siguiente figura. Dicha regla es predeterminada, no se puede eliminar y siempre será la última en aplicarse, cumpliendo así todos los requisitos establecidos para los niveles de seguridad bajo y medio establecidos en el ENS.



La creación de reglas para la autorización de tráfico se basa en asistentes que facilitan la identificación del flujo y el tipo de datos a permitir. MS Forefront TMG presenta varios tipos de asistentes para los distintos tipos de flujos a gestionar (véase la ilustración de la derecha). La publicación de servicios o reglas de acceso son claros ejemplos de ello.

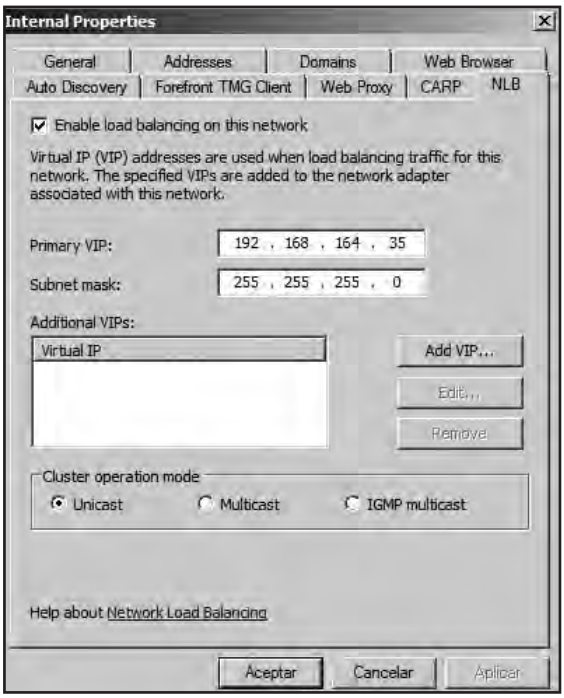
Nivel alto

En términos de perímetro seguro el ENS para el nivel alto establece el cumplimiento de los requisitos anteriores más la

necesidad de proporcionar sistemas redundantes, así como la existencia de varios sistemas cortafuegos de distintos fabricantes dispuestos en cascada.

Ambos requisitos son soportados por MS Forefront TMG. Este producto presenta por su parte compatibilidad 100% con cualquier otro sistema de cortafuegos del mercado, tanto de capa de transporte como de aplicación y ya sea delante o detrás en la infraestructura de protección perimetral.

MS Forefront TMG en su versión Enterprise presenta la posibilidad de implantar una solución de alta disponibilidad a nivel de cortafuegos con todas sus funcionalidades. La configuración es muy sencilla, ya que simplemente consiste en generar una matriz con los servidores MS TMG que se deseen proporcionar a la solución de alta disponibilidad, estableciendo la dirección IP de la solución perimetral en alta disponibilidad como se puede observar en la ilustración de la derecha .



La gestión de reglas de control de flujo, soluciones de VPN o cualquier otro tipo de configuración a realizar sobre la infraestructura de cortafuegos se realiza de forma conjunta, ya que todos los servidores de la matriz comparten la configuración. La gestión de la infraestructura de alta disponibilidad se realiza del mismo modo que un cortafuegos en modo *standalone* o independiente.

6.5.2. Protección de la confidencialidad

"Nivel MEDIO

a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

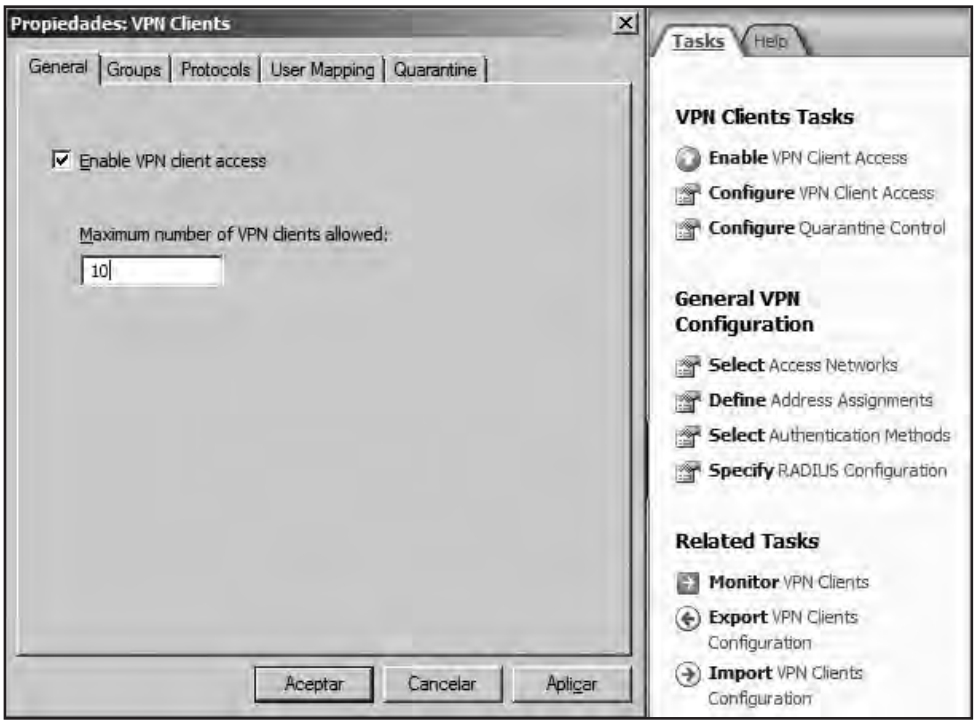
Nivel ALTO

a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

b) Se emplearán, preferentemente, productos certificados [op.pl.5]."

En la actualidad, las organizaciones presentan la necesidad de proporcionar mecanismos de acceso al sistema para sus trabajadores desde cualquier lugar. Este tipo de escenarios suelen ser altamente peligrosos, ya que en ellos se utilizan canales de comunicación no seguros, como Internet. En cuanto a los mecanismos de protección, el Esquema Nacional de Seguridad establece unas medidas mínimas a cumplimentar en los sistemas en función de los niveles de seguridad de la información que manejan. Las exigencias establecidas se deben fijar únicamente en los dos niveles más altos, siendo diferentes para cada uno de ellos.

El ENS establece para el nivel medio de seguridad la necesidad de utilizar redes privadas virtuales (VPN) para la comunicación, cuando esta discurra sobre redes ajenas al dominio de seguridad de la organización. MS Forefront Threat Management Gateway 2010 proporciona la funcionalidad de servidor VPN para la protección de las comunicaciones remotas. (Véase la siguiente ilustración.)



MS Forefront TMG soporta tres protocolos de red privada virtual: PPTP, L2TP/IPSec y SSTP. Cualquiera de estos protocolos de encapsulamiento son válidos para el nivel de seguridad medio, ya que utilizan algoritmos acreditados por el Centro Criptológico Nacional, requisito establecido por el ENS.

En el nivel alto de seguridad para la protección de la confidencialidad, el ENS establece que se deben emplear preferentemente dispositivos hardware para la implantación de redes privadas virtuales. Para el cumplimiento de este requisito, Microsoft

cuenta con soluciones de Appliance con MS Forefront TMG, que proporcionan soporte para redes privadas virtuales con algoritmos acreditados por el Centro Criptológico Nacional.

6.5.3. Protección de la autenticidad y la integridad

"Nivel BAJO

a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (ver [op.acc.5]).

b) Se prevendrán ataques activos, garantizando que al menos serán detectados. Y se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

1º La alteración de la información en tránsito.

2º La inyección de información espuria.

3º El secuestro de la sesión por una tercera parte.

Nivel MEDIO

a) Se emplearán redes privadas virtuales, cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

Nivel ALTO

a) Se valorará positivamente el empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.

b) Se emplearán, preferentemente, productos certificados [op.pl.5]."

Otro de los problemas más comunes a los que tiene que hacer frente una organización hoy en día, es la fiabilidad de la información recibida. En muchas ocasiones no se tiene la certeza de quién la ha enviado, y si es o no información veraz. El Esquema Nacional de Seguridad establece unas medidas a implementar para garantizar que la información recibida en cada momento tenga la fiabilidad de quien la envía, no habiendo sido además manipulada durante su tránsito. Con ello se atiende a uno de los pilares básicos de la seguridad de la información, la integridad.

El nivel de exigencia establecido por el ENS, es diferente para cada uno de los tres niveles de seguridad.

Nivel bajo

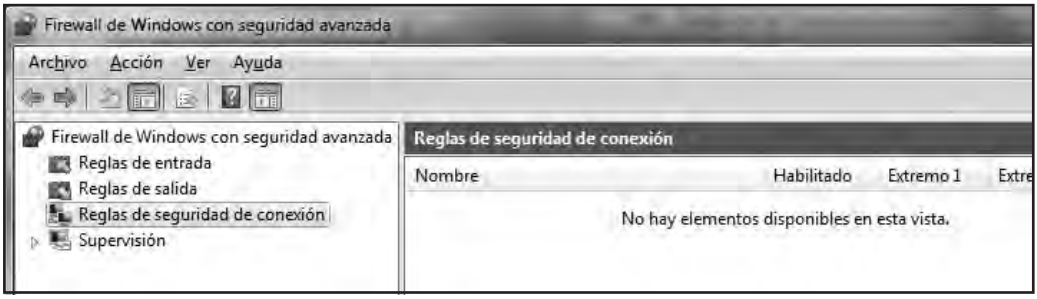
El ENS establece que todo sistema que contenga información de carácter bajo, debe asegurar la autenticidad del otro extremo de la comunicación como paso previo

al intercambio de información. Este procedimiento se trata en el punto de Mecanismos de autenticación. Otro de los requisitos para este nivel de seguridad debe ser la prevención de cualquier tipo de ataque activo, como pueden ser la alteración de la información en tránsito, la inyección de información espuria o el secuestro de la sesión por una tercera parte.

Para el cumplimiento de estos requisitos, los sistemas operativos de Microsoft implementan IPSec. Windows 7 y Windows Server 2008 R2 proporcionan un nuevo mecanismo de implementación de IPSec, a través del firewall de Windows. Esto requiere que éste se encuentre activo en los dos equipos que intervienen en la comunicación.

El proceso de configuración de IPSec es imprescindible realizarlo en ambos extremos de la comunicación. A continuación se detalla cómo realizar la configuración sobre uno de los ellos, procedimiento que es necesario repetir de igual modo en el otro extremo.

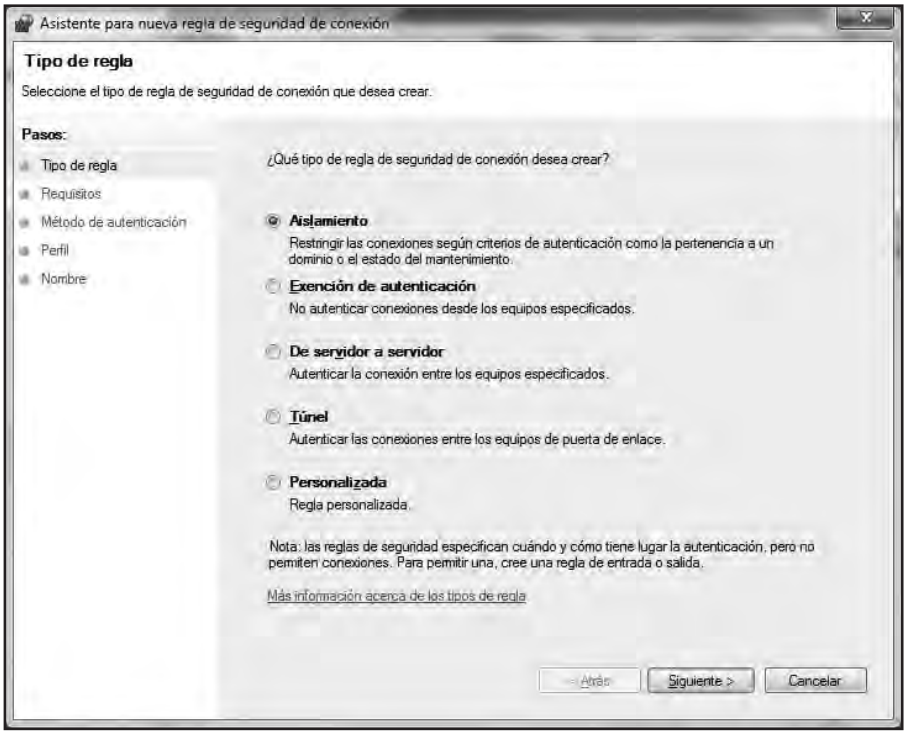
En la consola de Firewall de Windows con seguridad avanzada (véase la siguiente figura), existe un elemento denominado Reglas de seguridad de conexión, donde se establece qué comunicaciones se deben realizar de forma segura. El comportamiento del firewall con respecto a las reglas de seguridad, no sólo realiza la labor de proteger las comunicaciones, sino también puede autorizar o denegar éstas basándose en si el tráfico ha sido asegurado a través de IPSec.



La configuración de la seguridad de los extremos se realiza a través de reglas, con lo que se proporciona la mayor granularidad posible, con el objetivo de dotar al sistema de la flexibilidad requerida en cada situación. La creación de las reglas se realiza a través de un asistente que guiará en la configuración de las mismas, con el máximo detalle posible.

En una primera instancia, el asistente proporciona varios tipos de reglas predefinidas para escenarios concretos, como se puede observar en la primera ilustración de la siguiente página. Por otra parte, se suministra la alternativa de definir las reglas con total detalle partiendo desde cero. A partir de este momento, se tratarán las reglas de tipo personalizado, ya que son las que proporcionan el detalle completo del proceso.

Lo próximo que solicita la definición de regla es establecer cuáles van a ser los extremos de las comunicaciones. Será necesario determinar la dirección IP tanto de la máquina local como del otro extremo de la comunicación (véase la figura superior de

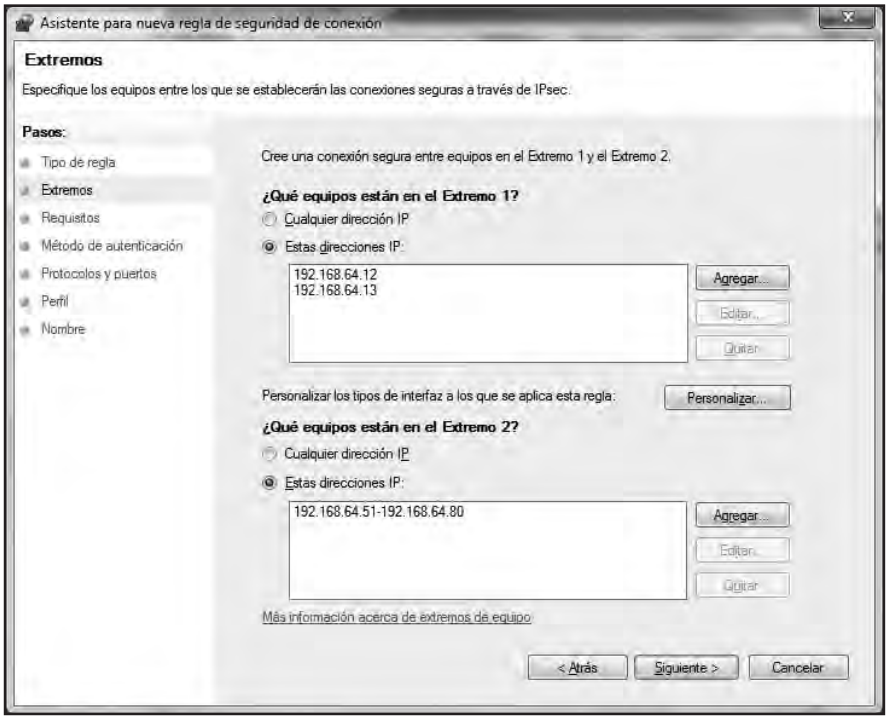


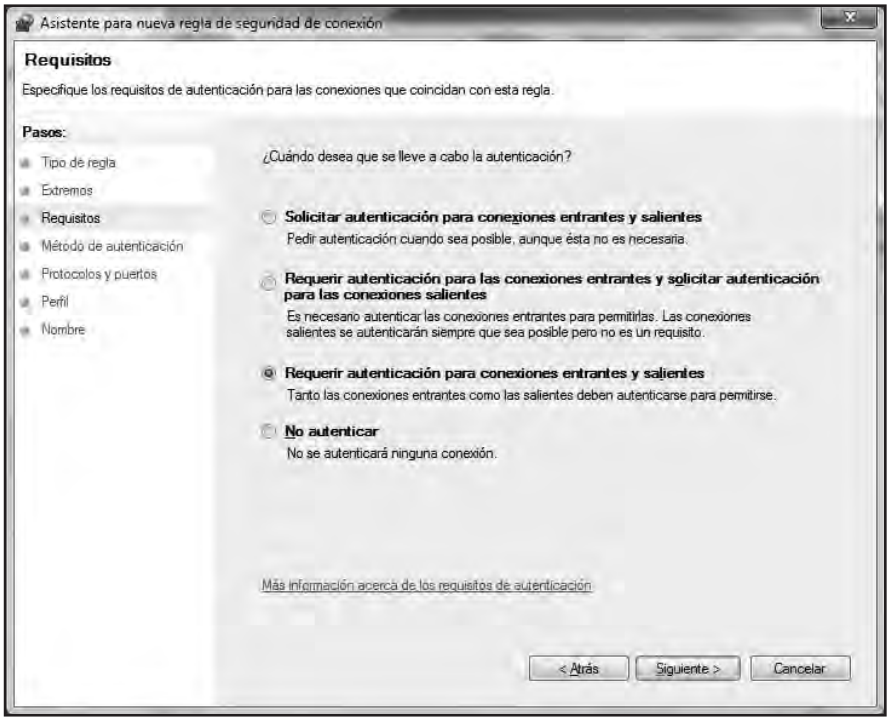
la siguiente página). De este modo es posible definir una sola regla para todos aquellos equipos con los que la máquina se debe comunicar de forma segura, simplificando la configuración y posterior administración de las reglas.

Tras establecer entre qué direcciones se debe realizar la comunicación segura, es el momento de definir qué tipo de autenticación se va a utilizar. Para el cumplimiento de las exigencias del ENS, es requisito imprescindible seleccionar la opción Requerir autenticación para conexiones entrantes y salientes, como se puede observar en la ilustración inferior de la siguiente página.

Una vez establecida la necesidad de autenticar cualquier tipo de conexión, se debe indicar el método de autenticación a utilizar (véase la primera figura de la página 157). Windows 7 y Windows Server 2008 R2 proporcionan varias posibilidades:

- **Predeterminado.** Esta opción establece que el tipo de protección IPSec quede determinado a través de la configuración establecida con el mecanismo tradicional de configuración, la consola administrativa de seguridad de IP.
- **Equipo y usuario (Kerberos V5).** Esta opción es válida cuando los equipos y usuarios que intervendrán en la comunicación pertenecen al mismo dominio de Active Directory, ya que utiliza los tickets Kerberos proporcionados por un controlador a cada usuario o equipo del dominio. Se requiere la validación del equipo y posteriormente del usuario para el proceso.


Asistente para nueva regla de seguridad de conexión
Extremos
Especifique los equipos entre los que se establecerán las conexiones seguras a través de IPsec.
Pasos:
Tipo de regla
Extremos
Requisitos
Método de autenticación
Protocolos y puertos
Perfil
Nombre
Cree una conexión segura entre equipos en el Extremo 1 y el Extremo 2.
¿Qué equipos están en el Extremo 1?
Cualquier dirección IP
Estas direcciones IP:
192.168.64.12
192.168.64.13
Agregar...
Editar...
Quitar
Personalizar los tipos de interfaz a los que se aplica esta regla:
Personalizar...
¿Qué equipos están en el Extremo 2?
Cualquier dirección IP
Estas direcciones IP:
192.168.64.51-192.168.64.80
Agregar...
Editar...
Quitar
Más información acerca de extremos de equipo
< Atrás
Siguiente >
Cancelar


Asistente para nueva regla de seguridad de conexión
Requisitos
Especifique los requisitos de autenticación para las conexiones que coincidan con esta regla.
Pasos:
Tipo de regla
Extremos
Requisitos
Método de autenticación
Protocolos y puertos
Perfil
Nombre
¿Cuándo desea que se lleve a cabo la autenticación?
Solicitar autenticación para conexiones entrantes y salientes
Pedir autenticación cuando sea posible, aunque ésta no es necesaria.
Requerir autenticación para las conexiones entrantes y solicitar autenticación para las conexiones salientes
Es necesario autenticar las conexiones entrantes para permitirlas. Las conexiones salientes se autenticarán siempre que sea posible pero no es un requisito.
Requerir autenticación para conexiones entrantes y salientes
Tanto las conexiones entrantes como las salientes deben autenticarse para permitirse.
No autenticar
No se autenticará ninguna conexión.
Más información acerca de los requisitos de autenticación
< Atrás
Siguiente >
Cancelar

- **Equipo (Kerberos V5).** Es otra opción válida cuando los equipos pertenecen al mismo dominio. Se utiliza el ticket Kerberos proporcionado al equipo por Active Directory, pero a diferencia de la opción anterior sólo se valida la autenticidad de los equipos que intervienen en la comunicación, no la de los usuarios.
- **Opciones avanzadas.** Esta última opción permite personalizar el tipo de mecanismos que se utilizarán para la autenticidad de los extremos de la conexión. Se pueden utilizar para ello tickets Kerberos, certificados o clave compartida, tanto para la primera autenticación de los equipos como en segunda instancia para los usuarios.

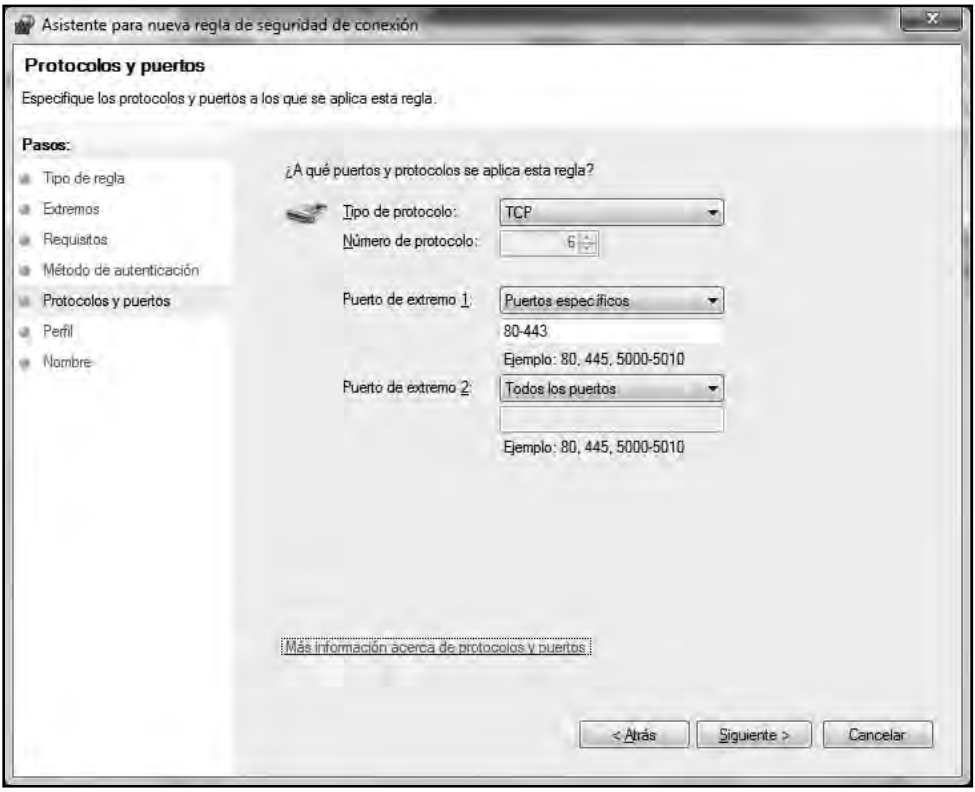
Según las exigencias del ENS y lo establecido en el apartado "Mecanismos de autenticación", la configuración idónea a implementar en los sistemas que manejan información confidencial es la autenticación en el proceso de comunicación a nivel de usuario y equipo (véase la doble autenticación en la primera figura de la siguiente página). El uso de certificados o tickets Kerberos para ello, depende del nivel de seguridad definido en los mecanismos de autenticación.

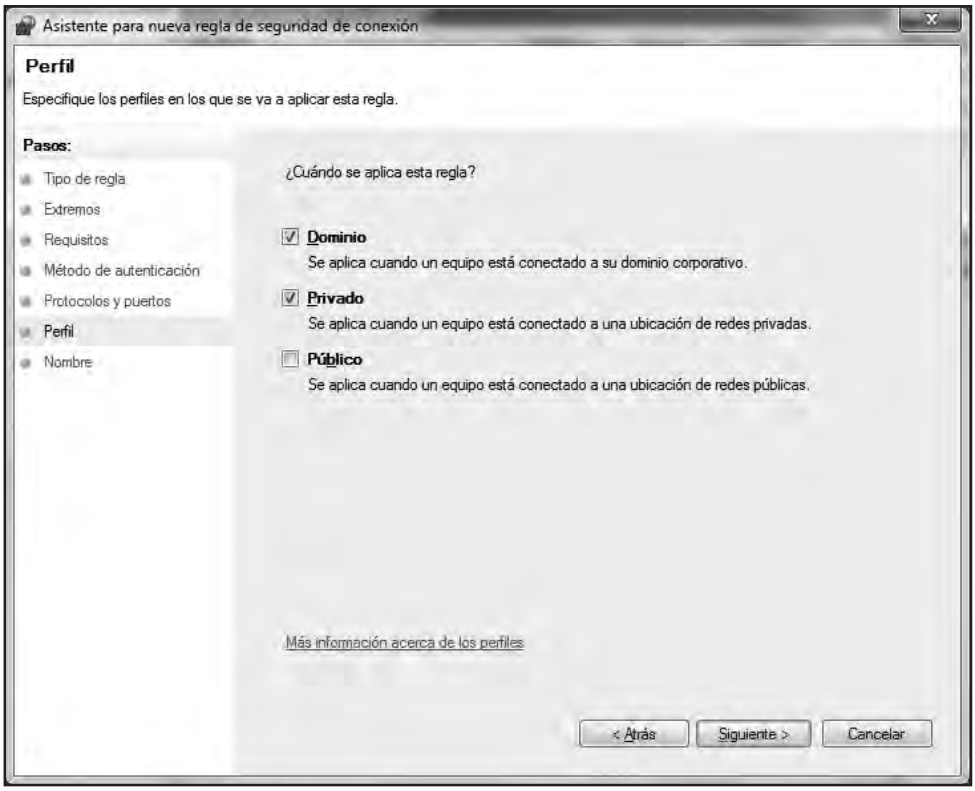
Tras definir el mecanismo de autenticación a requerir en la comunicación, es el momento de definir concretamente para qué tipo de tráfico se necesita protección mediante IPSec (véase la ilustración inferior de la siguiente página). Windows 7 y Windows Server 2008 R2 tienen la capacidad de establecer qué tipo de protocolo o puertos de origen y destino intervienen en la comunicación segura, proporcionando así la granularidad indicada anteriormente.

Finalmente, MS Windows 7 y MS Windows Server 2008 R2 proporcionan la posibilidad de definir el tipo de redes que se desean utilizar en la protección de la comunicación, como se puede observar en la primera ilustración de la página 159.

Tras identificar la regla de seguridad con un nombre descriptivo, es necesario repetir la configuración sobre el resto de dispositivos que intervienen en la comunicación, garantizando así los requisitos de autenticidad e integridad de ésta, tal y como establece el Esquema Nacional de Seguridad.


Personalizar métodos de autenticación avanzada
Primera autenticación
Especifique los métodos de autenticación de equipo que se van a usar durante las negociaciones IPsec. Los primeros de la lista se intentan en primer lugar.
Métodos de primera autenticación:
Método
Información adicional
Equipo (Kerberos V5)
Agregar...
Editar...
Quitar
La primera autenticación es opcional.
Segunda autenticación
Especifique los métodos de autenticación de usuario o un certificado de mantenimiento que se van a usar durante las negociaciones IPsec. Los primeros de la lista se intentan en primer lugar.
Métodos de segunda autenticación:
Método
Información adicional
Usuario (Kerberos V5)
Agregar...
Editar...
Quitar
La segunda autenticación es opcional.
No se puede especificar una segunda autenticación cuando una clave previamente compartida se encuentra en la lista de métodos de la primera autenticación.
Más información acerca de la configuración de autenticación
¿Cuáles son los valores predeterminados?
Aceptar
Cancelar


Asistente para nueva regla de seguridad de conexión
Protocolos y puertos
Especifique los protocolos y puertos a los que se aplica esta regla.
Pasos:
Tipo de regla
Extremos
Requisitos
Método de autenticación
Protocolos y puertos
Perfil
Nombre
¿A qué puertos y protocolos se aplica esta regla?
Tipo de protocolo:
TCP
Número de protocolo:
6
Puerto de extremo 1:
Puertos específicos
80-443
Ejemplo: 80, 445, 5000-5010
Puerto de extremo 2:
Todos los puertos
Ejemplo: 80, 445, 5000-5010
Más información acerca de protocolos y puertos
< Atrás
Siguiente >
Cancelar



Para simplificar la configuración en todos los extremos que intervengan en cualquier instante en la comunicación segura, Microsoft implementa la posibilidad de configuración desde políticas de grupo, como es posible observar en la ilustración de la siguiente página.

Niveles medio y alto

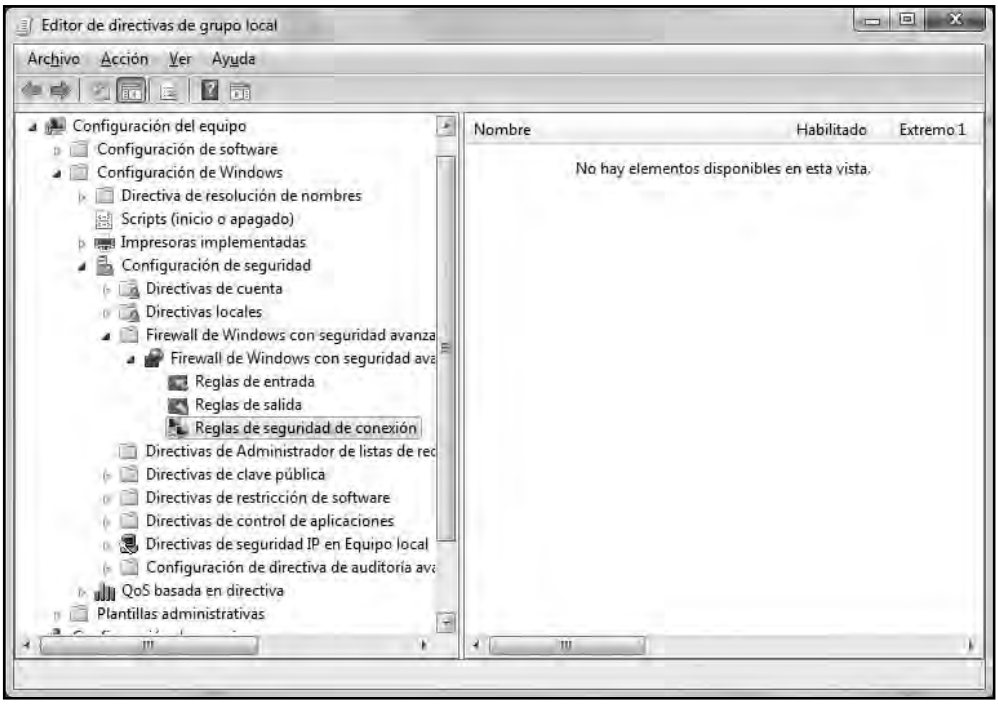
El ENS establece para los sistemas con información de nivel medio o alto la necesidad de utilizar redes privadas virtuales (VPN), con el objetivo de garantizar la seguridad de la información confidencial. Este es el único requisito establecido en el ENS para la protección de la confidencialidad en la comunicación

6.5.4. Segregación de redes

"La segregación de redes acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

La red se dividirá en segmentos de forma que haya:

a) Control de entrada de los usuarios que llegan a cada segmento.



b) Control de salida de la información disponible en cada segmento.

c) Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado (como en [mp.com.1]).”

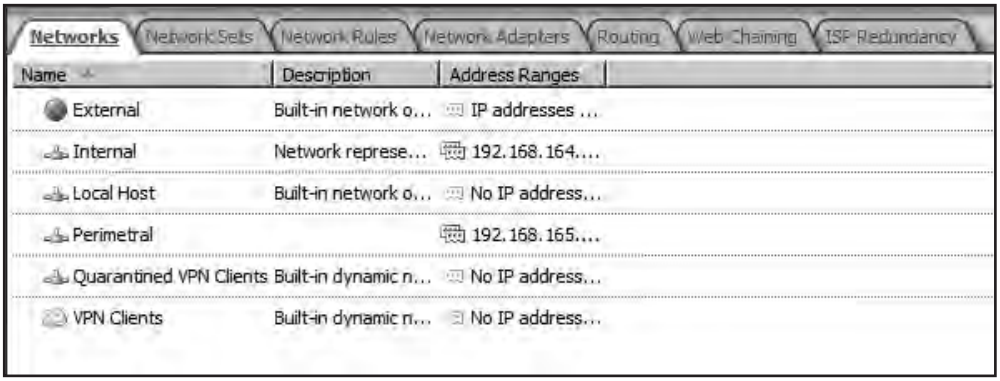
El Esquema Nacional de Seguridad establece la necesidad de segregar las redes de la organización, especialmente aquellos segmentos donde se encuentre la información confidencial. El objetivo consiste en acotar el acceso a la información y evitar así la propagación de incidentes de seguridad, quedando restringidos éstos al entorno donde ocurren y salvaguardando la información de otras ubicaciones. La segregación de redes es una exigencia únicamente para aquellos sistemas que contengan información confidencial de nivel alto.

Las exigencias establecidas para el nivel alto establecen la necesidad de segmentar las redes, controlar la entrada y salida de los usuarios y la información desde cada segmento, así como la posibilidad de monitorizar la actividad.

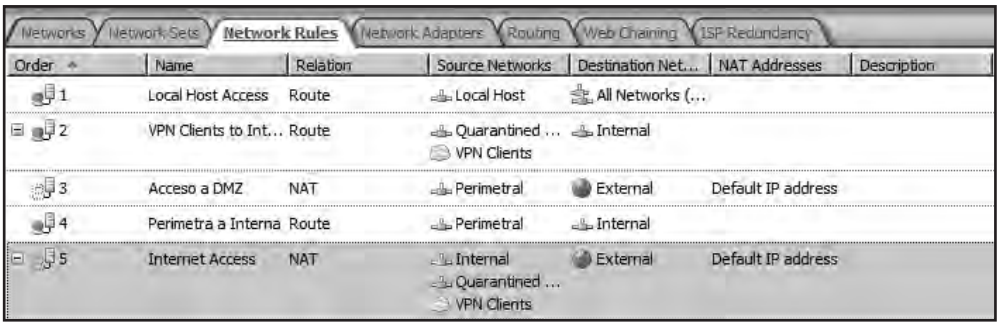
Para el cumplimiento de esta exigencia, Microsoft dispone de MS Forefront Threat Management Gateway 2010. Este aplicativo tiene la capacidad de gestionar redes, controlar el tipo de tráfico y los usuarios que tienen autorizado el acceso de una red a otra, así como la capacidad de registrar cada acceso que se produzca a través del mismo.

A continuación se detalla cómo se debe configurar MS Forefront TMG y su entorno para el correcto cumplimiento de la normativa. El primer requisito de todos

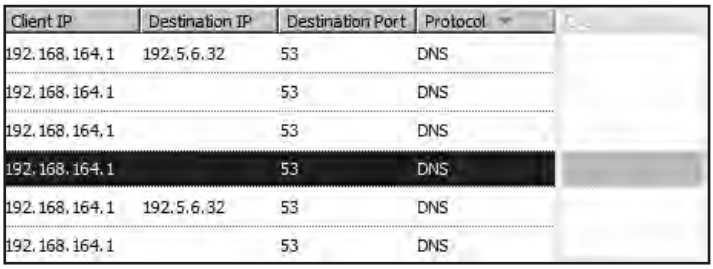
es determinar los distintos segmentos de red de la organización. MS Forefront TMG requiere que cada segmento se encuentre asociado a una interfaz de red dedicada. Tras lo anterior, es necesario dar de alta un objeto red para cada uno de los segmentos como se puede observar en la siguiente ilustración.



El siguiente paso consiste en establecer el tipo de conexión entre las redes. MS Forefront TMG 2010 permite dos tipos de interconexión: NAT y enrutamiento. Para que el tráfico pueda acceder de una red a la otra es necesario que exista una regla de red, ya sea de tipo NAT o de tipo enrutamiento.



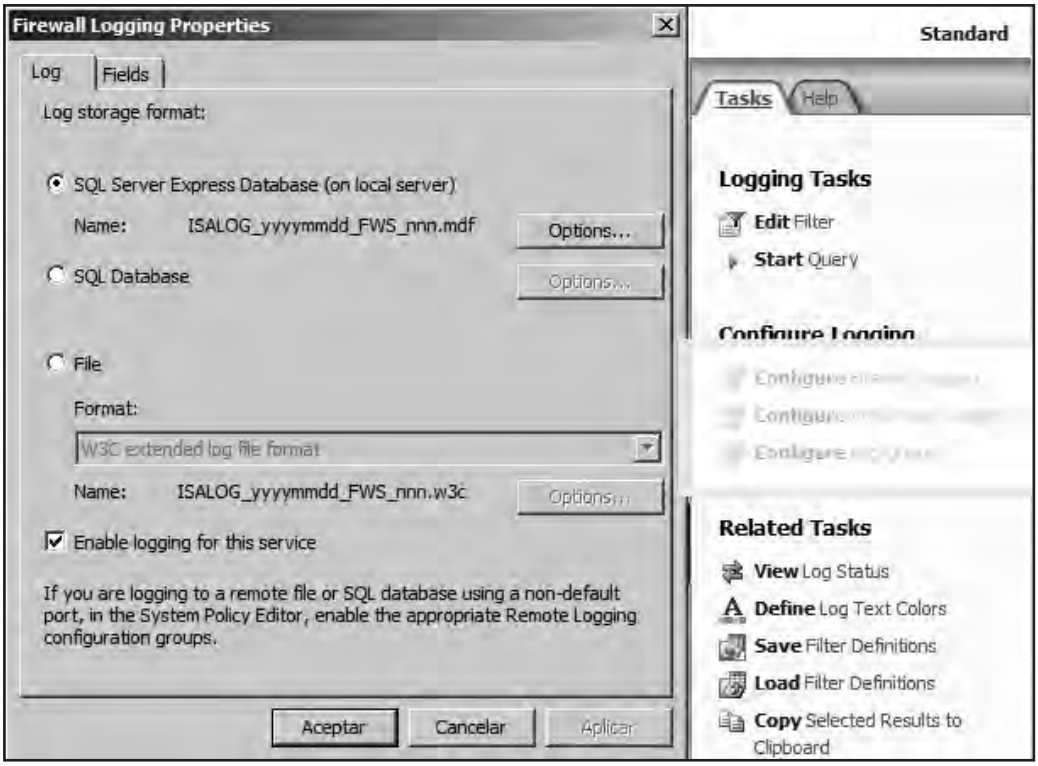
Con esta configuración se cumple el requisito de segmentación de la red, aunque por el momento no se atienden los requisitos de autenticación de los usuarios que acceden de un segmento a otro.



Para autenticar a todos los usuarios que acceden de un segmento de red a otro, es necesario instalar en todos los equipos que tendrán acceso a la información el cliente firewall, MS Forefront TMG Client. Gracias a este componente, todos los equipos que remitan información a través del firewall darán a conocer el nombre de usuario que realiza la comunicación, permitiendo así el cumplimiento del ENS en materia de control de acceso desde cada segmento.

Client IP	Destination IP	Destination Port	Protocol	[illegible]	Source Network
192.168.164.1	192.5.6.32	53	DNS	[illegible]	Internal
192.168.164.1	192.5.6.32	53	DNS	[illegible]	Internal
192.168.164.1	192.5.6.32	53	DNS	[illegible]	Internal
192.168.164.1	192.168.164.254	8080	http	anonymous	Internal

Finalmente, para un cumplimiento completo de la normativa en materia de segmentación de redes, es necesario que la actividad que se desarrolle entre los segmentos de red quede registrada para su posible análisis posterior. MS Forefront TMG 2010 permite el registro de todo el tráfico que se realiza a través de él, en una base de datos o archivo personalizable, tal y como muestra la siguiente imagen.



6.5.5. Medios alternativos

"Se garantizará la existencia y disponibilidad de medios alternativos de comunicación para en el caso de que fallen los medios habituales. Los medios alternativos de comunicación:

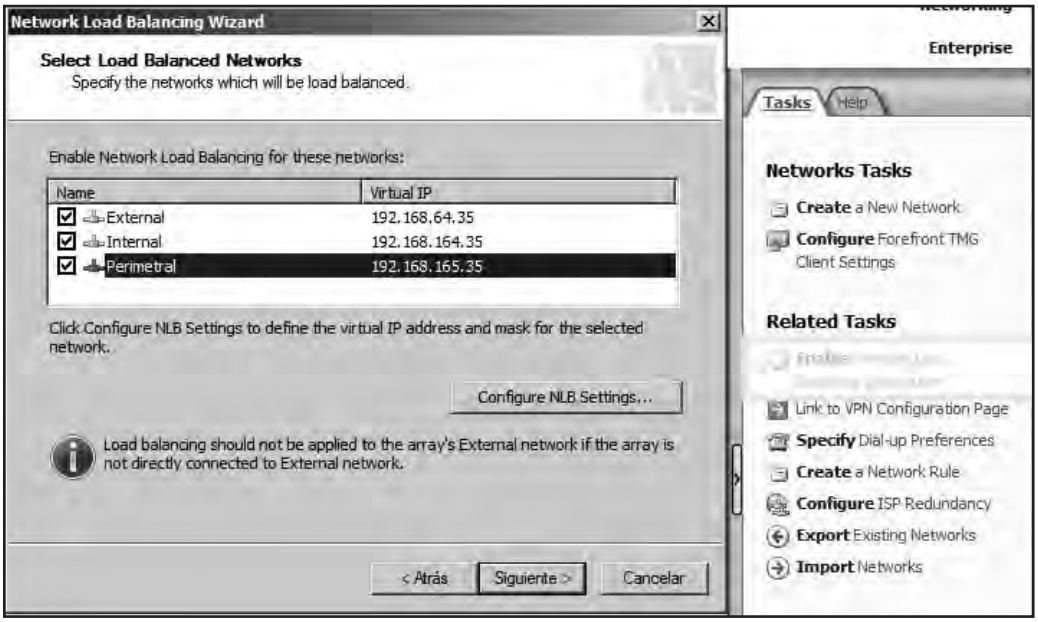
a) Estarán sujetos y proporcionarán las mismas garantías de protección que el medio habitual.

b) Garantizarán un tiempo máximo de entrada en funcionamiento."

El Esquema Nacional de Seguridad establece la necesidad de garantizar la existencia y disponibilidad de medios alternativos de comunicación en caso de fallo de los medios habituales. Los medios alternativos deben proporcionar las mismas garantías de protección, así como presentar un tiempo máximo de entrada en funcionamiento. Los medios alternativos son una exigencia únicamente para aquellos sistemas que contengan información confidencial de nivel alto.

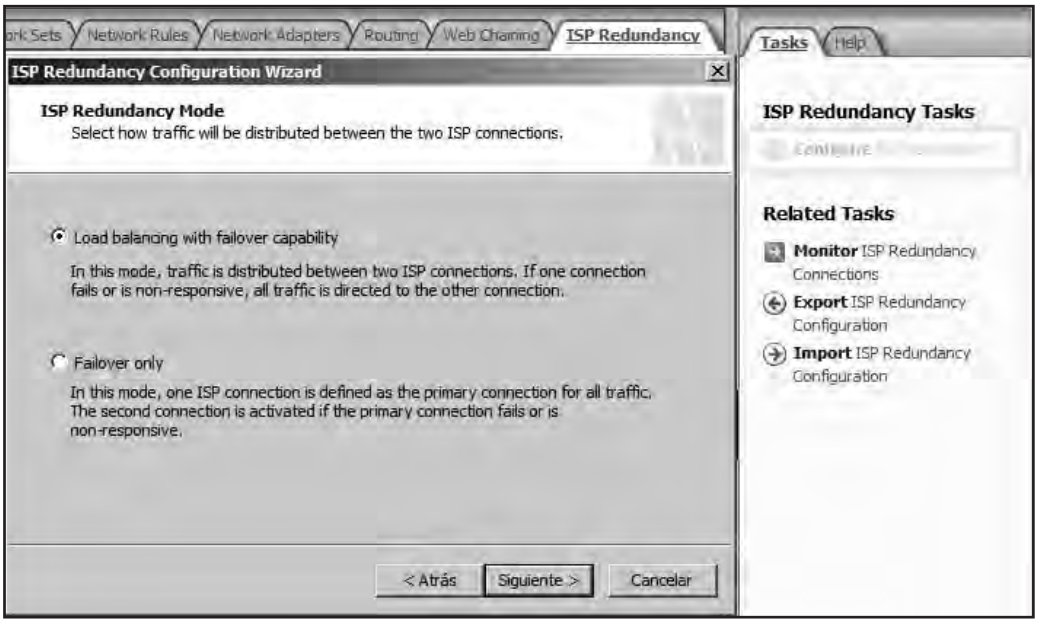
Las exigencias establecidas en el nivel alto determinan la necesidad de dotar a la infraestructura de alta disponibilidad. MS Forefront TMG 2010 soporta una infraestructura de alta disponibilidad consistente en un balanceo de carga, lo cual supone dotar a la solución de tolerancia a fallos y reducir a cero el tiempo de entrada en funcionamiento ante una posible caída. Esta posibilidad sólo se encuentra disponible en la versión Enterprise del producto.

El balanceo de carga consiste únicamente en crear una matriz con los servidores MS Forefront TMG 2010 Enterprise necesarios y configurar una dirección IP virtual única para toda ella, como se observa en la siguiente ilustración.



La gestión de la infraestructura se realiza de forma sencilla, ya que su configuración es necesaria realizarla una única vez sobre cualquiera de los servidores y automáticamente se propagará al resto de máquinas que componen la matriz. Con esta simple configuración tendríamos una solución de alta disponibilidad que cubre las exigencias establecidas por el ENS.

Otra de las características que proporciona MS Forefront TMG 2010 es la capacidad de configuración de redundancia de ISP. Esta funcionalidad permite dotar de alta disponibilidad en tiempo real a la conexión con la red exterior. Simplemente necesitamos contar con dos proveedores de Internet y configurar las salidas de tráfico con el asistente correspondiente.



6.6. Protección de las aplicaciones informáticas

Cuando una organización promueve el desarrollo interno de software, el primer factor que evalúa es su funcionalidad. Inicialmente, también se tiene en cuenta el factor económico y de mantenimiento, determinado junto a otros elementos por la cantidad de gente necesaria para su análisis y desarrollo. Pero, realmente, ¿se tiene en cuenta la seguridad a la hora de programar? Desafortunadamente, y aunque la situación se está modificando positivamente, no es la tónica general.

Sin embargo, para el Esquema Nacional de Seguridad se trata de un factor crítico. Dentro del desarrollo de una aplicación, se tienen que tener en cuenta varias medidas que van desde un desarrollo seguro, hasta la realización de pruebas adecuadas que verifiquen el cumplimiento de las medidas:

"Desarrollo de aplicaciones [mp.sw.1].

Categoría MEDIA

a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.

b) Se aplicará una metodología de desarrollo reconocida que:

1º Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.

2º Trate específicamente los datos usados en pruebas.

3º Permita la inspección del código fuente.

c) Los siguientes elementos serán parte integral del diseño del sistema:

1º Los mecanismos de identificación y autenticación.

2º Los mecanismos de protección de la información tratada.

3º La generación y el tratamiento de pistas de auditoría.

Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Aceptación y puesta en servicio [mp.sw.2].

Categoría BÁSICA

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

a) Se comprobará que:

1º Se cumplen los criterios de aceptación en materia de seguridad.

2º No se deteriora la seguridad de otros componentes del servicio.

b) Las pruebas se realizarán en un entorno aislado (pre-producción).

c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Categoría MEDIA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de vulnerabilidades.

b) Pruebas de penetración.

Categoría ALTA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de coherencia en la integración en los procesos.

b) Se considerará la oportunidad de realizar una auditoría de código fuente."

Tal y como se comentó en el capítulo correspondiente a la seguridad por defecto, Microsoft inició un proceso *Secure Development Lifecycle* (SDL), que ha ofrecido muy buenos resultados. A través de este ciclo se han generado una serie de herramientas que se han hecho públicas, como son SDL *Threat Modeling Tool* y *Threat Analysing & Modeling*. (Véase la Figura 6.6.1.) Estas permitirán a las entidades el desarrollo de aplicaciones pensando en la seguridad.

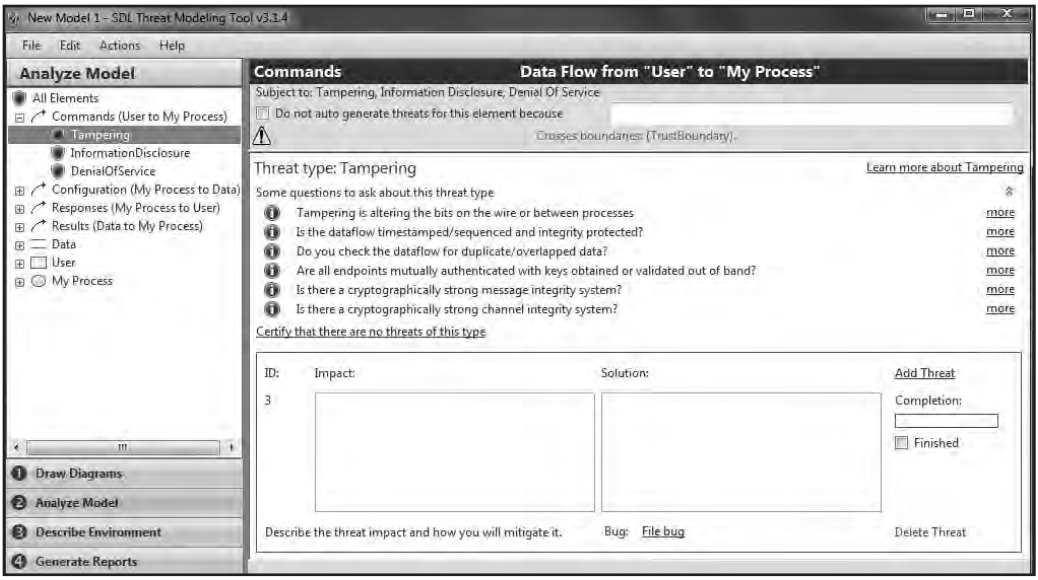


Figura 6.6.1. SDL *Threat Modeling Tool.*

Ambas herramientas permiten a los desarrolladores identificar y mitigar los problemas potenciales de seguridad antes de que se inicie la generación de código, ofreciendo una metodología que cualquier arquitecto de software puede dirigir de forma eficaz. Para ello, la pauta de trabajo se basa en la visión de las herramientas desde el punto de vista de las amenazas a las que pueden estar sujetos los proyectos.

En el caso de SDL Threat Modeling Tool el modelo de clasificación de riesgos se denomina STRIDE.

- **Spoofing (Suplantación).** Mediante el empleo de esta técnica un atacante intentaría la suplantación de uno de los participantes en la conversación. Se

agrupan aquí muchas de las técnicas de ataque, que como la de Man in the middle se producen en la red de datos.

- **Tampering (Manipulación).** La manipulación se produce cuando los datos, fruto de un ataque, son alterados en tránsito. Sumada a la suplantación permite acciones maliciosas combinadas que son ampliamente conocidas.
- **Repudiation (Repudio).** Consiste en la negación de una acción o evento en los sistemas de información. A través de estos hechos los registros de sucesos podrían quedar invalidados.
- **Information disclosure (Revelación de la información).** Se produce cuando se facilita información sensible de forma no deseada debido a un error de programación. Los datos obtenidos podrían ser utilizados posteriormente para otros tipos de ataques como la ingeniería social.
- **Denial of Service (Denegación de servicio).** El ataque tiene como objetivo la caída o el bloqueo del servicio o la aplicación. Estos ataques amenazan el cumplimiento del Esquema Nacional de Seguridad en materia de disponibilidad.
- **Elevation of privilege (Elevación de privilegios).** A partir de un error de programación, un atacante puede obtener privilegios que de forma convencional no tendría. Conseguir ser administrador del sistema para acceder o manipular los datos es uno de los objetivos principales perseguido por los hackers.

En el caso de Threat Analysing & Modeling (TAM) el modelo de amenazas es CIA:

- Confidencialidad.
- Integridad.
- Disponibilidad.

Para la identificación de las amenazas, se presentan librerías de ataques. De diferente factura, se relacionan a través del modelo CIA, determinando en qué medida el software podrá verse afectado. La Figura 6.6.2 muestra la librería de amenazas que proporciona TAM de forma predeterminada

Las aplicaciones, a través de la introducción de datos y la generación de casos de uso, proporcionan los riesgos a los que se pueden ver sometidos los diferentes diseños. La base de datos de conocimiento permitirá ofrecer diferentes metodologías y tecnologías de lenguaje de programación. Estas posibilitarán evitar las amenazas que se pueden presentar durante el desarrollo de una aplicación.

Para llegar a este resultado, es necesario suministrar de forma previa una serie de datos con objeto de poder generar el análisis correspondiente:

- Definición de roles.
- Definición de datos manejados por la aplicación.

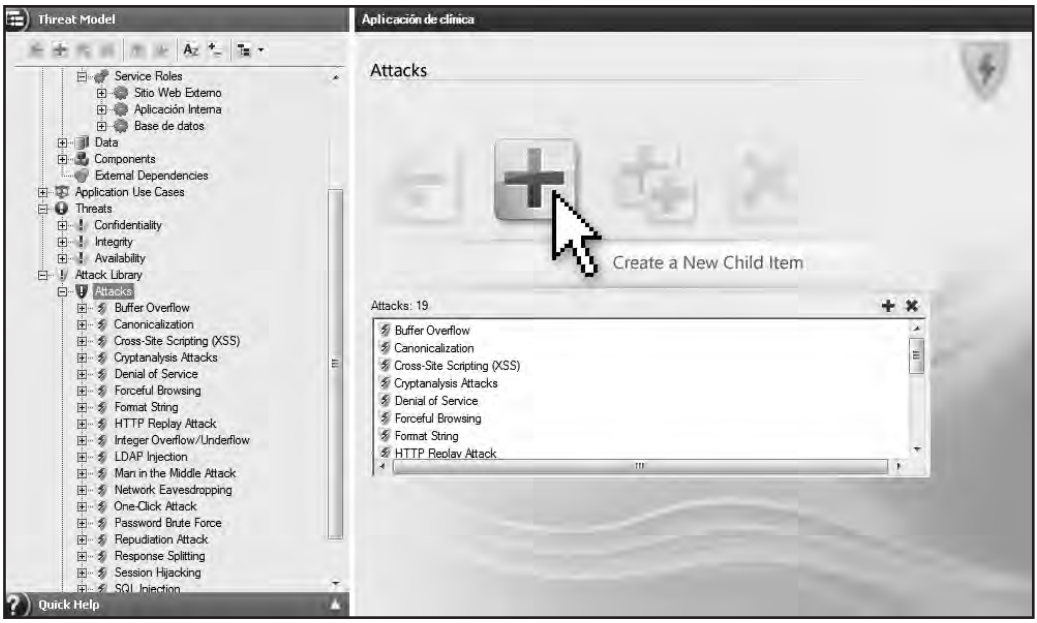


Figura 6.6.2. Librería de amenazas en *Threat Analysing & Modeling*.

- Establecer los permisos de acceso a datos para los roles asignados.
- Definir los casos de uso de la aplicación.
- Definir los módulos de la aplicación.
- Establecer los atributos relevantes que serán utilizados por los componentes de la aplicación.
- Definir las llamadas que definirán las acciones basadas en los casos de uso.

Una vez que el análisis ha sido realizado, se conocerán aquellos riesgos a los que se enfrentaría el desarrollo propuesto. Los informes, completos y fundamentados, permitirán conocer la información de los riesgos, los ataques que se pueden derivar de los mismos y la forma de testear, una vez que el desarrollo ha sido realizado, si la aplicación es vulnerable. La Figura 6.6.3 muestra la detección de un posible ataque Cross-Site Scripting sobre la aplicación analizada y cómo probar si éste es efectivo una vez que el desarrollo esté completado.

Conocer de forma previa las amenazas permite un desarrollo seguro más eficiente. A la hora de realizar las pruebas de vulnerabilidad y penetración exigidas por el Esquema Nacional de Seguridad, se conocerán de antemano los diferentes tests que deberán realizarse para probar la eficacia del código.

Deberá tenerse en cuenta que la realización de tests debe realizarse en un entorno controlado. Las pruebas que se realicen con información real deberán minimizarse

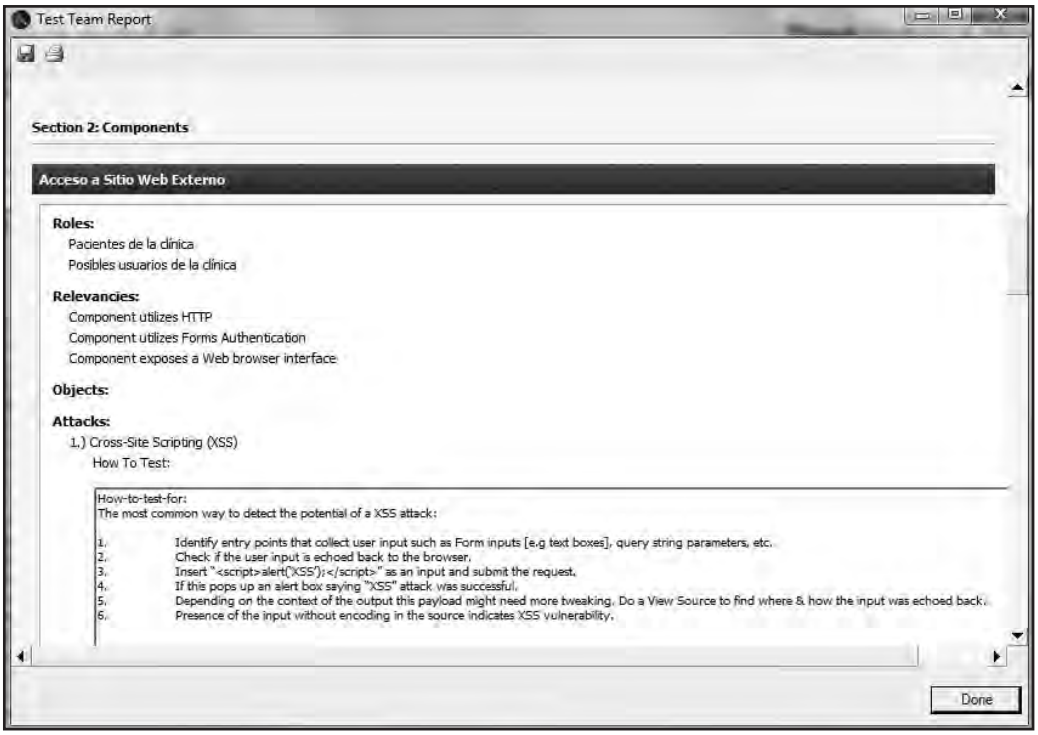


Figura 6.6.3. Informes de *Threat Analysing & Modeling*.

al máximo posible. En el caso de que quieran realizarse los tests en un escenario lo más cercano al real, se recomienda, como en situaciones anteriores, la utilización de escenarios virtualizados. La capacidad para convertir los sistemas físicos en virtuales, permite la realización de pruebas en escenarios lo más cercano a la situación real. No hay que olvidar, de todas formas, que en la realización de pruebas deberán extremarse las precauciones, especialmente si se realiza en los entornos de producción o utilizando datos reales.

6.7. Protección de la información

El fin último de la seguridad consiste en la protección de los datos, que en el caso de la Administración Pública, se corresponde directamente con la protección de los ciudadanos. No en vano, otra norma anterior como la Ley 15/1999 de Protección de Datos de Carácter Personal (LOPD), reconocía esa importancia y su Real Decreto de Desarrollo el 1720/2007, exigía también la aplicación de medidas en función del tipo de datos manejados. La Administración Pública también está sometida a esta ley, que siendo de tipo orgánica, reviste una importancia fundamental.

El ENS es consciente del hecho de que en muchas ocasiones los datos manejados por la Administración Pública estarán también tipificados como de carácter personal.

Por tanto, un sistema podrá estar sometido al ENS y sus datos tipificados por la LOPD. En este sentido y para cualquier tipo de categoría se estipula lo siguiente.

"Datos de carácter personal [mp.info.1].

Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.

Lo indicado en el párrafo anterior también se aplicará cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información."

Es decir, es necesario el cumplimiento de ambas normas y aplicar la suma de las medidas estipuladas por los dos reales decretos. No existe una contradicción de normativas, puesto que las medidas a aplicar, cuando no sean las mismas, podrán hacerlo de forma complementaria atendiendo cada una a su necesidad. Independientemente de la catalogación de los datos que establece la Ley Orgánica de Protección de Datos de Carácter Personal, el Esquema Nacional de Seguridad sigue sus propios parámetros. Estos se fundamentan en los riesgos y la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos. La valoración y calificación de la información se estipula por las medidas previstas en la protección de la información.

"Calificación de la información [mp.info.2].

Nivel BAJO

1. *Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma.*
2. *La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.*
3. *La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 43 y los criterios generales prescritos en el Anexo I.*
4. *El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.*
5. *El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.*

Nivel MEDIO

Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:

a) Su control de acceso.

b) Su almacenamiento.

c) La realización de copias.

d) El etiquetado de soportes.

e) Su transmisión telemática.

f) Y cualquier otra actividad relacionada con dicha información."

Dentro del concepto de protección de la información se incluye imposibilitar el acceso a la misma, pero también impedir su interpretación en caso de que éste haya sido posible a través de algún tipo de ataque no conocido. Esto se consigue a través del cifrado de datos que es un requerimiento para los sistemas que se hayan categorizado como de nivel alto, para el almacenamiento local o el tránsito de la información.

"Cifrado de la información [mp.info.3].

Nivel ALTO

Para el cifrado de información se estará a lo que se indica a continuación:

a) La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

b) Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en [mp.com.2].

c) Para el uso de criptografía en los soportes de información, se estará a lo dispuesto en [mp.si.2].".

Tal y como se cita, para la aplicación de mecanismos de cifrado se deberán emplear los mecanismos estipulados en las medidas de protección de comunicaciones y las medidas de criptografía aplicadas en los soportes. El cifrado con IPsec en las comunicaciones o EFS y Bitlocker permitirían el cumplimiento de estos requerimientos.

En el tratamiento de procesos de la Administración Pública, la tramitación de los documentos administrativos constituye uno de los procedimientos más habituales e importantes.

Garantizar que el proceso lo realiza la persona adecuada o que el documento obtenido es totalmente válido, constituye una necesidad a cubrir. Puesto que los sistemas informáticos facilitan la posible falsificación o modificación de documentos oficiales, deberán garantizarse procedimientos que certifiquen su validez.

El Esquema Nacional de Seguridad (ENS) estima como necesario el uso de los certificados digitales como medida de seguridad. Ésta se observará en dos medidas, como son la de firma electrónica y la de sellos de tiempo.

"Firma electrónica [mp.info.4].

La firma electrónica es un mecanismo de prevención del repudio; es decir, previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada.

La firma electrónica garantiza la autenticidad del signatario y la integridad del contenido. Cuando se emplee firma electrónica:

a) El signatario será la parte que se hace responsable de la información, en la medida de sus atribuciones.

b) Se dispondrá de una Política de Firma Electrónica, aprobada por el órgano superior competente que corresponda.

Nivel BAJO

Se empleará cualquier medio de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

1. *Los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso:*

   a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

   b) Se emplearán, preferentemente, certificados reconocidos.

   c) Se emplearán, preferentemente, dispositivos seguros de firma.

2. *Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la política de firma electrónica y de certificados que sea de aplicación. Para tal fin:*

   a) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

      1.º Certificados.

      2.º Datos de verificación y validación.

   b) Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.

   c) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes a) y b).

   d) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes a) y b).

Nivel ALTO

Se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel Medio, además de las siguientes:

a) Se usarán certificados reconocidos.

b) Se usarán dispositivos seguros de creación de firma.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].”

“Sellos de tiempo [mp.info.5].

Nivel ALTO

Los sellos de tiempo prevendrán la posibilidad del repudio posterior:

1. *Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.*
2. *Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.*
3. *Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.*
4. *Se utilizarán productos certificados (según [op.pl.5]) o servicios externos admitidos. Véase [op.exp.10].”*

Para el tratamiento de determinados procedimientos a partir de la categoría media se recomienda el uso de certificados generados por organizaciones especializadas en ello y ya citadas en el capítulo anterior. Sin embargo, para algunos otros de nivel medio y aquellos de tipo básico, podrían utilizarse los servicios de certificación que ofrece Microsoft a través de las diferentes versiones de sistema operativo servidor, desde Windows NT en adelante.

Este servicio de certificados, que admite su integración en Active Directory, permite el uso de procedimientos automatizados y controlados para la implantación de sistemas PKI. En su última versión de servidores Windows 2008 R2 se utiliza cifrado de nueva generación (CNG). Proporciona una plataforma de desarrollo criptográfico flexible que permite a los profesionales crear, actualizar y usar algoritmos de cifrado personalizados en aplicaciones relacionadas con la criptografía, como Servicios de Certificate Server de Active Directory (ADCS), Capa de sockets seguros (SSL) y Protocolo de seguridad de Internet (IPsec). CNG implementa los algoritmos de criptografía de Suite B del gobierno de EE.UU., que incluyen algoritmos para cifrado, firmas digitales e intercambio de claves. CNG aporta las siguientes capacidades:

- Permite a los clientes usar sus propios algoritmos criptográficos o implementaciones de algoritmos criptográficos estándar. También es posible agregar algoritmos de nueva generación.

- CNG es compatible con la criptografía en modo kernel. La misma API se usa tanto en el modo kernel como en el modo usuario para admitir todas las características de criptografía. La Capa de sockets seguros/Seguridad de la capa de transporte (SSL/TLS) e IPsec, además de los procesos de arranque que usan CNG, funcionan en modo kernel.
- El plan para CNG incluye adquirir certificación de nivel 2 del Estándar federal de procesamiento de información (FIPS) 140-2 junto con evaluaciones de Criterio común.
- CNG reúne los requisitos de Criterio común mediante el uso y el almacenamiento de claves de larga duración en un proceso seguro.
- CNG es compatible con el conjunto actual de algoritmos CryptoAPI 1.0.
- CNG proporciona compatibilidad con los algoritmos de criptografía de curva elíptica (ECC), Suite B del gobierno de EE.UU. Para ello, requiere una serie de algoritmos ECC.
- Cualquier equipo con un Módulo de plataforma segura (TPM) puede proporcionar aislamiento y almacenamiento de claves en TPM.

El siguiente grupo de medidas persiguen abordar una serie de problemas que a menudo no son considerados, como puede ser la limpieza de metadatos de documentos. Estos pueden suministrar información significativa que podría ser utilizada contra la organización. La disposición de esta información por parte de personas inapropiadas podría permitir la realización de un ataque posterior apoyado en información privilegiada o, incluso, dañar la imagen de la organización.

Un claro ejemplo se produjo en el año 2003 con el gobierno británico. Cuando se cernía el comienzo de la guerra de Irak, Tony Blair presentó un informe en la cámara alta del gobierno británico que había sido recibido del servicio de inteligencia de los Estados Unidos. Dicho informe se presentó como una prueba irrefutable de que en Irak existían armas de destrucción masiva. El presidente fue preguntado repetidas veces si ese documento había sido manipulado, modificado o tratado de alguna forma por el gobierno británico y la respuesta siempre fue negativa.

Sin embargo, el documento fue publicado en el sitio web del gobierno sin tener en cuenta los posibles metadatos y la información oculta que pudiera contener. El documento en cuestión había sido escrito en formato .doc, el formato nativo de Microsoft Word, y resultó que, al hacer un análisis de los metadatos, apareció una lista de ediciones realizadas por ciertos usuarios que demostraban que el documento sí había sido manipulado por personal del gobierno británico.

A través de los metadatos, se puede extraer información tal como el direccionamiento utilizado en la red interna, nombres de usuarios y de servidores, información de versiones de productos y otros datos de carácter crítico. La siguiente imagen (Figura 6.7.1) muestra el resultado de la extracción de información de metadatos realizada con la herramienta FOCA de Informática64.

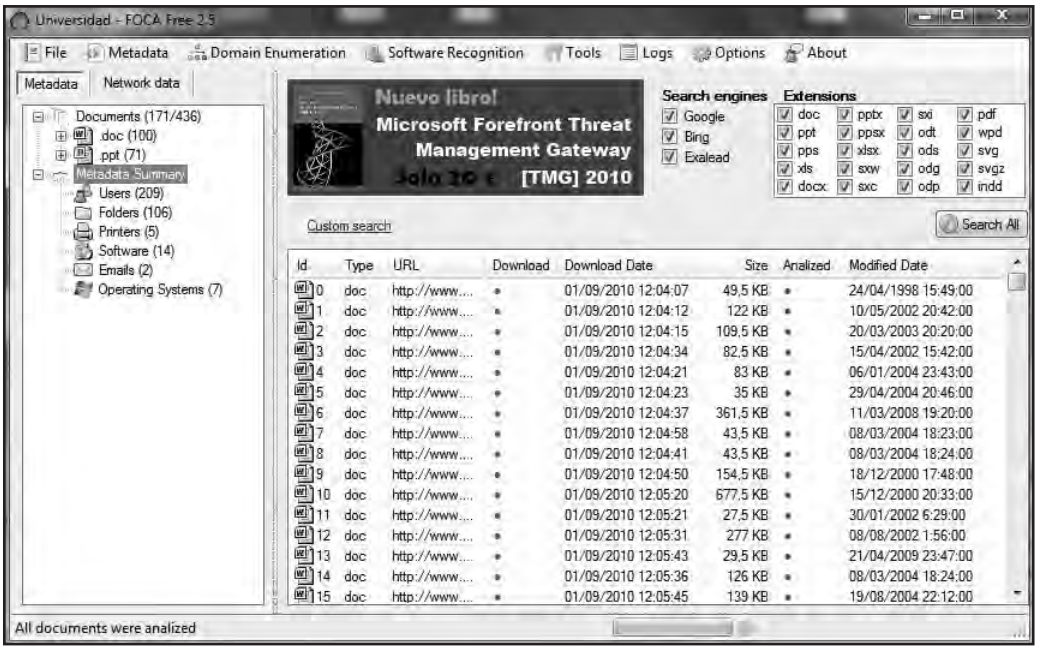


Figura 6.7.1. Extracción de metadatos con FOCA.

Aunque inicialmente no consista en un ataque directo, la existencia de metadatos o información adicional en documentos se considera una forma de fuga de información significativa. El Esquema Nacional de Seguridad recoge la necesidad de tratarlos adecuadamente en cualquiera de las categorías.

"Limpieza de documentos [mp.info.6].

En el proceso de limpieza de documentos se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.

b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.

c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer."

Aunque las aplicaciones como MS Office presentan mecanismos para la limpieza de metadatos, estos procedimientos deben ser realizados de forma manual y dependerán por tanto del buen hacer del usuario, un factor de difícil control (véase la Figura 6.7.2).

Para procedimientos de limpieza automatizada en los servidores web de MS Internet Information Server y otros tales como Microsoft SharePoint Server 2010, que hacen uso de sus servicios relacionados con el tratamiento de documentos, Informática 64 ha desarrollado Metashield Protector (véase la Figura 6.7.3). Esta solución que obtuvo un premio a la innovación en el año 2009 entregado por la revista Red Seguridad, presenta como base fundamental la limpieza de documentos presentados a través de servicios web. La solución funciona como un módulo de Internet Information Services y está totalmente integrada con la arquitectura del servidor web. Así, cuando el servidor web recibe la petición de un fichero ofimático, éste será entregado a MetaShield Protector para que lo limpie en memoria. Una vez que se han eliminado todos los metadatos del fichero o se han establecido unos previamente definidos por el administrador se entregará al cliente. MetaShield Protector se instala a nivel de servidor web y se activa o desactiva en cada sitio web de forma independiente.

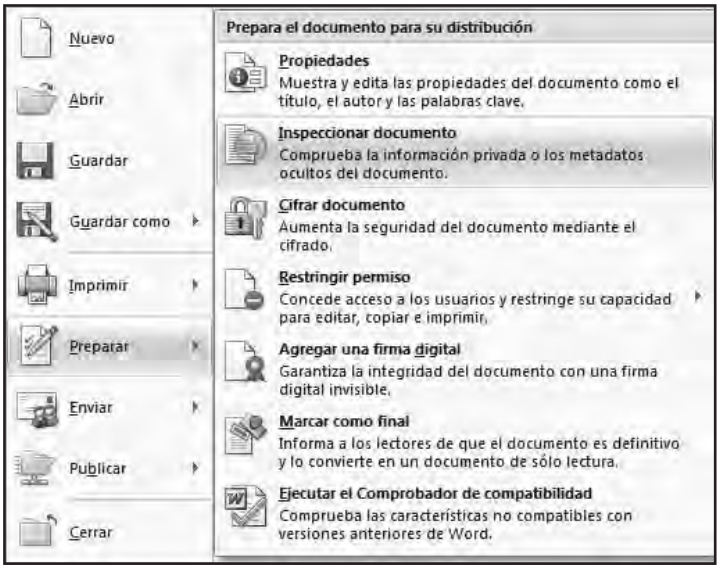


Figura 6.7.2. Tratamiento de la información privada en MS Word.

Para cada uno de los sitios será posible personalizar cuáles son los formatos de documento que han de ser limpiados de metadatos. En la última versión del producto se puede activar la limpieza para documentos Microsoft Office en binario, es decir, versiones desde MS Office 97 a MS Office 2003, de ficheros .doc, .xls, .pps o .ppt, ficheros de versiones OOXML para MS Office 2007, tipo docx, xlsx, ppsx o pptx, ficheros en formato PDF y ficheros de OpenOffice de tipo sxw, ods, odp, odt y odg. La configuración de la herramienta permite que ésta se realice por cada sitio web presente en el servidor permitiendo así al administrador realizar una administración granular, y optimizar los tiempos de respuesta de todos y cada uno de los sitios.

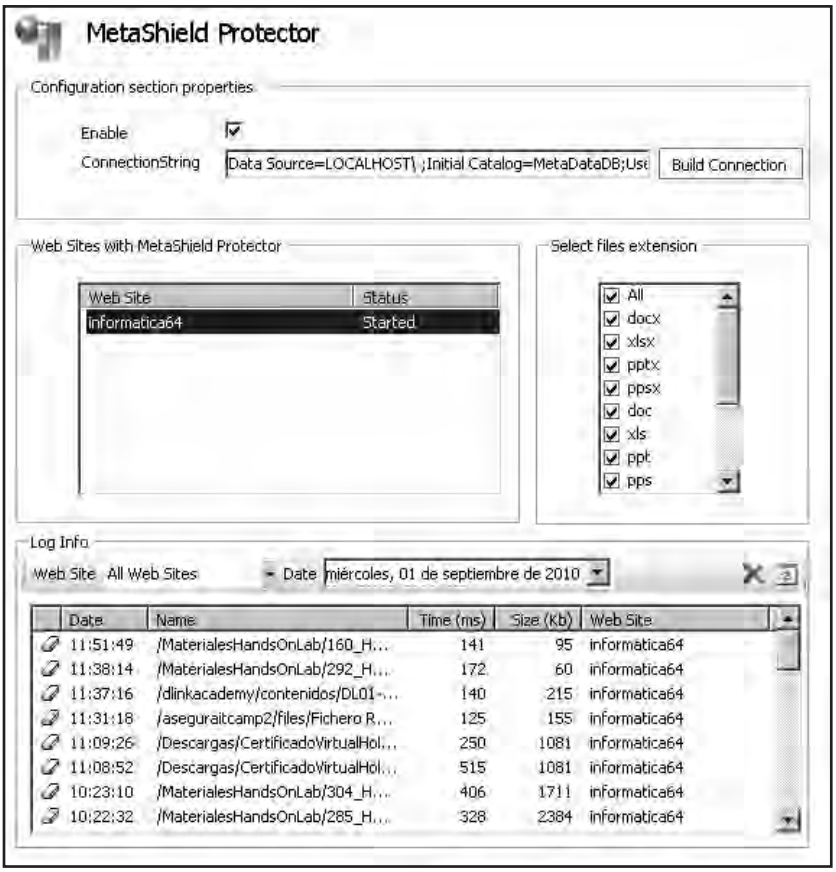


Figura 6.7.3. Limpieza de documentos con Metashield Protector en IIS.

La opción automatizada de limpieza resulta muy interesante puesto que independiza la seguridad del buen hacer del usuario. Aunque los usuarios sean conscientes de la necesidad, desafortunadamente se enfrentan a que en el trabajo diario, esta limpieza no siempre se realiza, o bien no se hace correctamente.

La última de las medidas previstas en el ENS para la seguridad de la información consiste en la necesidad de realizar copias de seguridad. De este modo, en caso de que se haya producido una incidencia será posible recuperar la información bien sobre el sistema en producción original o bien en uno alternativo. Los mecanismos de copia deberán estar previstos a partir del nivel medio de los sistemas categorizados.

"Copias de seguridad (backup) [mp.info.9].

Nivel MEDIO

Se realizarán copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada.

Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de respaldo deberán abarcar:

a) Información de trabajo de la organización.

b) Aplicaciones en explotación, incluyendo los sistemas operativos.

c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

d) Claves utilizadas para preservar la confidencialidad de la información."

Aunque muchos de los productos de Microsoft cuentan con su propio sistema de copia de seguridad, existe un servicio que permite la unificación y tratamiento de copia de seguridad de todos ellos. Bien sea de sistema operativo, bases de datos, sistemas de gestión de certificados, sistemas de virtualización o correo electrónico, MS System Center Data Protection Manager ofrece soluciones en modo agente servidor para todos ellos. En su versión 2010, aunque presenta los mismos objetivos fundamentales de sus antecesores, se han potenciado algunas de las funcionalidades:

- La capacidad para disponer de políticas de gestión centralizada para la protección y recuperación de datos de servidores de ficheros, de sistemas operativos y estaciones de trabajo.
- Mejora de la protección de escenarios de virtualización, incluyendo tecnologías de Hyper-V LiveMigration R2 y la posibilidad de recuperar un solo archivo dentro de copias de seguridad basadas en host.
- Se pueden obtener capacidades de protección y recuperación para servidores de aplicaciones de Windows basados en infraestructuras de base de datos como MS SQL Server, MS Exchange Server o MS SharePoint Server.
- Replicación nativa de sitio a sitio para la recuperación ante desastres, ya sea en otro servidor DPM o un proveedor de servicios ubicado en la nube.
- Significativo aumento de la escalabilidad empresarial para el despliegue de DPM en entornos de gran tamaño, junto con un sistema de gestión centralizada de su estado y procedimientos de recuperación.

6.8. Protección de los servicios

La permanente evolución de los sistemas es una realidad incuestionable. La prestación de servicios a través de Internet ha modificado las formas tradicionales de actuación de las organizaciones. De este modo, hechos como la progresiva sustitución del correo ordinario o el fax en favor del correo electrónico se han generalizado para

la práctica totalidad de las organizaciones. Lógicamente, la Administración Pública no es ajena a estos avances e incorpora dentro de sus procedimientos las ventajas que las nuevas tecnologías ofrecen, especialmente Internet.

Sin embargo, los servicios de Internet, junto a múltiples ventajas, han traído también inconvenientes a las organizaciones, haciendo necesario enfrentarse a nuevos problemas que los sistemas tradicionales no presentaban. Los posibles ejemplos son muchos. Una organización no se veía acosada por una gran cantidad de publicidad en su correo tradicional. Sin embargo, en el correo electrónico, el spam o correo basura constituye un hecho tan común que incluso se encuentra tipificado en la legislación española. La dispersión de malware a través del correo electrónico es otro reto a afrontar para minimizar los nuevos riesgos y amenazas a las que se ven sometidas las organizaciones por el uso de servicios de Internet.

El Esquema Nacional de Seguridad (ENS) aborda también la seguridad de los sistemas, desde la perspectiva de los servicios. No sólo la información, sino el propio servicio, como medio para la prestación de las funciones, debe ser protegido celosamente. Un servicio débil constituye una forma propiciatoria para obtener una información, a la que normalmente no se debería poder acceder. La protección de los servicios constituye por tanto una necesidad. El ENS presta especial atención al correo electrónico y a los servicios web, atendiendo a su uso generalizado y su carácter crítico. Por otra parte, se observa la continuidad del servicio como una prioridad fundamental, propiciando la aplicación de medidas técnicas que eviten posibles ataques de denegación de servicio.

6.8.1. Protección del correo electrónico

El correo electrónico se ha convertido en uno de los servicios más populares y de uso más generalizado por parte de las organizaciones. Constituye un elemento tan estratégico que la pérdida del mismo podría suponer serios problemas estructurales en una entidad. Muchos de los procesos de comunicación, incluso de carácter interno, se realizan mediante este mecanismo, sustituyendo a otros como la telefonía convencional. El abaratamiento de costes y la capacidad de comunicación son las banderas principales de este servicio.

Sin embargo, es evidente que además de considerables ventajas también presenta riesgos. Puesto que la comunicación, tanto interna como externa, a través del correo electrónico viaja por numerosas redes, es necesario garantizar la confidencialidad de la misma. Por otra parte, la recepción del correo basura no sólo constituye una incomodidad desde el punto de vista del usuario, sino que también implica el uso innecesario de recursos de almacenamiento.

Este tipo de correos constituyen en muchas ocasiones el noventa por ciento de la información que recibe una organización a través del servicio de mensajería. El almacenamiento, tratamiento y copiado del mismo supone por tanto un incremento notable en los costes finales si no es tratado adecuadamente.

El ENS trata proporcionalmente la protección del servicio de correo electrónico desde el nivel más básico. Para ello solicita de las organizaciones la aplicación de las siguientes medidas.

"Protección del correo electrónico (e-mail) [mp.s.1].

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico se protegerá tanto en el cuerpo de los mensajes, como en los anexos.

b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

1º Correo no solicitado, en su expresión inglesa «spam».

2º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.

3º Código móvil de tipo «applet».

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:

1º Limitaciones al uso como soporte de comunicaciones privadas.

2º Actividades de concienciación y formación relativas al uso del correo electrónico."

La aplicación de las medidas de carácter técnico busca el control de cuatro amenazas habituales del correo electrónico:

- Suplantación del correo electrónico.
- Captura de correo electrónico.
- Distribución del malware.
- Correo basura.

MS Exchange Server 2010 cuenta con mecanismos nativos e implantados por defecto para garantizar la comunicación segura en todos los ámbitos de la comunicación interna. La comunicación entre los diferentes roles de servidores intervinientes en la comunicación, Hub Transport o Edge Transport por poner un ejemplo, presentan mecanismos predeterminados para la comunicación segura mediante TLS. MS Exchange Server también proporciona sistemas seguros para la conectividad del cliente: bien a través de los accesos de MS Outlook con el cliente pesado, o bien en conexiones a través de HTTPS, como las que se realizan con Outlook Web App (OWA) u Outlook

Anywhere, garantizando en todo momento la confidencialidad en el acceso del usuario a su buzón. (Véase la Figura 6.8.1.)

Sin embargo, en el intercambio de correos que realice la entidad a través de Internet, el protocolo estandarizado SMTP (*Simple Mail Transfer Protocol*) no emplea de forma nativa ningún mecanismo que garantice la seguridad de la comunicación. Aunque MS Exchange Server ofrece mecanismos para el intercambio seguro mediante una implementación de SMTP sobre TLS, éste no es un mecanismo habitualmente empleado por las entidades y, por tanto, no puede garantizarse siempre la seguridad del servicio.

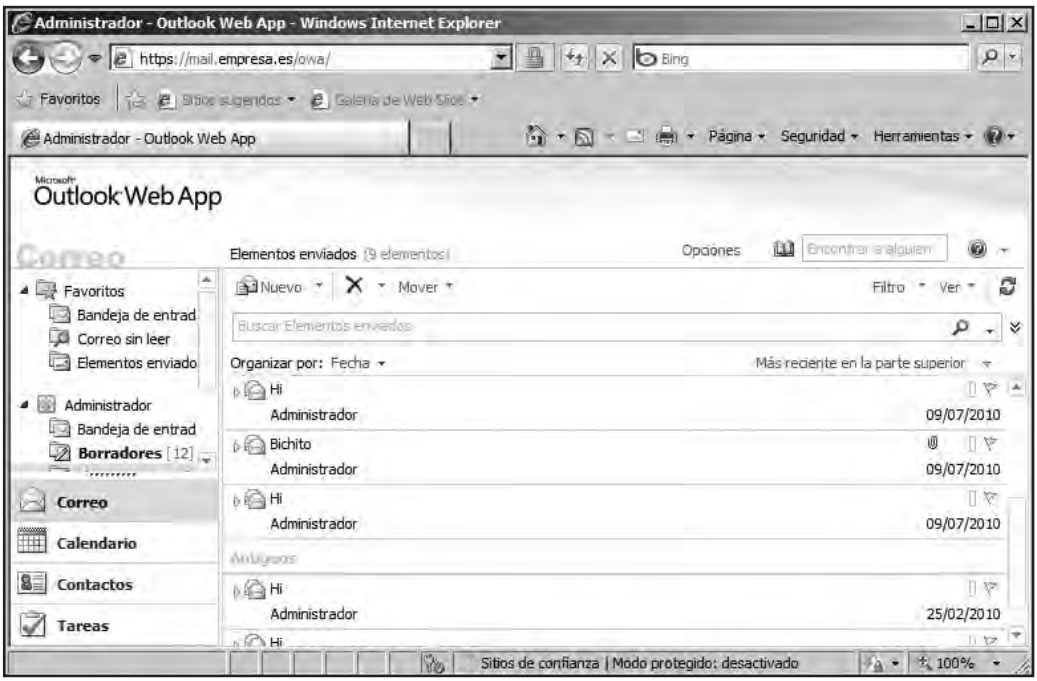


Figura 6.8.1. Acceso HTTPS Outlook Web App.

No obstante, el sistema de correo electrónico presenta de forma estándar mecanismos para garantizar la autenticidad e integridad de los mensajes intercambiados entre dos usuarios. S/MIME (*Secure / Multipurpose Internet mail Extensions*) proporciona un sistema basado en el uso de certificados digitales que puede ser empleado tanto para el firmado como para el cifrado de correo electrónico. Tanto los clientes Microsoft, Outlook, OWA o Windows Mail, como el propio servidor, son capaces de tratar correctamente los correos electrónicos asegurados. Sin embargo, esto presenta el inconveniente de que los sistemas de análisis perimetral de correos electrónicos perderían su eficacia al tener que realizar un tratamiento de mensajes que se encontrarían cifrados. Se requiere en este sentido que la aplicación de la seguridad se realice en el puesto cliente.

El empleo de S/MIME y la comunicación segura, sumado a los mecanismos de autenticación tanto para el acceso al buzón como para el envío de correo desde la organización, proporcionan mecanismos suficientes para garantizar la seguridad frente a la suplantación interna o el acceso indebido a correos en tránsito. No obstante, asegurar la identidad de la procedencia de un correo necesita mecanismos adicionales. Microsoft ha liderado un proyecto denominado SenderID que persigue este fin.

El objetivo básico de este framework es realizar consultas al servicio DNS de una organización intentado identificar su registro SPF (*Sender Policy Framework*) si éste se encontrase publicado. Dicho registro identificará los nombres y direcciones IP de los servidores MTA (*Mail Transfer Agent*) encargados de enviar los correos electrónicos de una entidad. Dicha información se contrastará con la que aparece en la cabecera de los correos electrónicos y que permite identificar el servidor MTA que envió el correo. La coincidencia o no de dicha información definirá si el correo ha sido o no suplantado. La respuesta positiva o negativa, o bien si la organización no tiene declarado el registro SPF, determinarán el comportamiento del servidor MS Exchange Server ante los mensajes (véase la Figura 6.8.2). Si desea más información o conocer si su empresa dispone del registro SPF creado, puede acceder a la siguiente dirección URL: http://www.microsoft.com/senderid.

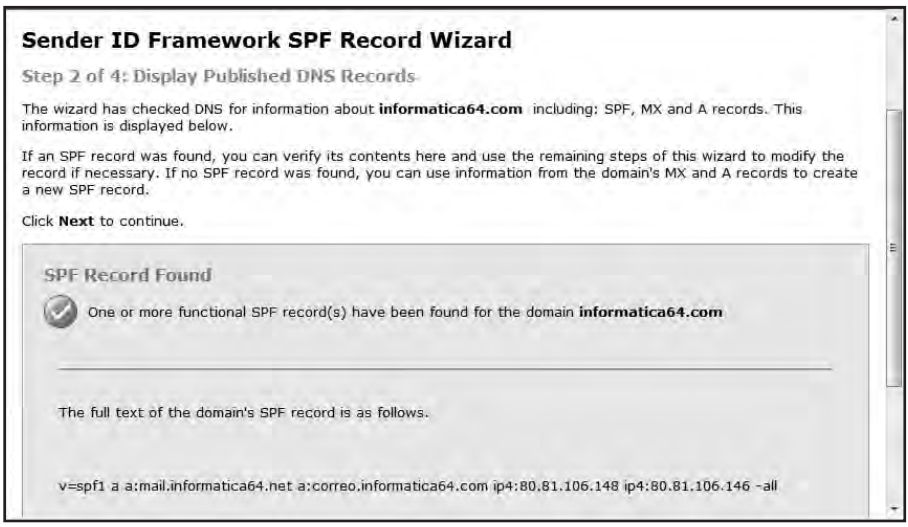


Figura 6.8.2. Consulta del registro SPF.

Una de las mayores preocupaciones de las organizaciones es la inseguridad que pueden ocasionar determinados correos tratados por ciertos usuarios. El spam constituye un procedimiento muy invasivo, no sólo por la cantidad de información inútil que genera, sino en ocasiones también por el contenido de ésta. Desafortunadamente, son habituales los casos de personas estafadas al proporcionar datos importantes en base a la información que portaba un correo proveniente supuestamente de una entidad bancaria. Estas técnicas maliciosas son conocidas como phising. El término

identifica estos nuevos mecanismos de estafa relacionados con las nuevas tecnologías que emplean la ingeniería social para hacer creer algo que realmente no es. También el spam y la ingeniería social sirven para que los usuarios abran a veces ficheros adjuntos que en un gran porcentaje tendrán contenido vírico y que pueden afectar de muchas formas a los sistemas de la organización. En definitiva, son múltiples las técnicas maliciosas y los casos que hacen uso del correo electrónico para el desarrollo de acciones malintencionadas, incluso delictivas.

Las organizaciones tienen, por tanto, la necesidad de luchar contra estas amenazas, contrarrestando el spam e impidiendo la entrada de malware a través del servicio de correo electrónico. Sin embargo, junto a lo anterior deberán intentar en la medida de lo posible minimizar el número de falsos positivos. Estos constituyen en esencia mensajes buenos que por uno u otro motivo han sido identificados como potenciales amenazas. El exceso de celo puede en sí mismo ser también un riesgo para la prestación del servicio.

Microsoft cuenta en MS Exchange Server 2007 y 2010 para garantizar la seguridad de los correos electrónico con MS Forefront Protection for Exchange 2010. En junio del año 2005 Microsoft hacía de la empresa Sybari una filial de la compañía. Con ello Microsoft incorporaba uno de los productos líderes en el mercado de soluciones antivirus multimotor y antispam para servidores de correo electrónico, Antigen. Su base funcional consistía en la implementación de un sistema multimotor para el correo electrónico, así como procedimientos para la detección y eliminación de spam, a través de la aplicación de diferentes filtros que el administrador podía configurar.

El sistema multimotor aporta la ventaja de poder actuar con más de un sistema antimalware, permitiendo una tasa de detección y eliminación mucho más alta que con los sistemas convencionales de un único motor. Los motores con los que cuenta actualmente MS Forefront Protection for Exchange 2010 son:

- Microsoft Antimalware Engine.
- Authentium Command Antivirus Engine.
- Karpersky Antivirus Technology.
- Norma Virus Control.
- VirusBuster Antivirus Scan Engine.
- Anti Worm.

Para la realización de una detección eficaz haciendo uso de varios motores, MS Forefront Protection for Exchange se basa en la técnica de análisis a través de escaneo en la memoria, mucho más eficaz que los sistemas de análisis en disco. Esto se suma al empleo de varios procesos para la realización de los diferentes test. El administrador podrá definir la estrategia que desea utilizar para los procedimientos de análisis. Puede sumar el empleo de múltiples roles para analizar con diferentes motores y según qué circunstancias los correos que entran o salen de una organización. Existen para

ello diferentes opciones en las que se evalúan no sólo los motores activados para una determinada tarea, sino también la disponibilidad de los mismos en el momento de que se lleve a cabo la identificación:

- Examinar con todos los motores.
- Examinar con el subconjunto de motores disponibles.
- Examinar con un subconjunto de motores seleccionado dinámicamente.
- Examinar con un solo motor.

La selección de los motores más adecuada se basa en las actualizaciones disponibles y las tasas de acierto y detección realizadas previamente. Este mecanismo, denominado selección dinámica, aporta una gran eficacia a la hora de detectar potencial malware. (Véase la Figura 6.8.3.)

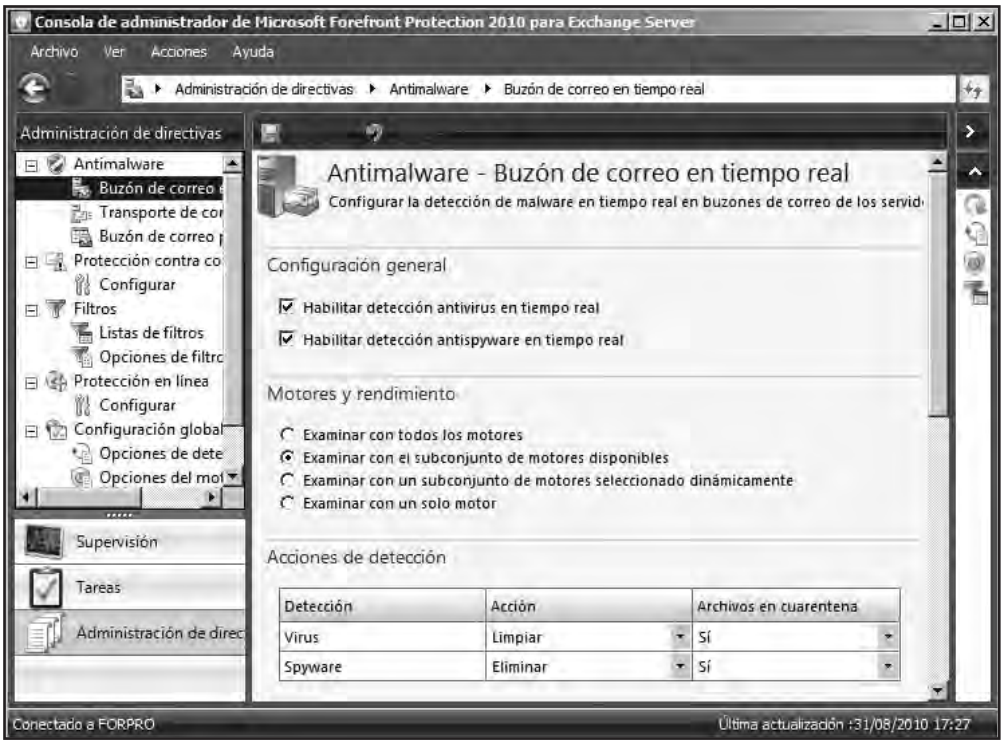


Figura 6.8.3. Selección del tipo de análisis.

Cuando un malware es detectado, se inicializa un procedimiento que permite definir qué hacer con el fichero que se encuentra infectado. Es posible diferenciar las acciones a realizar y el tratamiento en la cuarentena. Para ello se puede seleccionar:

- Omitir detección.

- Limpiar.
- Eliminar
- Suspender.

Determinadas opciones, como las de limpieza o eliminación, llevan definidas de forma predeterminada que los adjuntos sean sustituidos por mensajes que podrán ser editados por el administrador y que proporcionarán al usuario información sobre dicha acción. El mensaje, además de contener un texto identificativo de la acción, podrá estar sujeto a información preceptiva de seguridad de la organización, permitiendo identificar tanto el fichero como el malware (véase la Figura 6.8.4).

Todos los mensajes que proporciona MS Forefront Protection for Exchange 2010, tanto en la sustitución de un malware como en las notificaciones configuradas, son totalmente personalizables.

Figura 6.8.4. Adjunto con malware.

Sin embargo, la solución antimalware no es la única que ofrece MS Forefront Protection for Exchange 2010. También aporta una solución Antispam Premium que se suma a la funcionalidad que contra el correo basura proporciona el propio MS Exchange Server 2010. Este último aporta los siguientes mecanismos de filtrado:

- Filtrado de la conexión.
- Filtrado del contenido.
- Filtrado de los destinatarios.
- Filtrado de los remitentes.
- Sender ID.
- Reputación del remitente.

A estos, MS Forefront Protection for Exchange 2010 añade:

- **Filtrado de la conexión.** Examina la dirección IP del remitente original. Dispone de listas de direcciones IP estáticas configurables bloqueadas y permitidas, y una lista de DNS dinámicos bloqueados que Microsoft mantiene y que puede filtrar hasta el 90% de correo electrónico no deseado.

- **Filtrado de remitentes.** MS Forefront Protection for Exchange 2010 examina la información de los remitentes SMTP. Este filtro permite a los administradores configurar los remitentes permitidos y los bloqueados, en función de los dominios y las direcciones origen de los correos electrónicos.
- **Filtrado de id. de remitentes.** Se utiliza un marco de identificadores de remitente para validar que éste no está suplantando la identidad de otro.
- **Filtrado de los destinatarios.** Es posible configurar el permiso o bloqueo de los mensajes de correo electrónico dirigidos a ciertos destinatarios de la organización. Además, MS FPE presenta la capacidad, a través de las consultas del servicio de dominio de Active Directory, de validar que el destinatario exista en dicho servicio de la compañía.
- **Filtrado del contenido.** Se examina el contenido del propio mensaje, incluyendo la línea de asunto y el cuerpo del mensaje. MS FPE usa un motor de protección contra correo no deseado de terceros para detectar este tipo de correo en todos los mensajes.
- **Filtrado de retrodifusión.** Microsoft Forefront Protection for Exchange 2010 incluye una nueva tecnología que permite a los administradores evitar que los informes de no entrega (NDR) falsos que se generan en direcciones de remitente falsas entren en el entorno.

Adicionalmente, se pueden aplicar una serie de filtros globales para capacidades de detección y eliminación de determinados elementos en correos electrónicos (véase la Figura 6.8.5). Estos filtros se aplican como opciones de configuración manual por parte del administrador, para controlar la mensajería electrónica atendiendo a los criterios específicos de la organización.

- **Filtrado de remitentes permitidos**. Permite que se omitan determinados tipos de filtros para los remitentes que se especifiquen. Se trata de una lista blanca de remitentes a los que no se les aplicarán el resto de los filtros.
- **Archivo**. Filtrará mensajes que contengan nombres o tipos de datos adjuntos a correos electrónicos.
- **Palabra clave.** Permite establecer criterios de palabras en el cuerpo del mensaje para el bloqueo de correos electrónicos.
- **Línea de asunto.** Similar al filtro anterior, pero en este caso la detección se realizará sólo en el asunto del mensaje.
- **Remitente o dominio**. Permite filtrar mensajes de los remitentes o dominios que se especifiquen. Se trata de una lista negra de remitentes.

Aunque estos sistemas no dinámicos pueden generar una alta tasa de falsos positivos si no son utilizados adecuadamente, son una herramienta eficaz en determinados escenarios. Por ejemplo, se podría conocer un determinado malware de reciente aparición que se está distribuyendo en un tipo de correo muy característico y para el

que todavía no existe la firma correspondiente. A través del filtrado de archivo, palabra clave o línea de asunto podría bloquearse su distribución hasta la aparición de la firma adecuada. O bien, determinado correo que está invadiendo masivamente los buzones de los usuarios y no es detectado adecuadamente, podría ser identificado y filtrado atendiendo a alguna de sus características.

Los mecanismos que se proporcionan para identificar, notificar y hacer un seguimiento de las amenazas, constituyen un elemento fundamental para los administradores. En todo momento, éstos disponen de la información de todos los detalles de incidencias que han tenido lugar, así como de las estadísticas de detección y filtrado correspondientes. (Véase la Figura 6.8.6.)

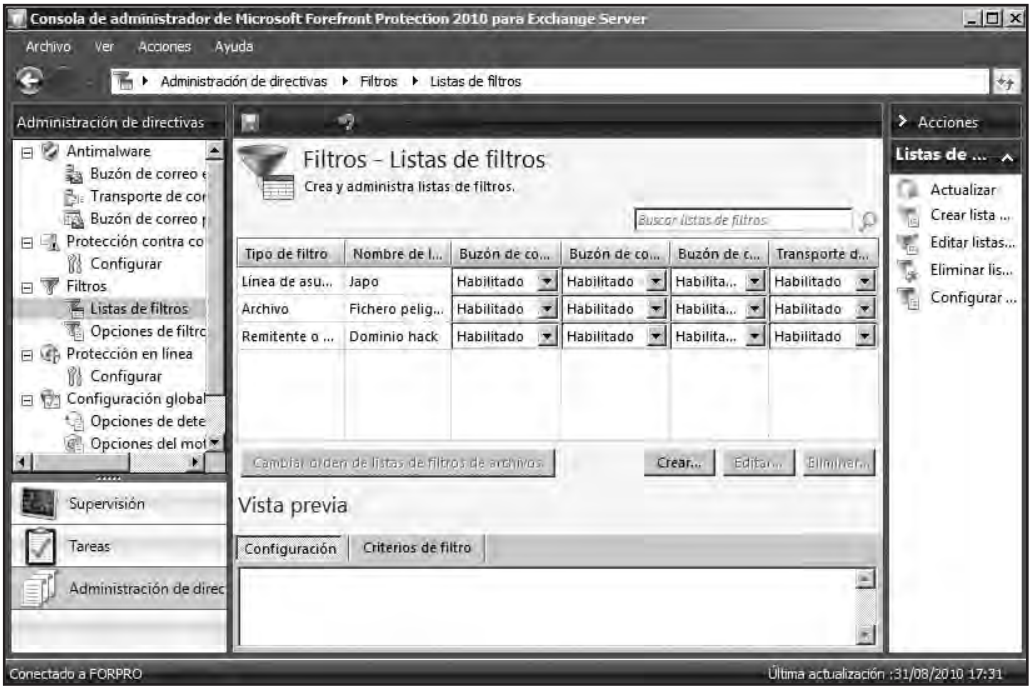


Figura 6.8.5. Configuración de filtros en MS FPE 2010.

Se permiten emplear mecanismos de notificación para que tanto el administrador como los usuarios sean conscientes de los incidentes que hayan tenido lugar con el servicio de correo electrónico. Los usuarios podrán solicitar que el administrador pueda recuperar de la cuarentena ficheros adjuntos que hayan podido ser eliminados o correos filtrados por los diferentes sistemas activados en el servidor.

La suma de todas las capacidades de MS Forefront Protectión for Exchange le facultan como una de las mejoras soluciones en la actualidad para la protección del correo electrónico.

Figura 6.8.6. Monitorización de incidencias en MS Forefront Protection for Exchange.

6.8.2. Protección de servicios y aplicaciones web [mp.s.2]

Los ataques a servidores web constituyen una de las amenazas más visibles que sufren las organizaciones por parte de los hackers. Notables son algunos de los ataques que se han realizado a lo largo de la historia afectando por igual a entidades públicas y privadas, a grandes y pequeñas organizaciones. Los objetivos son múltiples. La alteración de la información proporcionada vía web, el acceso a información y servicios internos o la generación de un daño en la imagen de la organización, son algunos de sus posibles efectos negativos.

El Esquema Nacional de Seguridad recoge algunos de los mecanismos de ataque ampliamente utilizados, conminando a luchar contra los mismos y aplicando para ello medidas de protección adecuadas.

"Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.

a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:

1º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

2º Se prevendrán ataques de manipulación de URL.

3º Se prevendrán ataques de manipulación de los fragmentos de información que se almacenan en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página; dichos fragmentos se conocen con el término inglés «cookies».

4º Se prevendrán ataques de inyección de código.

b) Se prevendrán intentos de escalado de privilegios.

c) Se prevendrán ataques de «cross site scripting».

d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cachés».”

Aunque las medidas van enfocadas principalmente a la aplicación de principios de desarrollo de código seguro, existen mecanismos adicionales que permiten el bloqueo de determinados ataques. Para el propio servidor web, se aporta por parte de MS Internet Information Service en sus últimas versiones, un nuevo diseño basado en la modularidad y en la utilización de las herramientas de seguridad incluidas:

a) **URL Authorization.** Permite el control de acceso a sitios o archivos sin la aplicación de permisos NTFS.

b) **Request Filtering.** Previene el acceso a URLs con determinado texto y diferentes tamaños para evitar el desbordamiento. Impide la descarga de diferentes ficheros en función de su contenido o extensiones.

Junto a lo anterior, se proporciona también una herramienta denominada UrlScan que evoluciona de versiones anteriores. En su última versión previene determinados ataques dañinos contra aplicaciones web soportadas en IIS:

- Mitiga ataques de SQL Injection. Puede ser configurada para el filtrado de determinadas consultas y encabezados HTTP.
- Permite crear reglas independientes para cadenas de caracteres y encabezados.
- Controla secuencias de escape utilizadas habitualmente en ataques web.
- Proporciona adicionalmente un formato de logs W3C para un tratamiento adecuado a través de aplicaciones de análisis de registros como Microsoft Log Parser.

Además de las características aportadas por el servidor Internet Information Server o algunos de sus módulos, existe la capacidad preventiva para mitigar posibles ataques en el perímetro (véase la Figura 6.8.7). Una de las últimas actualizaciones del motor NIS (*Network Inspection Service*) de MS Forefront Threat Management Gateway

2010, consiste precisamente en detectar y bloquear ataques de SQL Injection y Cross-Site Scripting entre otros. Estos bloqueos se realizarán contra ataques dirigidos a servidores web publicados por la organización.

El sistema de IPS (*Intrusion Prevention System*) conjuntamente con el analizador genérico de protocolo a nivel de aplicación (GAPA), proporcionan un sistema de análisis basado en firmas para identificar los ataques que se produzcan contra la organización. Aunque originalmente incluía solamente firmas para contrarrestar ataques que mediante exploits se producían contra determinadas vulnerabilidades, últimamente se han incluido mecanismos para filtrar ataques más genéricos, como los que se producen contra sistemas web, incluidos entre ellos algunos de denegación de servicio (DoS).

Aunque inicialmente este sistema de prevención se ha explotado ya en MS Forefront TMG 2010, se implementará también sobre otros servicios tales como MS Forefront Endpoint Protection 2010. La base operacional del sistema GAPA es:

- Identificación de las sesiones.
- Evaluación del estado de las operaciones.
- Correlación de información.
- Estratificación de los protocolos.
- Análisis de tiempos, excepciones y preexistencia de sesiones.

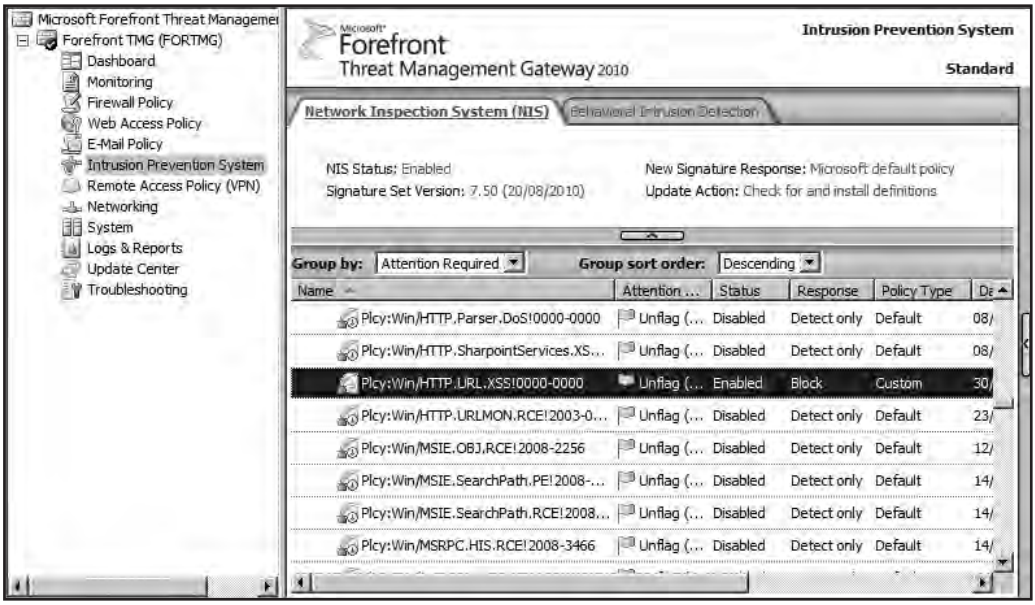


Figura 6.8.7. Prevención de ataques XSS en MS Forefront TMG 2010.

6.8.3. Protección frente a la denegación de servicios

Aunque ya ha sido tratado a lo largo del libro, el ENS remarca en todo momento la disponibilidad como una de las máximas a seguir por la Administración Pública en la prestación de los servicios. De forma expresa lo recoge en las medidas previstas en la prestación de servicios para los niveles medio y alto.

"Nivel MEDIO

Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS, Denial of Service). Para ello:

a) Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.

b) Se desplegarán tecnologías para prevenir los ataques conocidos.

Nivel ALTO

a) Se establecerá un sistema de detección de ataques de denegación de servicio.

b) Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

c) Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros."

La prevención contra los ataques por denegación de servicio comprende por tanto un objetivo a resolver para los niveles medio y alto. Nuevamente, MS Forefront Threat Management Gateway 2010 proporciona mecanismos suficientes para la prevención de ataques de denegación de servicios (véase la Figura 6.8.8).

Adicionalmente al módulo de NIS, que aporta firmas para prevenir ataques basados en la denegación contra determinados servicios, presenta una funcionalidad que previene contra el desbordamiento como técnica de ataque. Ésta impide ataques que por saturación anulen las funcionalidades que proporciona el servidor. Máximo número de conexiones por sesión o por segundo son algunos de los controles que permiten definir este sistema de filtrado. Puesto que la configuración es global para todo el sistema, se pueden generar excepciones en caso de que un cliente requiriera una conexión válida, aun superando los valores establecidos.

6.8.4. Medios alternativos

En el caso del nivel alto se requiere la existencia de medios que proporcionan alta disponibilidad.

"Se garantizará la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección que los medios habituales."

Todos los productos Microsoft citados anteriormente permiten su implantación en alta disponibilidad. Para ello, pueden desarrollarse modelos basados bien en la generación de matrices, o bien a través de granjas de servidores. En el caso de MS Forefront Threat Management Gateway 2010, como ya se ha mencionado, en su versión Enterprise cumplirá este cometido a través del servicio de NLB.

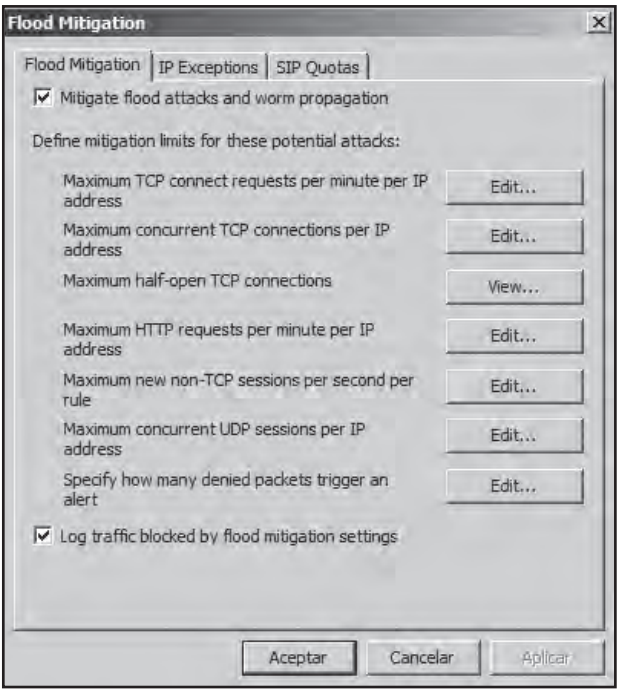


Figura 6.8.8. Prevención contra el desbordamiento en MS Forefront TMG 2010.

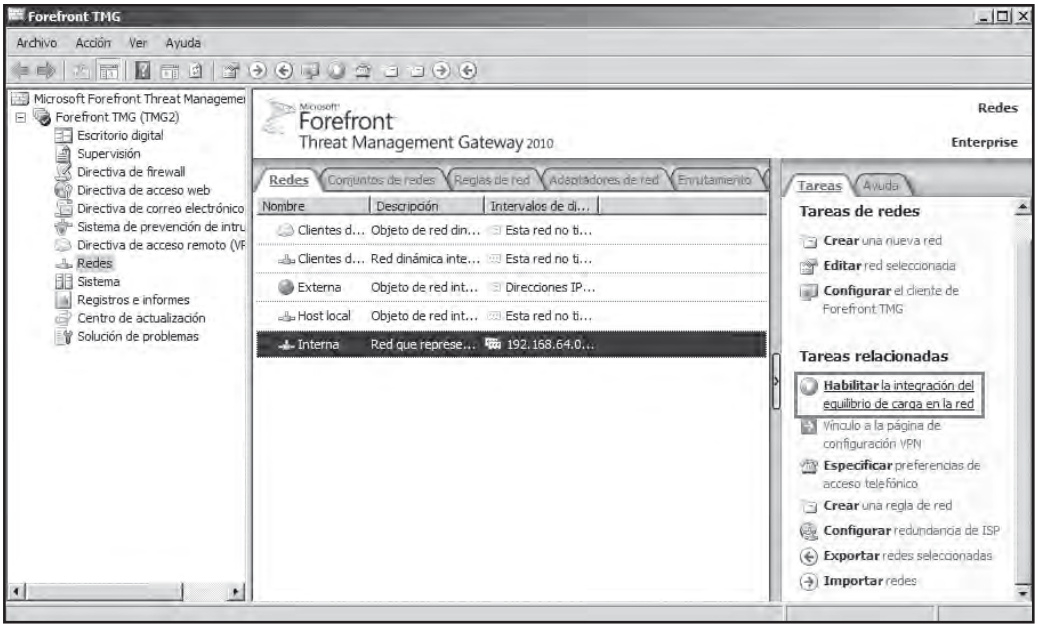


Figura 6.8.9. Habilitar la configuración NLB en MS Forefront TMG 2010.

7

Premios, reconocimientos y certificaciones de los productos Microsoft

El Real Decreto 3/2010 recoge la necesidad de utilizar productos reconocidos internacionalmente, en función de lo estipulado por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información. Además de la propia certificación de seguridad de productos y sistemas de tecnologías de la información según los procedimientos establecidos, se admiten los certificados *Common Criteria*. Estos, emitidos por diferentes organismos de certificación, se encuentran reconocidos por múltiples países, siendo España uno de sus integrantes con capacidad de emisión a través del de Certificación de la Seguridad de las Tecnologías de la Información adscrito al Centro Criptológico Nacional (CCN).

La valoración que se realiza de los diferentes productos se categoriza mediante EAL (*Evaluation Assurance Level*). Los niveles factibles van desde EAL1 a EAL7 atendiendo a los distintos argumentos de certificación y a las pruebas realizadas en laboratorio sobre los productos. Normalmente, los niveles EAL5 a EAL7 están orientados a productos con técnicas y objetivos muy especializados, por lo que no suelen emitirse a los sistemas que se distribuyen comercialmente.

Las últimas certificaciones obtenidas por productos Microsoft son:

- Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 2008 Datacenter Edition con EAL4* ALC_FLR.3.
- Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050 con EAL4* ALC_FLR.3.

- Microsoft Internet Security and Acceleration Server 2006 Standard / Enterprise Edition, Build 5.0.5720.100 con EAL4+ ALC_FLR.3 AVA_VLA.3.
- Microsoft Windows Rights Management Services (RMS) 1.0 SP2 con EAL4+ ALC_FLR.3.
- Microsoft SQL Server 2008 Enterprise Edition (English) x86 and x64, Version 10.0.1600.22 EAL1+ ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1.
- Microsoft System Center Mobile Device Manager 2008-Service Pack 1 con EAL4+ ALC_FLR.3.
- Microsoft Exchange Server 2007 Enterprise Edition (English), Version/Build 08.02.0176.002 con EAL4+.

Estas son las últimas certificaciones recibidas. Es necesario considerar que el proceso de obtención de éstas es largo. MS ISA Server 2006 obtuvo su certificación el 9 de febrero de 2009. Múltiples productos Microsoft, como los de la línea de Forefront y las versiones de sistemas operativos más actuales, Windows 7 o Windows Server 2008, han sido remitidos también para su evaluación en las diferentes categorías, siendo necesario esperar un tiempo para conocer la certificación obtenida. Es de esperar que estas certificaciones sean iguales a las de sus productos antecesores, máxime cuando los nuevos productos han mejorado sensiblemente las características y funcionalidades en el ámbito de la seguridad.

Por otra parte, las soluciones Microsoft no han obtenido exclusivamente el reconocimiento del mercado en formato de certificación del producto, sino que también diferentes premios y acreditaciones los reconocen y valoran mundialmente. Se muestra a continuación, a modo de ejemplo, los obtenidos por los productos de línea MS Forefront:

- MS Forefront Client Security ha recibido el último CESG Claims Tested Mark (CCTM) Award por protección integral. Es uno de los cuatro productos de MS Forefront que han sido finalistas en la categoría de Info Security 2008 Global Product Excellence and 2008 Outstanding Awards. La Certificación ICSA Lab en Laboratorios de Antivirus y Anti-Spyware. La Certificación West Coast Labs´Checkmark Certification y el VB100 de Virus Bulletin.
- MS Forefront Protection 2010 for Exchange Server ha sido nombrado como "2010 Hot Technology and Solution". Ha recibido la certificación West Coast Labs´Checkmark Certification y el VBSpam de Virus Bulletin.
- MS Forefront Protection 2010 for SharePoint Server ha recibido la certificación West Coast Labs´Checkmark Certification.
- MS Forefront Security for SharePoint ha obtenido el premio 2009 Global Product Excellence Award for Document Protection de Info Security Products Guide organization.
- MS Forefront Security for Office Communications Server ha recibido la certificación West Coast Labs´Checkmark.

- MS Forefront Threat management Gateway 2010 ha recibido el galardón 2010 Product Innovation Award for Anti Malware Solution de Network Products Guide, an industry-leading technology research and advisory guide.

Estos y otros productos Microsoft obtienen también posiciones destacadas en muchos de los tests de seguridad que realizan empresas independientes, llegando incluso a liderar algunos de los rankings. Este es el caso de MS Forefront Protection 2010 for Exchange Server, que en la categoría de solución Antispam de VBSpam ha obtenido los mejores registros con una puntuación superior al 96%. Para la obtención de este registro se ha hecho uso de la exigente fórmula que mide el ratio de correo Spam Detectado (*SC: Spam Caught*) y el ratio de falsos positivos (*FP: False Positive*). Estos resultados se combinan en la fórmula que da el resultado final, **Resultado = SC - (3 X FP)**.

En el año 2010, en diferentes resultados publicados sobre este mismo producto, es posible observar la obtención de las mejores puntuaciones, con el menor número de falsos positivos y el mayor porcentaje de detección de correos spam.

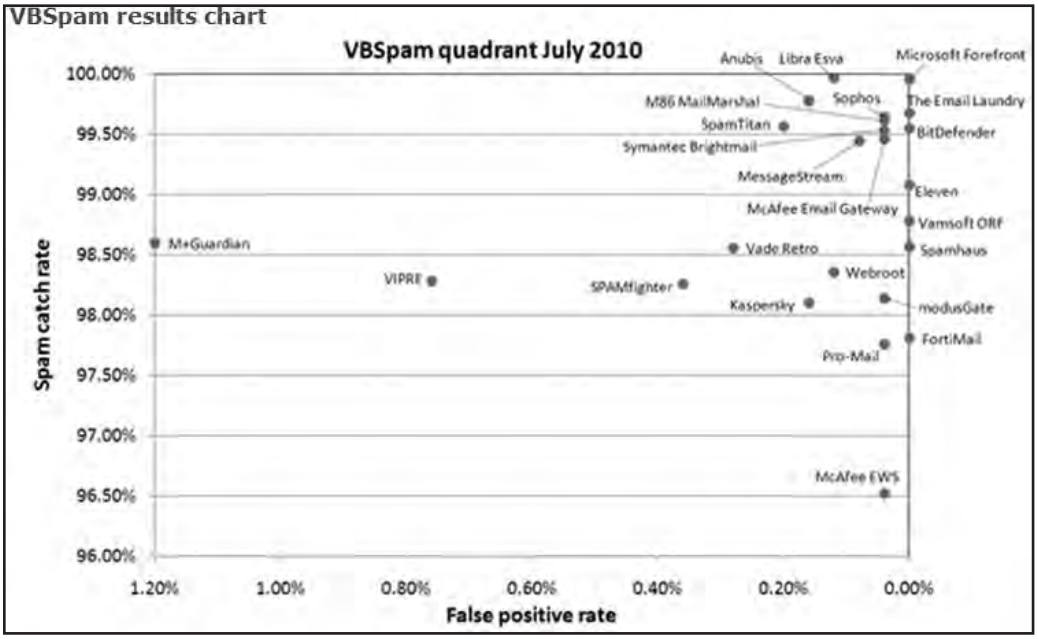


Figura 7.1. Resultado del test Antispam en Julio de 2010.

Pero también el motor antimalware cosecha buenos números en las diferentes pruebas realizadas. Destacan entre ellas las correspondientes a la detección proactiva basada en el análisis heurístico consiguiendo la más alta cualificación, *Advanced+ por AV comparatives*. Estas pruebas tienen como objetivo no evaluar el uso de firmas, sino los sistemas de detección basados en heurísticas, donde el objetivo es detectar la presencia de malware no conocido. Para ello se utiliza una misma máquina en las

mismas condiciones para todos los antivirus. Se provee a las soluciones de una firma correspondiente a un mismo día, pasando a ejecutar posteriormente diferentes tipos de malware que han hecho su aparición 10 días después de la aparición de la firma a testear. Puesto que las diferentes soluciones antimalware no contarán con la firma para detectar los virus, deberán contar únicamente con sus sistemas basados en análisis de comportamiento para detectar la presencia del malware.

El test persigue dos objetivos concretos: determinar el índice de acierto en detección, y evaluar el número de falsos positivos que puede llegar a dar el antivirus.

Finalmente, también se han cosechado importantes logros en lo concerniente a eliminación de malware o la detección de éste por firmas conocidas.

8

Seguridad y privacidad en la nube

Luis Miguel García de la Oliva (Director de Seguridad y Privacidad de Microsoft) y Héctor Sánchez (Director de Tecnología de Microsoft)

¿Cuánto podría mejorar una compañía si todos sus empleados pudiesen trabajar desde cualquier sitio y en cualquier momento? En el mundo actual, es crucial tener una visión competitiva que permita ayudar a las empresas a ser mejores.

En la mayoría de los casos, más flexibilidad, productividad y eficacia permitirán experimentar una nueva manera de trabajar y al final hacer a las compañías más rentables. Los servicios en la nube de Microsoft pretenden **hacer crecer su negocio** manteniendo la seguridad y la privacidad y facilitando a las empresas la posibilidad de dedicar más recursos a mejorar en el negocio.

Con las soluciones de los Servicios Online de Microsoft las compañías se beneficiarán de costes más bajos, back-ups automatizados, acceso universal y máxima fiabilidad – sin tener que hacer ninguna concesión-. Microsoft aplica los más altos estándares y las últimas tecnologías para permitirle centrarse en su negocio y no preocuparse por la seguridad.

8.1. Seguridad y privacidad: un proceso integral y continuo

El Programa de Gestión del Riesgo de Microsoft enmarca la estructura de seguridad y privacidad de los Servicios Online. Este programa se centra en la mejora de la seguridad y disponibilidad de los Servicios Online con un cumplimiento contrastado de los estándares de la industria en el suministro del servicio. Hace hincapié en cuatro áreas fundamentales con los siguientes requisitos:

- **Seguridad**. El entorno de Microsoft debe incluir características diseñadas para protegerle de los ataques, intencionados o no.
- **Privacidad**. Los datos y las operaciones del cliente deben ser considerados como específicos de cada uno e inaccesibles para cualquier otro cliente.
- **Continuidad**. Los servicios de Microsoft y los datos asociados de sus clientes deben estar disponibles cuando sean solicitados y deben existir unas capacidades sólidas para permitir la recuperación ante catástrofes.
- **Cumplimiento**. Los servicios de Microsoft deben operar bajo el cumplimiento de las políticas de seguridad de Microsoft y los estándares de la industria.

Las soluciones de los Servicios Online de Microsoft, que incluyen servicio de email, colaboración, desarrollo de aplicaciones y aplicaciones de negocio, están diseñadas para administradores de clientes o personal autorizado con acceso a los datos de clientes. Esta característica permite al cliente reforzar las políticas de seguridad y privacidad de su compañía.

8.2. Sistemas de gestión de Microsoft y control de acceso

El personal de Microsoft gestiona y refuerza las políticas de seguridad de forma centralizada desde los servidores dedicados a controlar y monitorizar los sistemas. Un modelo de gestión por delegación habilita a los administradores de Microsoft a tener acceso a los sistemas únicamente para desempeñar tareas específicas, reduciendo el potencial de error y permitiendo el acceso a los sistemas y funciones sólo en lo estrictamente necesario. Las medidas de seguridad a nivel de infraestructura incluyen **un modelo de administración de tres niveles que aísla las tareas administrativas y el control de acceso a sistemas** basados en el rol del usuario y en el nivel de acceso de administración para el cual el usuario está autorizado.

8.3. Eventos y actividades de registro

El acceso y las actividades de registro son facetas importantes de la seguridad. Proporcionan una forma de ayudar a contabilizar problemas importantes de seguridad, ayudan a asegurar la cuenta de usuario y puede proporcionar pruebas en caso de una brecha de seguridad. Las operaciones de los programas de los Servicios Online monitorizan y registran las actividades como registros, gestión de cuenta, acceso al directorio de servicios, acceso a objetos, cambios de política, uso privilegiado, seguimiento del proceso y eventos del sistema.

Tanto por solicitud como por periodicidad, Microsoft proporcionará registros que detallan el servicio de acceso del administrador a los buzones de mail de los usuarios para ayudar a los clientes a auditar y reforzar sus políticas relativas a la conducta adecuada de sus administradores de servicio. Estos registros también detallarán el acceso de partners de soporte y personal de soporte de Microsoft, excepto cuando lo prohíba un proceso legal.

8.4. Certificados estándar de cumplimiento

Microsoft emprende auditorías independientes y certificaciones del entorno de los Servicios Online de Microsoft para validar el diseño de control y la efectividad operativa. Las actividades de cumplimiento de Microsoft se aplican al desarrollo de servicios y despliegue físico de infraestructuras y operaciones. Los certificados de terceros permiten a los clientes no solo tener más confianza en la seguridad de las soluciones de los Servicios Online, sino que también ayudan a satisfacer sus obligaciones legales, reglamentarias y de cumplimiento.

Microsoft desarrolla estrategias de cumplimiento basadas en los siguientes estándares y certificaciones:

- Auditorías de terceros.
- Centros de datos con certificaciones SAS 70 e ISO 27001 .
- Servicios con certificaciones SAS 70 e ISO 27001.
- Servicios de infraestructura con certificaciones ISO 27001 y SAS 70.

8.5. Guía de cliente para políticas de cumplimiento

Las medidas en seguridad y privacidad comienzan por el cliente. Los Servicios Online de Microsoft incluyen documentación, aplicaciones y utilidades para que al cliente y a los administradores les resulte más fácil unirse a Microsoft y mantener sus datos seguros y privados.

Los clientes son responsables de asegurar el cumplimiento de sus propias políticas aplicables, prácticas y regulaciones adaptando de manera adecuada las características de los Servicios Online para satisfacer sus necesidades específicas. Por ejemplo, los clientes tienen la responsabilidad de aplicar las leyes de privacidad y las regulaciones relevantes; notificar y obtener el consentimiento de los empleados y otros usuarios sobre la localización de datos y procesamiento; y definir el nivel apropiado de protección para las distintas categorías de información personal recogida por su organización.

La información personal almacenada en el entorno de los Servicios Online será recogida, procesada y transferida sólo con el consentimiento del cliente o según lo requiera la ley.

Los Servicios Online de Microsoft ayudan a apoyar la estrategia definida de cada cliente para hacer frente a las leyes de privacidad generalmente aplicables. Sin embargo, Microsoft no proporciona consejo legal. Es responsabilidad del cliente el idear una estrategia de cumplimiento, evaluando la oferta de los Servicios Online y asegurando que el servicio proporciona las características apropiadas para llevar a cabo dicha estrategia.

Los clientes podrán acceder y controlar sus datos y, al final de una subscripción de cliente o del uso del servicio, podrán extraer sus datos.

8.6. Data centers, procesador y controlador de datos

Para una compañía que registra su localización en Europa y conduce ahí sus operaciones primarias, Microsoft mantiene, hoy en día, dos centros de datos en la Unión Europea para el almacenamiento principal y el backup de los datos de Servicios Online de Microsoft. Estos data centers están en Dublín (Irlanda) y Amsterdam (Holanda). Microsoft está comprometido a mantener el alojamiento principal del cliente y de caída de datos (alojamiento de recuperación por desastres) en la región y los datos en la región, sea cual sea la práctica.

Con respecto a nuestro manejo de datos personales, nosotros siempre cumpliremos la ley aplicable. Microsoft actúa como *procesador de datos*[1] para los datos de cliente, lo que incluye todo el contenido generado por el cliente durante el uso de los Servicios Online de Microsoft. Como ejemplo incluye los datos personales contenidos en mails, los archivos online de SharePoint, los datos del directorio de cliente y de las libretas de direcciones, y los registros de acceso administrativo.

Para permitir la transferencia de los datos del servicio en EEUU, Microsoft se basa en la certificación **Safe Harbor**, que incluye una certificación para **Swiss Safe Harbor Framework**.

Microsoft actúa como *controlador de datos*[2] para el registro y la facturación. Como controlador de datos, Microsoft cumple con las leyes de privacidad para transferir los datos fuera de la Unión Europea. Éste se atiene al marco de privacidad de Safe Harbor según lo dispuesto por el Departamento de Comercio de los EEUU con respecto a la recogida, el uso, la transferencia y la retención de datos de la Unión Europea, del Área Económica Europea y Suiza.

Se puede verificar el cumplimiento con los principios de Safe Harbor en la web www.Export.gov, que está gestionada por el Department of Commerce's International Trade Administration de EEUU.

MS coopera con EPA (*European Privacy Association*). EPA indica que suscribiendo sus materias al acuerdo con Safe Harbor y sus certificaciones ISO 27001 y SAS 70, los Servicios Online de Microsoft están en cumplimiento con los principios de seguridad de datos establecidos por la directiva de privacidad europea.

1 **Procesador de datos**. *Es la persona física o jurídica encargada de procesar datos personales "en nombre del controlador." En otras palabras, un procesador de datos es despojado en gran medida de la autoridad independiente de decidir cómo y por qué deben procesarse los datos personales.*

2 **Controlador de datos**. *Es la persona física o jurídica que de forma aislada, o conjunta, "determina los propósitos y los medios" para el procesamiento de los datos personales.*