Escuela Politécnica Superior
Departamento de Informática

PROYECTO FIN DE CARRERA

Ingeniería Técnica en Informática de Gestión

Auditoría de los sistemas y la seguridad en entornos mixtos (Linux - Windows)

Autor: Roberto Garrido Pelaz

Tutor: Miguel Ángel Ramos González

Leganés, Noviembre de 2014

Título: Auditoría de los sistemas y la seguridad en entornos mixtos (Linux - Windows)

Autor: Roberto Garrido Pelaz

Tutor: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 2014 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de _____.

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

A Rebeca, porque das sentido a mi vida.

Gracias a Miguel y Carmen, mis padres, por vuestro trabajo de toda una vida, por haberme enseñado el valor del esfuerzo y el trabajo. También gracias a mi hermano Miguel, por servirme de inspiración para seguir mejorando.

A mi tutor Miguel Ángel Ramos, por tu experiencia, por tu apoyo y paciencia.

Gracias a todos los que habéis contribuido a mi crecimiento personal y profesional durante estos años.

Y a la música, por acompañarme durante todos mis caminos andados.

Resumen

Los sistemas de información son ya activos estratégicos para cualquier organización, y la ventaja actual reside en el gran número de alternativas para las organizaciones en cuanto a tecnologías de la información. Nos encontramos con entornos cada vez más heterogéneos y modelos más flexibles, con los que se intenta alcanzar una ventaja competitiva a todos los niveles, y donde es fundamental el uso de ciertos protocolos y estándares tecnológicos.

Para minimizar los riesgos y amenazas asociadas al uso de las tecnologías de la información, es necesario llevar a cabo una buena gestión de la seguridad de la información, destacando el control de accesos a los recursos y la gestión de las identidades. En esta gestión eficaz es importante la revisión y evaluación periódica de la seguridad, a través de la puesta en práctica de auditorías de sistemas y de seguridad.

Existen diferentes marcos de referencias y estándares, que sirven como guías para las empresas que buscan la eficacia y eficiencia en las tareas de gestión de los activos de información. Entre estos estándares destacan por su grado de aceptación a nivel internacional COBIT e ISO/IEC 27002.

El presente proyecto trata de ofrecer una guía de buenas prácticas sencilla y asequible para cualquier tipo de organización, haciendo hincapié en la seguridad centrada en el control de accesos lógico y gestión de identidades. En el proceso de definición de este tipo de guías es importante hacer una revisión de las tecnologías disponibles en el entorno, que en este caso trata de aquellos donde conviven sistemas Windows y Linux.

Abstract

Information Systems are now strategic assets to any organization, and the current advantage consists in the large number of information technologies alternatives for enterprises. We run into more and more flexible models and heterogeneous environments, in attempts to achieve a competitive advantage at all business levels, and using technology standards and protocols is a major factor.

It is mandatory to reduce information technology associate risks and threats. This is achieved with information security management, where resources access control and identity management are noteworthy issues. For the efficient management it is important to develop regular checks and continuous assessments too, across of running security and system audits.

There are several frameworks and standards for the previous purpose, and these standards are good for enterprises that see the efficience in information assets managment as one of their principal objectives. From among these standards we can emphasize COBIT and ISO/IEC 27002, because of their international degree of acceptance.

This Project aims to provide a simple good practices guide for any kind of organization, focused on information security, with logic access control and identity management as a key factors. In this guide definition process it is important to review the technologies availables in the environment too, which in this case are limited by Windows and Linux systems

Índice

Índice de figuras

Índice de tablas

1 Introducción y Objetivos

1.1 Problema a resolver

Existen en la actualidad un gran número de marcos de referencia y estándares aplicables a diferentes ámbitos relacionados con las tecnologías de la información. Esta situación puede generar confusión en cuanto a la utilidad de los estándares, dificultando la toma de decisiones en cuanto a la adopción de ciertas prácticas para un uso efectivo de las tecnologías de la información. Es de vital importancia establecer un dominio de actividades al que nos queremos enfrentar, para después hacer una revisión de los posibles marcos de referencia que facilitan la gestión del dominio elegido.

Existen pocas referencias donde se hable de forma clara y resumida sobre los diferentes estándares, marcos de referencia y metodologías existentes en relación a las tecnologías de la información y al subgrupo de actividades que tratan. Se tratará de ofrecer una referencia sencilla en cuanto a los dominios y marcos de referencia que aplican en el caso de este proyecto, tomando especial importancia la gobernanza y la seguridad de la información, como elementos clave en cualquier organización.

Relacionado con el punto anterior, desde hace pocos años se han ido actualizando una serie de estándares en previsión de las necesidades actuales y futuras de las tecnologías de la información. Es el caso de COBIT, para la gobernanza, e ISO/IEC 27002, para la seguridad de la información, de los que no existen todavía muchos trabajos que se basen en sus últimas versiones: COBIT 5 e ISO/IEC 27002:2013; y la relación entre ambas.

Por otra parte, la evolución de los últimos años en cuanto a arquitecturas de sistemas ha permitido establecer dos modelos de implementación: tradicional y computación en la nube. El nuevo modelo de computación en la nube y sus elementos relacionados pueden generar incertidumbre a la hora de enfrentarnos a una decisión en cuanto al diseño de la arquitectura empresarial que esté en línea con los objetivos estratégicos de la organización. En este proyecto se tratará de ver las diferentes posibilidades técnicas a la hora de enfrentarse a un entorno de sistemas heterogéneos donde existe un sistema centralizado de gestión de identidades y control de accesos.

Por último, se encuentran muchos trabajos referentes a auditoría informática que tratan los puntos a evaluar desde un nivel alto, pero en este trabajo se tratará de encontrar mejores prácticas y un proceso de auditoría a nivel técnico para el escenario en cuestión.

1.2 Objetivos

El principal propósito de este proyecto es obtener una **guía de auditoría práctica** que ayude al lector en la búsqueda de puntos a evaluar cuando se enfrente a entornos tecnológicos heterogéneos frecuentes. Sin embargo, el abanico de posibilidades en cuanto a entornos mixtos es muy elevado, aún más en la actualidad con el uso de modelos de computación en la nube. Por este motivo, centraremos el objetivo de la guía de auditoría en alguno de los sistemas centralizados de gestión de identidades (*Active Directory*) al que pueden conectarse clientes basados en Windows y en Linux.

Las características principales que se buscan para la guía de auditoría son las siguientes:

- Obtener una guía combinando las buenas prácticas de dos de los estándares más importantes que existen para gestión de las tecnologías de la información (TI) y seguridad de la información. Estos modelos son COBIT e ISO/IEC 27002, y su acoplamiento permitirá alcanzar el máximo desempeño en el proceso de control y auditoría.
- Enfocada a entornos empresariales pequeños y medianos, así como escenarios donde el uso de entornos mixtos / heterogéneos es habitual, soportados cada vez más por arquitecturas de computación en la nube.
- Poniendo énfasis en aspectos relacionados con el control de acceso lógico y gestión de identidades, al tratarse del punto de entrada principal a cualquier sistema, plataforma y servicio.

Para conseguir estos objetivos, se llevará a cabo un análisis de los marcos de referencia COBIT e ISO 27002, así como una revisión tecnológica de los sistemas operativos y arquitecturas más importantes: computación en nube, sistemas operativos Windows y Linux (Suse u otras distribuciones Linux); dando especial importancia a los puntos relativos a seguridad y control de accesos.

1.3 Estructura del documento

El documento se divide en cinco secciones principales:

Sección I: presentación de la problemática que se trata resolver y objetivos del proyecto. El contenido se puede encontrar en el capítulo 1 de la memoria.

Sección II: introducción al estado de la cuestión. Se ofrecen los conceptos básicos de auditoría informática, se enumeran y describen los estándares y normativas actuales dentro de la temática tratada. También se describe la situación actual en cuanto a sistemas operativos se refiere. Esta sección está formada por los capítulos 2 y 3 del documento. En el capítulo 3 se ofrece un estudio-resumen de COBIT (versión 5) e ISO/IEC 27002:2013, además de un alineamiento de los dos marcos de trabajo.

Sección III: se realiza una revisión tecnológica de entornos mixtos frecuentes y se analizan los modelos y configuraciones de los sistemas analizados. El contenido está distribuido entre los capítulos 4 y 5 del documento.

En el capítulo 4 se trata la importancia de los estándares tecnológicos para la interoperabilidad, y se tratan algunos de los protocolos más importantes. En el capítulo 5 se tratan los entornos mixtos que son objetivo del proyecto, centrándose en el control de accesos y gestión de identidades.

Sección IV: Se plantea la guía de auditoría, y se ofrecen las conclusiones y futuras ampliaciones. Esta sección está formada por los capítulos 6, 7, 8 y 9. El capítulo 6 abarca el contenido de la guía de auditoría. El capítulo 7 contiene el presupuesto del proyecto. El capítulo 8 presenta las conclusiones del trabajo realizado. El capítulo 9 establece líneas futuras de investigación y/o ampliaciones que puedan servir como continuación de este proyecto.

Sección V: ofrece información complementaria distribuida entre los capítulos 10, 11 y 12. En el capítulo 10 se encuentra el glosario de términos. El capítulo 11 contiene todas las referencias utilizadas para el desarrollo de este proyecto. En el capítulo 12 se incluyen los anexos que sirven de referencia al lector

.

2 Estado del Arte

2.1 Marcos de referencia, estándares y normativas

Desde comienzos de este siglo existe una continua actividad en cuanto a la revisión de estándares relacionados con la gestión de las tecnologías de la información (TI), así como en la definición de algunas necesidades no cubiertas hasta ese momento.

Parece lógico pensar que esta actividad es consecuencia del grado de madurez que están alcanzando las tecnologías de la información, las comunicaciones y el uso de Internet en todas las sociedades a nivel global.

Debido al actual grado de penetración de las TI en la sociedad, y siendo parte fundamental en los planes presentes y futuros de toda organización, cada vez se hace más necesario establecer entornos formales y seguros que garanticen un desempeño más eficaz del uso de la información, mejorando su utilización y reduciendo los riesgos asociados a la misma.

Con el fin de facilitar las tareas involucradas en el ámbito de TI, existen una serie de marcos de referencia y buenas prácticas de referencia en el sector. Para facilitar la organización de estos estándares, marcos de referencia y buenas prácticas, podemos utilizar el concepto de *Dominio de actividad de TI*, que representa a nivel alto el tipo de sub-actividades, capacidades de gestión y/o administración que se llevan a cabo dentro de cada marco. Algunos de estos dominios de actividad de TI que podemos tratar, aún sin tener que ser exclusivos del ámbito tecnológico, son:

- Gobernanza
- Gestión de servicios
- Gestión de proyectos
- Gestión de riesgos
- Entrega de valor
- Seguridad de la información
- Arquitectura empresarial
- Calidad
- Evaluación de la madurez
- Control interno
- Gestión de la continuidad del negocio

En la tabla 2-1 se muestra un listado de los dominios más significativos y los estándares relacionados más importantes en la actualidad, algunos de los cuales se introducirán brevemente.

DOMINIOS DE TI	ESTÁNDARES
Gobernanza de TI	• ISO/IEC 38500:2008 • COBIT 5
Gestión de servicios de TI	• ITIL® 2011 Edition • ISO/IEC 20000:2011
Gestión de proyectos	• PRINCE2® 2009 Edition • PMBOK® 5th Edition (2013)
Gestión de riesgos	• COSO ERM (Enterprise Risk Management (2004) • RISK IT™ (2009) • Management of Risk (M_o_R) (2002 – 2010) • OCTAVE® (2001) • ISO 31000:2009
Entrega de valor	• ValIT™ (2008) • Management of Value (MoV™) (2010)
Seguridad de la información	• Serie ISO/IEC 27000 • NIST serie 800 • MEHARI • "Standard of Good Practice for Information Security" (2013) del ISF
Arquitectura empresarial	• TOGAF®- "The Open Group Architecture Framework" • Zachman Framework for Enterprise Architecture. • CEAF – "Commission Enterprise Architecture Framework". • FEA – "Federal Enterprise Architecture"
Calidad	• "The Deming Cycle", conocido como PDCA (Plan – Do – Check – Act) • Juran's Managerial Breakthrough • Kaizen • Total Quality Management (TQM), basado en PDCA • Six Sigma • Baldridge National Quality Program (BNQP) • Lean – Metodología de integración eficaz basada en datos • European Foundation for Quality Management (EFQM) • ISO 9000, basado en BS5750 → Actualmente ISO 9001:2008
Evaluación de la madurez	• CMM® • CMMI®

	• ISO/IEC 15504
Control interno	• COSO • Sarbanes-Oxley Act • Basilea III
Gestión de la continuidad del negocio	• ISO 22301:2012, basado en BS25999-2 (2007) • BS 25777

Tabla 2-1: Dominios y estándares TI[1]

Existen en la práctica más dominios de conocimiento en cuanto a gestión y administración dentro de las actividades de las empresas, sin embargo, se puede considerar que los expuestos en la tabla 2-1 cubren la tendencia actual en cuanto a estándares a tener en cuenta al hablar de TI.

Por otra parte, al tratar el tema de auditoría, podemos destacar tres marcos:

- **ISO/IEC 19011:2011**: es el estándar de referencia en cuanto a Directrices para la auditoría de Sistemas de Gestión.
- **ITAF (***A Professional Practices Framework for IS Audit/Assurance)*: es un modelo de referencia de buenas prácticas para auditoría y control de sistemas de información publicado por ISACA. La última edición es la tercera, de septiembre de 2014.
- **SSAE 16** (*Statement on Standards for Attestation Engagements*): es un nuevo estándar de 2011 que sustituye a SAS 70 (*Statement on Auditing Standards*). SAS 70 era un estándar desarrollado por el AICPA (*American Institute of Certified Public Accountants*). El objetivo de SSAE 16 es establecer un marco de trabajo y guía de ayuda para el reporte y control de entidades de servicios.

En cuanto al marco regulatorio y normativo español, estas son las referencias más significativas relacionadas con TI:

- **UNE-ISO/IEC 27001:2007**, que anula la UNE 71502:2004 y que será anulada por PNE-ISO/IEC 27001. Es la norma equivalente a ISO/IEC 27001:2013.
- **LODP**: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que debe cumplir cualquier entidad que trate con datos de carácter personal. A esta ley le sigue otra normativa publicada como Real

[1] Fuente [19]

Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

- **LSSICE**: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Esta ley tiene como objetivo regular los servicios de la sociedad de la información y la contratación de los mismos por vía electrónica: obligaciones de los prestadores de servicios, intermediarios, requisitos de las telecomunicaciones y régimen sancionador.
- **Firma Electrónica**: Ley 59/2003, de 19 de diciembre, de firma electrónica. Esta ley trata de establecer el marco jurídico para poder dar validez y reconocimiento a los documentos electrónicos, firmados digitalmente utilizando una serie de tecnologías.
- **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas): como su nombre indica es una metodología española de análisis y gestión de riesgos de los sistemas de información. Es una metodología pública al alcance de cualquier entidad que quiera utilizar un método de trabajo que garantice la seguridad en los sistemas de información.

El dominio de actividad de TI común y transversal que debería englobar a todos los demás es el de Gobernanza de TI. Podemos considerar que todo trabajo presente o futuro que trate cualquiera de los estándares vistos en este punto desde una perspectiva de TI, debe encuadrarse dentro del paraguas de la Gobernanza de TI.

Al estar enfocado en la seguridad de los sistemas y seguridad, el presente proyecto profundiza en el capítulo tres en COBIT 5 como marco de referencia a partir del cual se seguirá un proceso en cascada pare entrar a analizar también ISO/IEC 27002:2013. No obstante, ofrecemos una breve introducción a algunos estándares destacables.

2.1.1 ISO/IEC 38500:2008

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) define el bueno gobierno corporativo como "El sistema por el cual las entidades son dirigidas y controladas. La estructura del buen gobierno corporativo comprende la distribución y responsabilidades entre todos los diferentes participantes de la entidad, tales como los accionistas, el consejo de administración, las gerencias y otros agentes económicos que mantengan algún interés en la entidad. El bueno gobierno corporativo también provee la

estructura a través de la cual se establecen los objetivos de la empresa y los medios para alcanzar estos objetivos, así como la forma de hacer un seguimiento a su desempeño" [1].

En el caso de las TIC, surge la norma ISO/IEC 38500 [2] en el año 2008, que trata de fijar los estándares para un buen gobierno de los procesos y decisiones empresariales relacionados con las tecnologías de la información. Está basada en la norma australiana AS8015:2005 y su principal objetivo es proporcionar un marco para evaluar, dirigir y supervisar el uso de TI, al tratarse de una herramienta fundamental para los negocios. El origen de este tema lo podemos encontrar en el *Informe Cadbury* (1992).

2.1.2 COBIT 5

Control Objectives for Information and Related Technology (COBIT) [3] es un marco de referencia único e integrado, formado por un conjunto de marcos y guías, que la *Information Systems Audit and Control Association* (ISACA) ha construido y evolucionado desde 1996 para cubrir los aspectos relativos a la gobernanza de TI. El objetivo de COBIT®5 es ayudar a las empresas a alcanzar sus objetivos de gobierno.

La principal característica de COBIT es que está orientado al negocio, y está diseñado para ser utilizado tanto por proveedores de servicios de TI y usuarios, como por personal de niveles administrativos y ejecutivos centrados en la toma de decisiones. Trata de dar respuesta a las necesidades del negocio manteniendo cierta independencia con respecto a las plataformas tecnológicas.

Es uno de los marcos de trabajo que se utiliza como referencia en el desarrollo del proyecto por lo que se trata más en detalle en el capítulo 3.

2.1.3 COSO

El informe COSO (*Committee of Sponsoring Organizations of Treadway*) [4] es un informe publicado por primera vez en 1992 por dicho comité (en Estados Unidos) que establece una serie de directivas para el control interno de cualquier organización, y junto con COBIT es uno de los modelos más utilizados para tal fin, convirtiéndose en un estándar en el sector de la auditoría.

A diferencia de COBIT, es un modelo pensado para toda la organización. Mientras que el primero se centra en lo relacionado con TI, COSO está orientado a cualquier ámbito de aplicación de la empresa, principalmente ámbito financiero y

administrativo. También cabe destacar que en él no se hace referencia a la seguridad de la información, algo sí tenido en cuenta en COBIT.

2.1.4 ITIL e ISO/IEC 20000:2011

Information Technology Infrastructure Library (ITIL) [5] es un marco de trabajo repartido en varios tomos que establece una guía de buenas prácticas según la experiencia de expertos a nivel mundial para promover la calidad en la entrega de servicios dentro del sector de TI.

Tuvo su origen en la Agencia Central de Telecomunicaciones e Informática británica (CCTA, *Central Computer and Telecomunications Agency*) como respuesta a la baja calidad en la gestión de TI a finales de la década de los 80. Se publica a través de la Oficina para el Comercio Gubernamental Británica (OGC, *Office of Government Commerce*), que absorbió a la CCTA.

La última versión es la 3, publicada en mayo de 2007, basada en 5 tomos principales: estrategias de servicio (SS), diseño del servicio (SD), transición del servicio (ST), operaciones del servicio (SO), y mejora continua del servicio (CSI).

En los últimos años ITIL se ha convertido en uno de los marcos de procesos de gestión más aceptados y utilizados, formando junto con ISO 27001/27002 y COBIT los estándares que mejor se complementan para alcanzar una gestión total de TI a todos los niveles.

La serie ISO/IEC 20000 [2], publicada inicialmente en diciembre de 2005, es el estándar reconocido internacionalmente para la gestión de servicios de TI. Conceptualmente es el marco sobre el que se desarrolla ITIL, y proviene de la adopción de la serie BS 15000. Es una norma certificable a nivel mundial.

2.1.5 Serie ISO/IEC 27000

La serie ISO/IEC 27000 [2] es un conjunto de estándares desarrollados o en fase de desarrollo, publicados por la Organización Internacional de Estandarización (ISO, *International Organization for Standardization*) y la Comisión Electrotécnica Internacional (IEC, *International Electrotechnical Commision*). Esta serie es desarrollada por el Comité Técnico ISO/IEC JTC 1/SC 27.

La serie 27000 ofrece un marco de gestión de la seguridad de la información disponible para cualquier tipo de organización. Tiene su origen en la publicación de la norma BS 7799 de BSI en 1995.

Dentro de la serie, y según la numeración, cada estándar se centra en temáticas específicas. Así por ejemplo, los estándares que van del 27011 al 27019 se dedican a la seguridad de sectores concretos. Algunos de los estándares más importantes de la serie son:

- ISO/IEC 27000: contiene términos y definiciones a emplear en toda la serie 27000.
- ISO/IEC 27001: es la norma principal de la serie. Contiene requisitos del sistema de gestión de seguridad de la información. Es la norma con arreglo a la cual se certifican por auditores externos los Sistemas de Gestión de Seguridad de la Información, SGSI, de las organizaciones.
- ISO/IEC 27002: es una guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a seguridad de la información. Es la norma objeto de este capítulo. ISO/IEC 27001, que es la noma certificable, utiliza como base el conjunto de controles que se exponen en la 27002.
- ISO/IEC 27003: es una guía de implementación de un SGSI e información acerca del uso del modelo PDCA (*Plan-Do-Check-Act*; Planificar-Ejecutar-Verificar-Actuar) y de los requerimientos de sus diferentes fases.
- ISO/IEC 27004: especifica métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Las métricas se utilizan principalmente para la medición de los componentes de la fase "Ejecutar" del ciclo PDCA.
- ISO/IEC 27005: establece directrices para la gestión del riesgo en la seguridad de la información. Apoya conceptos generales especificados en ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ISO/IEC 27006: especifica requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- ISO/IEC 27007: consiste en una guía de auditoría de un SGSI. Está fuertemente basada en la ISO 19011.

- ISO/IEC 27011: es una guía de gestión de seguridad de la información específica para el sector de las telecomunicaciones.
- ISO/IEC 27031: es una guía de continuidad del negocio en cuanto a tecnologías de la información y comunicaciones se refiere.
- ISO/IEC 27032: es una guía referente a la seguridad en Internet.
- ISO/IEC 27033: consiste en varias partes referentes a la gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes, acceso remoto, comunicaciones en redes con VPNs y otros temas relativos a redes. Sirve como revisión de la ISO 18028.
- ISO/IEC 27034: consiste en una guía de seguridad de aplicaciones.
- ISO/IEC 27799: referente a la gestión de seguridad de la información en el sector sanitario aplicando ISO/IEC 27002.

Debido al auge del modelo de computación en nube, cobran especial atención las recientes:

- ISO/IEC 27018:2014: referente a protección de datos en sistemas en la nube
- ISO/IEC 27017: relativa a la gestión de la seguridad de la información en sistemas en la nube.

Fuente: [6], [2]

2.1.6 NIST serie 800

El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, *National Institute of Standards and Technology*) [7] publica desde 1990 una serie de documentos de interés general sobre Seguridad de la Información. Esta serie, llamada Serie 800 es el resultado del esfuerzo de industrias, gobiernos y organizaciones académicas para todos los interesados en la seguridad.

Las publicaciones cubren procedimientos y criterios para el aseguramiento, gestión de vulnerabilidades, implementación de la seguridad, entre otros.

2.1.7 MEHARI

El Método para el Análisis de Riesgos Armonizado (MEHARI, *Method for Harmonized Analysis of Risk*) [8] es una metodología de análisis y gestión de la

seguridad de la información y los riesgos asociados a ella, desarrollada desde 1996 por el Club Francés de la Seguridad de la Información (CLUSIF, *Club de la Sécurité de l'Information Français*). MEHARI cumple con el estándar de gestión de riesgos ISO/IEC 27005 y se puede utilizar como método de implementación de un SGSI según lo establecido en ISO/IEC 27001. Para lograr los objetivos, MEHARI plantea cuatro módulos:

- Analizar los principales problemas
- Analizar las vulnerabilidades
- Disminuir y controlar los riesgos
- Supervisar la seguridad de la información

2.1.8 Estándar de Buenas Prácticas para la Seguridad de la Información

El Foro para la Seguridad de la Información (ISF, *Information Security Forum*) publica anualmente el Estándar de Buenas Prácticas para la Seguridad de la Información [9]. Cubre de una forma práctica todo el espectro completo de acuerdos de seguridad de la información que se necesitan para preservar a las empresas de los riesgos asociados. La versión de 2014 incluye nuevas guías relativas a:

- "Ciber-resiliencia" (capacidad de las empresas para resistir amenazas inesperadas de la red)
- Seguridad en la cadena de suministro
- Seguridad en dispositivos móviles del empleado (BYOD)
- Privacidad de datos en la nube
- Infraestructuras críticas

2.1.9 SANS Institute

SANS (*SysAdmin Audit, Networking and Security Institute*) [10] es una institución fundada en 1989 cuyo objetivo es reunir información sobre seguridad de la información y ofrecer formación y certificación a los profesionales de la seguridad informática. Entre algunas de sus publicaciones podemos encontrar la lista de 20 controles críticos en cuanto a seguridad de la información [11]:

CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN
Inventario de dispositivos autorizados y no autorizados.
Inventario de software autorizado y no autorizado.
Configuraciones seguras para hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores.
Evaluación continua de la vulnerabilidad
Defensa ante malware
Seguridad en las aplicaciones software
Control de acceso inalámbrico
Capacidad de recuperación de datos
Habilidades de seguridad y formación apropiada
Configuración segura de dispositivos de red: firewalls, routers y switches.
Limitación y control de puertos de red, protocolos y servicios
Uso controlado de privilegios administrativos
Defensa de los límites de la red
Mantenimiento, monitorización y análisis de registros de auditoría
Control de acceso basado en la "necesidad de saber"
Monitorización y control de cuentas
Protección de datos
Gestión de respuesta a incidentes
Ingeniería de red segura
Test de penetración y ejercicios de equipo rojo

Tabla 2-2. Controles de Sans Institue para la seguridad de la información

2.2 Sistemas operativos y modelos de computación

2.2.1 Breve historia de Windows

En 1985 Microsoft publicó la primera versión de Windows (Windows 1.0), una interfaz gráfica de usuario (GUI) para el sistema operativo MS-DOS. Esta primera versión no era muy potente (se basaba en tecnología de 16 bits), ni tampoco se hizo muy popular, ya que al publicarse después del sistema MacOS, estaba muy limitada legalmente y por lo tanto sus funciones no estaban desarrolladas al máximo.

A lo largo de la década de los ochenta, Microsoft continúo publicando nuevas versiones de su interfaz, con mejoras y nuevas características, aunque nunca llegaron a tener el éxito que pretendían. De hecho, la primera versión popular de Windows fue la 3.0, publicada en 1990, y que se beneficiaba de los procesadores 80386 de Intel, que por esa época permitían mejoras en las capacidades multitarea de las aplicaciones Windows.

Además, durante la segunda mitad de la década de los 80, Microsoft e IBM colaboraron en el desarrollo de un nuevo sistema, el OS/2, que estaba previsto sustituyera al viejo DOS, pero las diferencias entre ambas compañías hicieron que cada una siguiera caminos distintos: IBM desarrollaría OS/2 y Microsoft se encargaría de crear Windows NT. Así llegamos al año 1992, cuando IBM publicó el OS/2 2.0. Microsoft, como respuesta a este lanzamiento, sacó al mercado Windows 3.1, que luego ampliaría a Windows 3.11, y que traía consigo pequeñas mejoras respecto a Windows 3.0, pero que seguía utilizando tecnología de 16 bits y no podía competir con OS/2.

Después de esto, mientras Microsoft sacaba Windows NT (basado en 32 bits) sin mayor éxito y con el dominio del mercado por parte de OS/2, Microsoft empezó a desarrollar Windows 95, que tras su aparición en agosto de 1995 supuso un giro en el mercado de las interfaces gráficas, ya que esta versión sí empezaba a competir con OS/2.

De esta forma, la compañía de Redmond estableció dos familias en cuanto a sistemas operativos: una basada en Windows 95 y otra en Windows NT (que adquiere la interfaz de Windows 95 para su mejor aceptación).

A lo largo de los años, el desarrollo de Microsoft llevó a crear sistemas mejorados de ambas familias. Así, en 1998 nació Windows 98, que luego se ampliaría a Windows 98 SE (Segunda Edición). En el año 2000, Microsoft publicó Windows Millennium (Me), que no dejaba de ser una ampliación de Windows 98, y por otra parte, también

veía la luz Windows 2000, un sistema basado en Windows NT, pero que mejoraba sustancialmente sus características al permitir los dispositivos "*plug and play*" y ofrecer una cantidad aceptable de recursos para los administradores de red.

Tras esto, la unificación de los núcleos de ambas familias vino de la mano de Windows XP, liberado en 2001 y que mejoraba la interfaz de los sistemas Windows 95, 98 y Me, pero cuyo núcleo estaba basado en los sistemas NT.

Debido a la evolución de las tecnologías de la información y a los diferentes ámbitos de aplicación, Windows 2000 se desarrolló en cuatro versiones: Profesional, Server, Advanced Server y Datacenter Server. Pero las exigencias del mercado y de las empresas requerían más prestaciones, de modo que Microsoft desarrolló y publicó Windows Server 2003 en abril de 2003, basado en el núcleo de Windows XP y disponible en cuatro versiones, según las necesidades: Standard Edition, Enterprise Edition, Datacenter Edition y Web Edition. A partir de Windows Server 2003 empiezan a utilizarse versiones del sistema para arquitecturas de 64 bits.

En diciembre de 2005 apareció Windows Server 2003 R2, que ofrecía una serie de mejoras, orientadas principalmente a la conectividad y gestión de identidades, y que se convirtió en un sistema operativo robusto y muy utilizado en todos los ámbitos empresariales a nivel de servidor, así como Windows XP sería el sistema más utilizado a nivel de usuario y oficina.

En 2007 Microsoft publicó Windows Vista, orientado tanto a la informática personal como profesional. A su vez, en febrero de 2008 Microsoft publicó el nuevo sistema operativo orientado a servidores, Windows Server 2008, sustituto de Windows Server 2003. Tanto la línea de sistemas Windows Vista como Windows Server 2008 están basados en núcleos 6.x, y se pueden implantar en arquitecturas de 32 y 64 bits.

En julio de 2009, apareció Windows Server 2008 R2, segunda implementación del sistema que sólo está disponible para arquitecturas de 64 bits. Por otra parte, desde la primera versión de Windows Server 2008 existe un modo de instalación del sistema llamada "*Server Core*" que reduce las funcionalidades instaladas, no incluye interfaz gráfica por lo que se realizan las tareas a través de línea de comandos, y está orientado a servidores con funcionalidad básica como servidores DNS, controladores de dominio, servidores de ficheros y otros usos elementales.

En octubre de 2009 Microsoft publicó Windows 7, disponible para arquitecturas de 32 y 64 bits, y con seis ediciones: Starter, Home Basic, Home Premium, Professional, Enterprise y Ultimate.

Hasta la fecha, las últimas versiones de Windows para servidores son Windows Server 2012, disponible desde septiembre de 2012 y Windows Server 2012 r2 en octubre de 2013. Las ediciones disponibles de Windows Server 2012 son: Foundation, Essentials, Standard y Datacenter. Siguiendo con la filosofía de Windows Server 2008, este servidor sólo está disponible para arquitecturas x86 de 64 bits.

En cuanto a versiones de Windows para escritorio, la última versión es Windows 8.1, publicada también en 2013 y lanzada como mejora de Windows 8, de 2012. Esta versión tiene soporte para las arquitecturas IA-32, x86-64 y ARM.

2.2.2 Breve historia de Linux

La historia de GNU/Linux comenzó en septiembre de 1983 cuando Richard Stallman inició el proyecto GNU (acrónimo de GNU is Not UNIX) para el desarrollo de un sistema operativo libre, compatible con UNIX y los estándares POSIX. El hecho de ser compatible con UNIX hizo que se pensara en una arquitectura compuesta de piezas de software más pequeñas.

En 1985, Richard Stallman creó la Fundación para el Software Libre (FSF, *Free Software Foundation*) que dotaba de estructura organizativa y financiera al proyecto GNU. De esta forma, a través de la FSF, su plantilla de programadores y principalmente, de voluntarios y organizaciones importantes interesadas en el proyecto, se llevó a cabo el desarrollo de varios proyectos de software libre importantes como Emacs (editor de textos), GCC (compilador para C) y otros componentes importantes de un sistema típico UNIX.

Para proteger el software libre y en general todos los proyectos involucrados en GNU, en febrero de 1989 se publicó la primera versión de la licencia GNU GPL (GNU *General Public License*). El propósito principal de GNU GPL es proteger de intentos de apropiación que restrinjan las libertades del software libre, de forma que todo el software bajo licencia GNU GPL, está obligado a mantener dicha licencia en cualquier ámbito de distribución, modificación y uso.

No obstante, había un inconveniente para el progreso de GNU: el núcleo; componente principal del sistema operativo que, habiendo pasado entre diferentes

proyectos, como TRIX (en el *Massachusetts Institute of Technology)* y Hurd (en la Universidad Carnegie Mellon) se había estancado debido a razones técnicas y conflictos entre los programadores.

En esta situación se llegó a agosto de 1991, cuando Linus Torvalds publicó la primera versión de un sistema operativo al que llamó Linux y que desarrolló utilizando el sistema operativo Minix y el compilador de C de GNU: GCC. Esta primera versión funcional 0.02 la publicó en la red Usenet de su universidad bajo una licencia propia basada en una licencia de código fuente compartido, y restringida contra la acción comercial.

Fue en diciembre de 1992 cuando Linus Torvalds decidió unir Linux al proyecto GNU publicando la versión 0.99 bajo licencia GNU GPL. De esta forma, a lo largo de los siguientes años se unieron cada vez más programadores que aportaron código y funcionalidad al núcleo de Linux y lo adaptaron al ambiente GNU. En 1993 se liberó la primera distribución y más antigua, Slackware, y apareció por primera vez el proyecto Debian.

En 1994 apareció la primera versión estable de GNU/Linux, versión 1.0 y empresas como Red Hat y Suse publicaron sus primeras versiones de distribuciones GNU/Linux. Es importante también en estas fechas la aparición del proyecto XFree86.

Desde ese momento, los hechos más importantes relacionados con GNU/Linux fueron el desarrollo y evolución del núcleo Linux, cuya última versión estable es la 3.17.1, así como también la aparición de multitud de distribuciones del sistema operativo. En cuanto a las versiones estables del núcleo, los años más importantes fueron 1992, cuando se publicó la versión 1.0. En 1996 y 2001 se publicaron respectivamente las versiones 2.0 y 2.4. Ya en 2003, se publicó la serie del núcleo 2.6, y hasta 2011 no apareció la versión 3.0.

Debido a que en este documento se tratan aspectos de SUSE Linux, se ofrece a continuación una breve historia de dicha distribución.

La historia de SUSE (acrónimo original de la empresa alemana *Software Und Systementwicklung*) comenzó en 1994 con la publicación en marzo de dicho año de la versión 1.0, la cual estaba basada en Slackware. A lo largo de los años, y hasta octubre de 2003 aparecieron diversas versiones de la distribución, hasta llegar a la 9.0.

En noviembre de 2003 la empresa Novell anunció la compra de la compañía alemana, que se llevó a la práctica en enero de 2004. Después de la adquisición por parte de Novell, en agosto de 2005 la compañía comunicó que se iniciaba el proyecto openSUSE, dejando a la comunidad el desarrollo y contribución libre a la distribución. En septiembre de 2005 vio la luz la versión 10.0, y a partir de esta fecha es habitual que se publiquen al menos entre una y dos versiones al año de la distribución. La última versión de OpenSuse es la 13.1, publicada en noviembre de 2013.

De entre la gama de productos que ofrece Novell, aquellos más relacionados con SUSE Linux son:

- Orientados al centro de datos y servidores: SUSE Linux Enterprise Server, SUSE Linux Enterprise Server for System Z, SUSE Linux Enterprise para aplicaciones SAP, SUSE Linux Enterprise Server para computación de alto rendimiento, a las que se pueden incluir extensiones para alta disponibilidad y tiempo real.
- Además de la línea libre e independiente de la comunidad OpenSUSE, Novell ofrece para el usuario final SUSE Linux Enterprise Desktop, entre otras opciones orientadas a virtualización y otros servicios más específicos.

En cuanto a la opción para servidores, SUSE Linux Enterprise Server incluye toda su funcionalidad independientemente de la plataforma hardware de implantación. Está disponible para las siguientes arquitecturas con los siguientes límites de capacidad, certificados en situaciones reales:

- **X86**: 32 sockets y 16 GB de memoria RAM.
- **X86 de 64 bits**: 64 sockets y 512 GB de memoria RAM.
- **Itanium**: 64 sockets y 4 TB de memoria RAM.
- **IBM Power**: 64 sockets y 512 GB de memoria RAM.
- **IBM System Z**: 64 sockets y 256 GB de memoria RAM.

Para entornos de escritorio, Novell ofrece SUSE Linux Enterprise Desktop, que es una opción de SUSE Linux con soporte de Novell, basada en OpenSUSE, pero orientada a entornos empresariales donde hay necesidad de incluir un soporte de sistema operativo.

2.2.3 Situación actual

Al hablar de sistemas operativos tenemos que diferenciar el ámbito de uso. Aunque hasta hace un par de décadas el uso de sistemas operativos se reducía prácticamente a servidores y puestos de trabajo (escritorio y portátiles), en estos momentos, con el uso de Internet y su grado de penetración tan grande, hemos entrado en la era del Internet de las cosas (IoT, *Internet of Things*), y nos encontramos en situaciones donde existe una interconexión entre dispositivos y personas de cualquier tipo y en cualquier ámbito. En gran parte, esto ha sido posible gracias a la evolución en la última década de los teléfonos móviles hacia teléfonos inteligentes (*smartphones*) y a la implementación de sistemas operativos ligeros y embebidos como iOS y Android.

No obstante, el Internet de las cosas es un mundo recién nacido y el uso de estos sistemas es todavía relativamente pequeño en comparación con el uso de los sistemas operativos para fines tradicionales (servidores y puestos de trabajo). Existen en la actualidad tres sistemas operativos fundamentales aplicados a la informática tradicional:

- Windows (en todas sus versiones)
- Linux (englobando a todas sus diferentes distribuciones)
- Mac OS

Por otra parte, podemos diferenciar claramente el entorno de utilización de estos sistemas operativos en dos: entorno de usuario y entorno empresarial.

Si hablamos de entornos de usuario o domésticos, los sistemas operativos más utilizados son Windows y Mac OS. Sin embargo, en entornos empresariales, son Windows y Linux los que más porcentaje de utilización tienen. Podemos ver que, excepto en el mundo del diseño y artes gráficas, Mac OS no es todavía a día de hoy un sistema operativo muy extendido en el mundo empresarial y corporativo, a pesar de que cada vez se utiliza más.

Tomamos como referencia válida los últimos datos de septiembre de 2014 de W3Schools, que muestran los siguientes resultados en cuanto al uso de sistemas operativos (ver tabla 2-3):

- Un 80% de sistemas Windows (en alguna de sus versiones)
- Un 9,6% de sistemas con Mac
- Un 5,5% de sistemas con Linux

- Un 4,3% de accesos a través de sistemas operativos móviles

	Win8	**Win7**	**Vista**	**NT***	**WinXP**	**Linux**	**Mac**	**Móvil**
Sep-2014	18,1%	55,6%	1%	0,2%	5,9%	5,5%	9,6%	4,3%
Sep-2013	10,2%	56,8%	1,6%	0,4%	13,5%	4,8%	9,3%	3,3%

Tabla 2-3: Uso de sistemas operativos en los dos últimos septiembres (2014,2013)

Por otro lado, en la serie histórica de 10 años, podemos ver la evolución en cuanto al uso de los sistemas operativos. La conclusión a la que podemos llegar es que, aunque existen fluctuaciones entre las versiones de Windows, tomando como referencia la época de publicación de Windows XP, los sistemas de Microsoft han dominado el mercado, mientras que el uso de Linux se ha mantenido prácticamente constante con algún crecimiento, así como Mac OS ha incrementado su cuota de mercado pero con una subida muy moderada (ver figura 2-1).

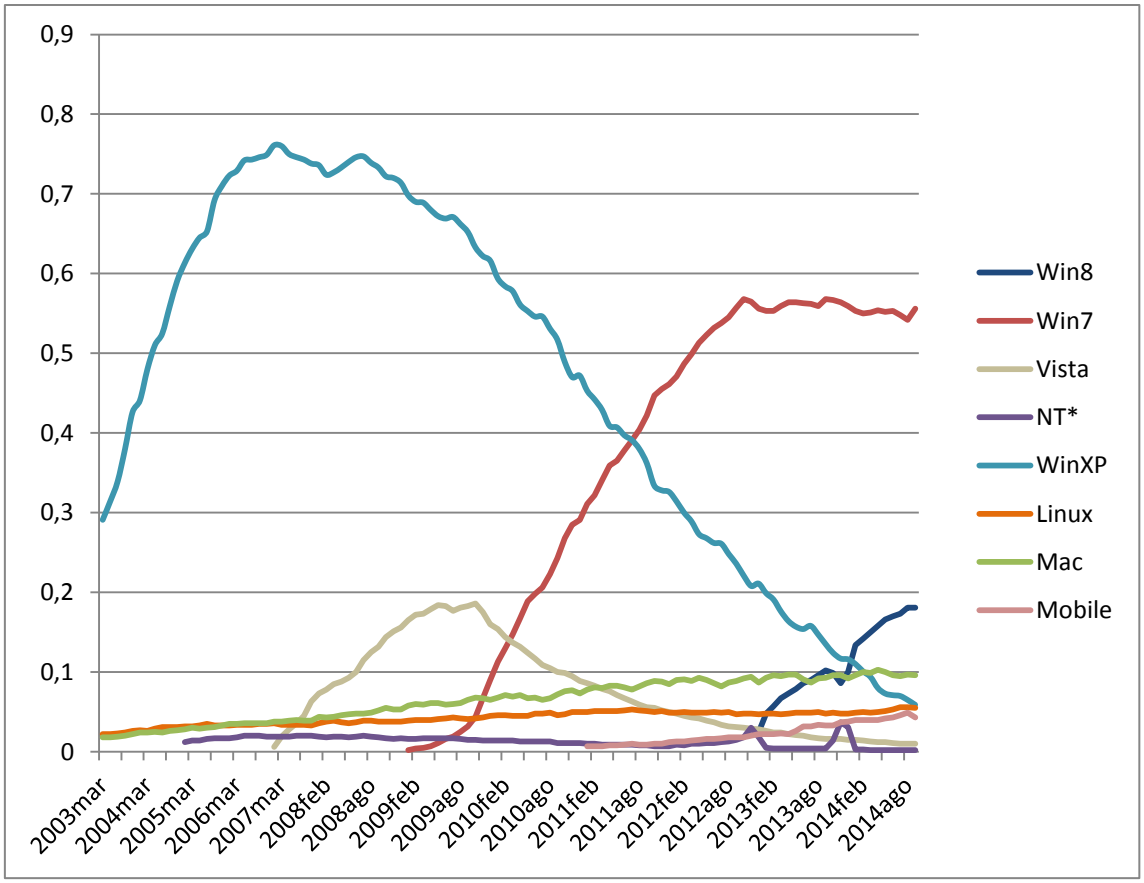


Figura 2-1: Estadísticas de uso de Sistemas Operativos (navegación web)[2]

En cuanto a la distribución de la cuota de mercado de los sistemas operativos en servidores, es difícil encontrar estadísticas de uso de sistemas internos ya que no es habitual que las empresas ofrezcan dicha información. Sin embargo, si tomamos como referencia la implementación de servidores web, podemos tener una idea de la distribución según se muestra en la figura 2-2. A diferencia de los equipos de trabajo, donde Windows es claro dominante, en el caso de servidores web el sistema que domina es Linux, que incluyendo todas las distribuciones ocupa un 95,03% según datos de diciembre de 2012 obtenidos de www.solvedns.com.

[2] Consolidación de datos obtenidos de http://www.w3schools.com/browsers/browsers_os.asp. Datos de septiembre de 2014

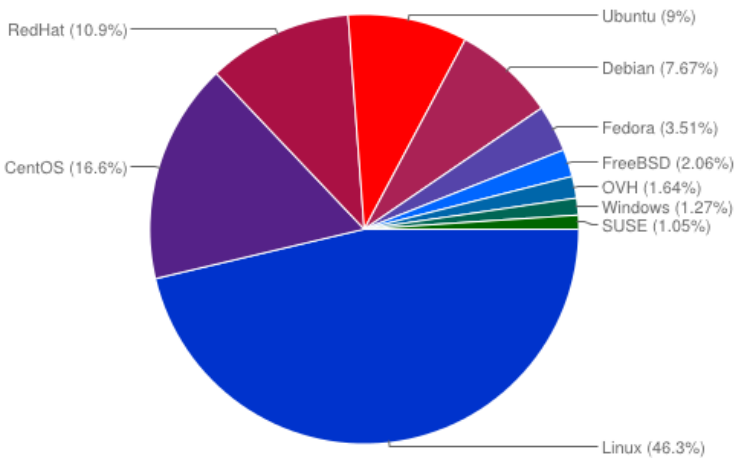


Figura 2-2: Distribución de Sistemas Operativos (servidores web)[3]

Por último, si entramos a ver el uso de distribuciones de Linux más utilizadas, según datos de www.distrowatch.com, OpenSuse se encuentra entre las cinco o seis distribuciones más utilizadas (datos de octubre de 2014), por debajo de Linux Mint, Ubuntu, Debian y Mageia. Además, Suse es una de las distribuciones más recomendadas para entornos empresariales (junto con Red Hat y Debian).

No es propósito de este proyecto realizar una valoración positiva o negativa sobre cualquiera de los dos sistemas en cuestión, sino hacer reflexionar sobre la implantación de entornos mixtos utilizando Windows y Linux, aprovechando las ventajas de cada uno, y de esta forma conseguir unos procesos de información lo más eficaces y robustos posibles, logrando implementaciones que estén acorde a las políticas planteadas para lograr los objetivos de la empresa y manteniendo los niveles de seguridad exigidos.

En cuanto a los entornos mixtos, actualmente son conocidas algunas políticas empresariales para logar la convivencia entre ambos sistemas/mundos, como es la establecida en 2006 entre Microsoft y Novell para fomentar la interoperabilidad entre Windows y Suse Linux [12]. Esto hace pensar que la interoperabilidad entre ambos sistemas es inevitable, viendo como muchas empresas solicitan y tienen entornos de múltiples plataformas, una práctica ya habitual en los centros de proceso de datos (CPDs).

[3] Fuente: www.solvedns.com. Datos de diciembre 2012

2.2.4 Computación en la nube

El Instituto Nacional de Normas y Tecnología (NIST, *National Institute of Standards and Technology*) define la computación en la nube como:

"Modelo que permite obtener, desde cualquier lugar y bajo demanda, un cómodo acceso a través de una red a un conjunto (*pool*) compartido de recursos informáticos configurables, el cual se puede conformar y suministrar rápidamente con un esfuerzo de gestión mínimo o con una interacción mínima con el proveedor de los servicios" [13].

La computación en la nube es un concepto esencial en estos momentos, concentrando la atención en muchos debates y decisiones que se producen en el ámbito de las tecnologías de la información. Surgió hace pocos años como un nuevo modelo de suministro de servicios, impulsada por los avances en virtualización de sistemas.

El atractivo principal de la computación en la nube es que permite a las empresas modificar la distribución de los costes relacionados con la tecnología, traspasando gastos de capital (inversiones en infraestructura tecnológica) hacia gastos operacionales, con la ventaja de que en principio el coste de entrada es más bajo y flexible. No obstante, más allá de los aspectos económicos y técnicos de la adopción de la computación en la nube, el desafío más importante es entender como aporta valor estratégico a las organizaciones, y como equilibrar el valor aportado con los riesgos operacionales y técnicos asociados al modelo.

Los beneficios más destacados de la computación en la nube son:

- Agilidad
- Contención de costes
- Arquitectura común multiempresa
- Confiabilidad
- Escalabilidad

Pero la adopción de la computación en la nube también conlleva una serie de riesgos. Si bien es cierto que normalmente estos riesgos están normalmente asociados a las características técnicas del despliegue de este modelo a través de la virtualización, también es importante tener en cuenta la resistencia al cambio que puede generar y la dificultad en la adaptación a la nueva forma de gobernanza y gestión.

Existen diferentes modelos de implantación de computación en la nube:

- Según el tipo de nube:
    - Infraestructura (IaaS, *Infrastructure as a Service*): se ofrece hardware y almacenamiento para el despliegue de infraestructura. Algunos ejemplos son: Amazon Web Services (AWS), Microsoft Azure, Rackspace Cloud.
    - Plataforma (PaaS, *Platform as a Service*): se ofrecen conjuntos de hardware y software preparados para el despliegue y desarrollo de soluciones. Algunos ejemplos son Google App Engine, Microsoft Azure.
    - Servicio (SaaS, *Software as a Service*): se ofrecen servicios llave en mano a través de la web, donde el cliente sólo se centra en el uso y administración básica. Algunos ejemplos son Google Apps, Office 365.

Estos modelos están evolucionando y ya se ofrecen otro tipo de servicios basados en los anteriores como Seguridad (SecaaS, *Security as a Service*)

- Según el tipo de prestación:
    - Nube pública: los servicios se ofrecen directamente al usuario como modelos de pago por consumo y/o *freemium*[4]. La infraestructura en este caso es compartida (*multitenant*) y por tanto los costes son los más bajos que se puedan encontrar.
    - Nube privada: la infraestructura es exclusiva de un cliente, ya sea gestionada de forma interna o externa. Normalmente implican acuerdos de nivel de servicio (SLAs) más exigentes y el nivel de inversión es superior a la nube pública.
    - Nube híbrida: consiste en la combinación de servicios de nube pública y privada. La idea es que la empresa utilice la nube privada como recurso principal, enfrentándose a picos de demanda mediante el uso de la nube pública.

Por último, destacamos el concepto de virtualización ya que es la tecnología que sustenta los modelos de computación en la nube. Existen cuatro tipos principales de virtualización [14]:

[4] Modelo de negocio donde se ofrecen servicios básicos gratuitos, mientras se cobra por otros más avanzados o especiales

- Virtualización de servidor: un sistema operativo huésped se virtualiza completamente como una imagen que se ejecuta en un hipervisor, compartiendo recursos de computación con otros sistemas operativos virtualizados en el mismo anfitrión.
- Virtualización de aplicación: una aplicación se encapsula y opera de forma aislada por encima del sistema operativo y el hardware, a lo que a veces se denomina "sandboxing".
- Virtualización de escritorio: un usuario puede operar en varios entornos de escritorio encima del sistema operativo anfitrión utilizando software de virtualización. Se diferencia de la virtualización de servidor en la capa subyacente (virtualización de servidor → hipervisor; virtualización de escritorio → sistema operativo).
- Virtualización de almacenamiento: la abstracción de varios dispositivos de almacenamiento físicos independientes hace que parezcan un único objeto de almacenamiento.

Por último, es importante tener en cuenta algunos riesgos asociados al uso de virtualización:

- En proyectos de virtualización normalmente no se presta atención a la seguridad.
- Si se compromete la capa de virtualización, todos los sistemas que la utilizan y sus cargas de trabajo también se ven comprometidos.
- La posible falta de visibilidad en las capas de red de los sistemas virtualizados puede dificultar el trabajo de los mecanismos y medidas de la política de seguridad.
- Las cargas de trabajo de diferentes niveles de confianza se consolidan en un mismo servidor físico, obviando la separación necesaria.
- Falta de controles adecuados en el hipervisor y las herramientas administrativas.
- Pérdida potencial en la separación de funciones para los controles de red y seguridad.

La computación en la nube cobra especial importancia a la hora de hablar de entornos mixtos, ya que permite el cambio y adaptación de manera flexible según las necesidades de la empresa en cada momento.

Los actores más destacados en el mundo de la virtualización son: VMWare, Citrix, Microsoft y Xen,

Fuentes: [13]

2.3 Seguridad y auditoría en informática

2.3.1 Seguridad de la información

El software libre de errores no existe y es imposible de lograr. Según algunos autores, esta afirmación se puede demostrar desde un punto de vista matemático teórico utilizando los teoremas de incompletitud de Gödel (1931). Por lo tanto, si nos enfrentamos a un escenario donde el software siempre tiene errores, es de vital importancia realizar esfuerzos para proteger los activos relacionados.

Según datos de Symantec [15], el 2013 fue el año con la serie de ciberataques más perjudiciales de la historia. El número de fallos de seguridad se incrementó en un 62% respecto a 2012. Según el Informe de Seguridad de Internet de 2014 de la misma compañía [16], el número de fallos de seguridad con exposición de información personal con más de 10 millones de afectados fue de 8 en 2013 (respecto a 1 en 2012), siendo los datos más revelados: nombres, fechas de nacimiento y números de identificación gubernamentales. El número total de identidades expuestas fue de 552 millones (un 493% más respecto al año anterior).

En este y otros informes se puede ver como la seguridad debe ser tratada como un factor clave en cualquier organización, debido al fuerte impacto que puede provocar su mala gestión o falta de concienciación. Además, una buena gestión de la seguridad cobra cada vez más importancia debido a la evolución de la tecnología, encontrándonos con entornos más complejos y con requisitos de personal más especializado.

El objetivo de la seguridad de la información es buscar que dicha información cumpla unos requisitos o criterios [3]:

- Efectividad: se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- Eficiencia: se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
- Confidencialidad: se refiere a la protección de información sensible contra divulgación no autorizada.
- Integridad: se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

- Disponibilidad: se refiere a que la información esté accesible cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- Confiabilidad de la información: se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.
- No repudio: se refiere a la propiedad de asegurar que un mensaje es enviado por su autor original y recibido por el destinatario adecuado, de forma que un tercero pueda verificar la veracidad de la fuente.

El punto sobre el que pivota la mayor parte de la seguridad de los sistemas de información es el acceso de las personas a localizaciones, equipos, sistemas y aplicaciones. De ahí la importancia que se le dará en este proyecto al control de accesos y gestión de identidades.

2.3.2 Auditoría en informática

No existe una definición oficial única del concepto de auditoría informática, aunque la siguiente se acerca con suficiente exactitud a lo que se quiere expresar:

"La auditoría informática es el proceso encargado de recoger, agrupar y evaluar de forma independiente y objetiva las evidencias relacionadas con el entorno informático, las políticas, estándares y procedimientos de una entidad, así como el grado de satisfacción de usuarios y directivos, los controles existentes y los posibles riesgos relacionados con la informática" [17].

Como método de evaluación, la auditoría informática implica un proceso de revisión del control interno, en cuanto a:

- Cumplimiento de políticas, planes, procedimientos y estrategias definidos para la gestión de las tecnologías de la información.
- Estudio de las vulnerabilidades de los activos de la empresa, entendiendo estos como activos informáticos: equipos, software, datos y bases de datos etc.

- Comprobar la exactitud e integridad de la información, estableciendo controles a la entrada, proceso y salida de la información.

La auditoría informática también puede utilizarse como medio para realizar un estudio de los costes de la tecnología utilizada, así como de apoyo a la auditoría financiera. La auditoría puede ser interna o externa, siendo compatibles y complementarias.

Podemos definir control como "una actividad, acción o grupo de acciones realizadas por uno o varios elementos (humanos, máquinas) para prevenir, detectar y/o corregir errores, omisiones o irregularidades que afecten al funcionamiento de algo".

Un sistema de control interno es un conjunto de procesos, funciones, actividades, subsistemas y dispositivos, cuya misión total o parcial es garantizar que se alcanzan los objetivos de control.

La función principal de una auditoría informática es evaluar los controles internos que existen en una organización y contrastarlos con los objetivos de control establecidos por diferentes guías y estándares, según las necesidades de la empresa, para posteriormente emitir un informe de auditoría con recomendaciones de mejora.

Los controles pueden ser:

- Preventivos
- De detección
- De corrección
- Directivos

En función de los objetivos definidos para una auditoría informática podemos encontrar diferentes tipos de auditoría:

- Auditoría de la dirección
- Auditoría física
- Auditoría de la ofimática
- Auditoría de la explotación
- Auditoría del desarrollo
- Auditoría del mantenimiento
- Auditoría de bases de datos

- Auditoría de la calidad
- Auditoría de redes
- Auditoría de aplicaciones
- Auditoría jurídica de entornos informáticos
- Auditoría de técnica de sistemas
- Auditoría de la seguridad

En cuanto a las técnicas y herramientas más utilizadas para llevar a cabo una auditoría informática, podemos clasificarlas en dos grupos:

- Técnicas clásicas:
    - Cuestionarios
    - Entrevistas
    - Flujogramas
    - Muestreo estadístico
    - Comunicaciones escritas
- Técnicas avanzadas:
    - Engloba a todas las herramientas software que ayudan al proceso de auditoría, como pueden ser aplicaciones específicas según el campo de actuación, sistemas expertos, etc.

Fuentes: [18]

2.3.3 Niveles de control

Como se ha visto en el punto 2.3.2 anterior, para poder realizar una auditoría, es necesario saber contra que se quiere auditar, siendo lo habitual verificar el uso de controles. Para ello, en el proceso de auditoría es fundamental realizar una primera fase de análisis de controles. Normalmente este análisis debe ir determinado por los objetivos de la auditoría a realizar.

Como se podrá ver en el capítulo tres, y basándonos en la información disponible en los diferentes marcos de trabajo y estándares analizados para este proyecto, hemos detectado que existen ciertos aspectos comunes planteados cuando se trata de seguridad de la información. Es por esto que podemos definir una taxonomía sobre los controles basada en niveles:

Nivel general

El nivel general abarcaría los controles básicos esenciales, desde un punto de vista de cumplimiento, de gestión y de las personas, siendo conceptos que debería definir cualquier organización en cuanto a seguridad de la información se refiere. Este nivel se divide en dos subniveles:

- **Subnivel esencial legislativo**: en este nivel se incluyen aquellos controles a implementar por las necesidades de cumplimiento legal y normativo según el entorno de la organización.
- **Subnivel de prácticas comunes**: en este nivel se incluyen aquellos controles relacionados con buenas prácticas comunes en cuanto a seguridad de la información.

Nivel técnico

El nivel técnico abarcaría los controles relacionados con los sistemas de información, más concretamente con la técnica de sistemas y la tecnología. Este nivel se divide en dos subniveles:

- **Subnivel técnico común**: incluye aquellos controles relacionados con buenas prácticas comunes en cuanto a elementos técnicos de los que dispone cualquier organización en la actualidad.
- **Subnivel de solución técnica**: incluye aquellos controles necesarios para una solución técnica y/o tecnología concreta implantada en una organización.

Siguiendo esta taxonomía, podemos definir los siguientes controles que, de una forma u otra, son comunes a cualquier marco de referencia.

NIVEL GENERAL

- Subnivel esencial legislativo:
    - Derechos de propiedad intelectual.
    - Protección de registros de la organización.
    - Protección de datos y privacidad de información personal.
    - Leyes de comercio electrónico e Internet.

- Subnivel de prácticas comunes:

- Conjunto de políticas de seguridad: definición, revisión y cumplimiento de políticas y estándares de seguridad.
- Organización y asignación de responsabilidades en cuanto a seguridad de la información, tanto de personal interno como externo.
- Cultura y capacitación en seguridad.
- Clasificación de la información.
- Planificación de la arquitectura empresarial y de los sistemas.
- Gestión de incidentes y mejoras en seguridad.
- Gestión de la continuidad del negocio.
- Monitorización
- Auditoría

NIVEL TÉCNICO

- Subnivel técnico común:
  - Gestión de la vulnerabilidad técnica.
  - Protección contra código malicioso y móvil.
  - Gestión de copias de respaldo o *back-up.*
  - Gestión de medios.
  - Gestión de seguridad de la red.
  - Control de acceso: red, sistema operativo, aplicaciones, información.
  - Controles criptográficos.
- Nivel de solución técnica: este nivel depende de la tecnología implantada, y por tanto los controles son dependientes de la solución. Por ejemplo, podemos hablar de controles específicos de seguridad para:
  - Windows
  - Linux
  - Active Directory
  - Oracle
  - Sistemas ERP
  - Sistemas CRM
  - Etc.

3 Marcos de Referencia

3.1 COBIT®5

Control Objectives for Information and Related Technology (COBIT) es un marco de referencia único e integrado y aceptado internacionalmente, formado por un conjunto de marcos y guías, que la *Information Systems Audit and Control Association* (ISACA) ha construido para tratar de cubrir los conceptos establecidos por el estándar ISO/IEC 38500:2008 para una buena gobernanza de TI. El objetivo de COBIT®5 es ayudar a las empresas a alcanzar sus objetivos de gobierno y gestión en cuanto al uso corporativo de las TI.

El estándar ISO/IEC 38500:2008 define seis principios esenciales para un buen gobierno corporativo de TI:

- Responsabilidad: se refiere a la aceptación de responsabilidades respecto a TI por parte de todas las personas involucradas con la organización.
- Estrategia: deben existir planes estratégicos de TI alineados con los planes estratégicos de negocio.
- Adquisición: las adquisiciones de TI deben basarse en análisis transparentes, buscando un equilibrio entre beneficios, oportunidades, riesgos y costes.
- Rendimiento: dimensionar las TI para dar soporte a la organización con calidad y cumpliendo necesidades actuales y futuras.
- Conformidad: el gobierno de TI debe cumplir las legislaciones y normativas obligatorias aplicables en cada caso y entorno.
- Conducta humana: las políticas, prácticas y decisiones de TI deben mostrar respeto al factor humano, teniendo en cuenta las necesidades actuales y futuras.

Para cumplir estos principios de gobernanza, la dirección debería aplicar un modelo sustentado en tres tareas principales:

- Evaluar: examinar y juzgar sobre el uso actual y futuro de las TI.
- Dirigir: asignar las responsabilidades oportunas para transformar los planes y políticas en proyectos que tengan impacto en las infraestructuras, en las operaciones y en el negocio, fomentando siempre la cultura del buen gobierno.
- Monitorizar: vigilar el rendimiento de TI, asegurando que está en línea con los planes estratégicos y los objetivos del negocio.

Fuentes: [19] [1] [3]

3.1.1 Historia y evolución de COBIT

COBIT® se basó originalmente en los Objetivos de Control de la *Information Systems Audit and Control Foundation* (ISACF) y ha sido mejorado con los actuales y emergentes estándares internacionales a nivel técnico, profesional, regulatorio y específicos de la industria.

Los Objetivos de Control desarrollados se han basado en términos como "generalmente aplicable y aceptado" que es utilizado explícitamente en el mismo sentido que los *Principios de Contabilidad Generalmente Aceptados* (PCGA).

A través de los años y con el objetivo de cubrir las necesidades de TI, COBIT ha evolucionado desde un marco de auditoría en su primera versión (1996) hasta un marco integrado de gobierno corporativo de TI en su última versión publicada.

La última edición de COBIT, utilizada para el desarrollo de este proyecto, es la versión 5, publicada en 2012. Esta versión ha surgido como respuesta a la publicación en 2008 del estándar ISO/IEC 38500:2008. El objetivo de esta última versión es integrar los procesos de control publicados en COBIT 4.1 junto con otros marcos y normas como Val IT, Risk IT e ITIL.

La versión anterior COBIT 4.1, fue publicada el 8 de mayo de 2007, liberada por el *IT Governance Institute* (ITGI), y sirvió como revisión y mejora de la versión 4.0 (2006). Anteriormente, la versión COBIT 3 fue liberada por la ISACF en 2000.

Es importante destacar que a partir de COBIT 4 (2006) el marco de referencia se utiliza como herramienta de cumplimiento de, entre otras, la ley Sarbanes-Oxley *(Sarbanes-Oxley Act of 2002)* así como las directivas marcadas por la OCDE.

En la figura 3-1 se muestra la evolución de COBIT en relación a los conceptos a manejar en cuanto a gobierno de TI.

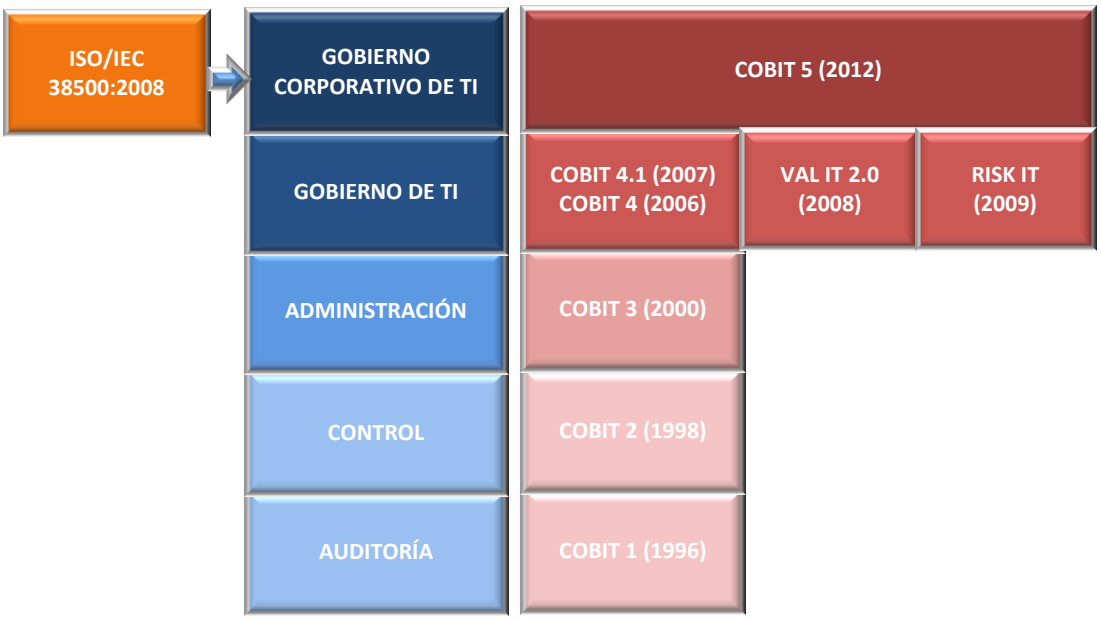


Figura 3-1: Evolución de necesidades de TI y COBIT

3.1.2 Entender COBIT®5

COBIT 5 es un marco bastante amplio y complejo, donde se relacionan muchos elementos con el objetivo de cubrir de forma global los principios para un buen gobierno y gestión de TI (ISO/IEC 38500:2008). Podemos identificar cuatro conceptos clave para entender COBIT 5:

1. Orientado al negocio.
2. Su implementación ofrece unos beneficios.
3. Es una familia de productos.
4. Basado en cinco principios.

El principal concepto a tener en cuenta es que COBIT 5 está **orientado al negocio**, por lo tanto, no se puede olvidar que el objetivo de todo lo tratado a través del mismo es cumplir con las necesidades de las partes interesadas en el negocio de la empresa.

Por otra parte, toda implementación de un marco de referencia, estándar y/o metodología se justifica siempre que ofrezca unos beneficios a las organizaciones. Los **beneficios** de implantar COBIT 5 son:

- Creación de valor para la empresa.
- Satisfacción del usuario.
- Cumplimiento.

A diferencia de COBTI 4.1 que era un documento que servía como marco de referencia para el gobierno de TI, COBIT 5 es una **familia de productos** formada por:

- Framework: documento con el resumen ejecutivo.
- Guías de catalizadores: donde podemos encontrar las guías de referencia de los procesos.
- Guías profesionales: guía de implementación, guía para la seguridad y otras guías en desarrollo.
- Entorno colaborativo online.

Por último, los cimientos sobre los que se desarrolla todo el marco de referencia son los cinco **principios** que define COBIT 5, y que se desarrollarán a continuación:

1. Satisfacer las necesidades de las partes interesadas de la organización
2. Cubrir la organización de forma integral
3. Aplicar un solo marco integrado
4. Habilitar un enfoque holístico
5. Separar el Gobierno de la Gestión

Principio 1. Satisfacer las necesidades de las partes interesadas

El objetivo de las empresas es **crear valor** para las **partes interesadas**. La forma de crear valor puede ser diferente para cada parte interesada. La función de gobierno es la encargada de **equilibrar** los intereses de las diferentes partes y transformar estos intereses en metas de negocio específicas. El objetivo de crear valor se consigue teniendo en cuenta:

- Realización de beneficios: ¿quién recibe los beneficios?
- Optimización de recursos: ¿qué recursos son necesarios?
- Optimización de riesgos: ¿quién asume el riesgo?

COBIT 5 utiliza un método en cascada. A partir de las **metas de negocio** se establecen las **metas de TI**, que a su vez determinan las **metas de catalizadores**. Los **procesos** son un tipo de catalizador. En la figura 3-2 se muestra la cascada de metas de COBIT 5.

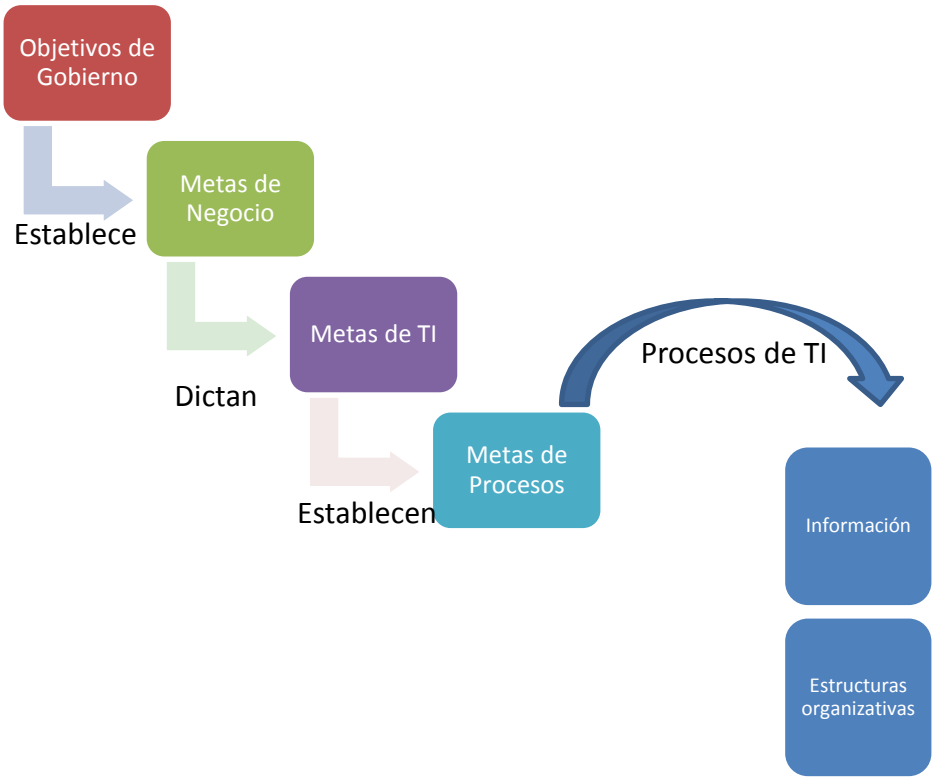


Figura 3-2: Cascada de metas de COBIT

En el ANEXO I se ofrece un listado con las metas de negocio y metas de TI.

Principio 2. Cubrir la empresa extremo a extremo

COBIT 5 permite integrar el sistema de gobierno de TI de la empresa en cualquier sistema de gobierno. Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información, ya sea a través de elementos (procesos y servicios) internos o externos. Se dice que es extremo a extremo porque involucra todo y a todos los catalizadores relevantes para el bueno gobierno y gestión de TI.

Principio 3. Aplicar un marco de referencia único integrado

Existen muchos estándares, buenas prácticas y metodologías para diferentes ámbitos y dominios de TI. COBIT 5 se puede alinear a alto nivel con diferentes estándares de forma que sirva como marco de trabajo principal para el gobierno y gestión de TI.

Por otra parte, ofrece un lenguaje común y no dependiente de ninguna tecnología, y aglutina todo el conocimiento adquirido durante años de trabajo en ISACA, representado por diferentes marcos como el propio COBIT, Val IT, RiskIT y BMIS.

Principio 4. Hacer posible un enfoque holístico

Con el objetivo de cumplir con los objetivos de una forma global e integral, COBIT 5 establece siete **catalizadores:**

1. Principios, políticas y marcos: permiten traducir el comportamiento deseado en guías prácticas para la gestión diaria.
2. Procesos: definen las prácticas y actividades para alcanzar los objetivos y metas de TI
3. Estructuras organizacionales: entidades que toman las decisiones dentro de la organización
4. Cultura, ética y comportamiento: la manera de actuar de las personas es un factor de éxito en las actividades de gobierno y gestión.
5. Información: toda la información producida y utilizada en la organización.
6. Servicios, infraestructura y aplicaciones: proporcionan a la empresa la capacidad de procesamiento de la información.
7. Personas, habilidades y competencias: permiten completar todas las actividades de forma correcta, tomar las decisiones adecuadas y realizar las acciones correctivas oportunas.

Principio 5. Separar el Gobierno de la Gestión

COBIT 5 marca una diferencia clara entre los conceptos de Gobierno y Gestión:

- Gobierno: *"El Gobierno **asegura** que se **evalúan** las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; **estableciendo** la dirección a través de la priorización y la toma de decisiones; y **midiendo** el rendimiento y el cumplimiento respecto a la dirección y metas acordadas"* [3].

  La función de gobierno corresponde normalmente a la Junta Directiva, liderada por el Presidente.
- Gestión: *"La gestión **planifica, construye, ejecuta y controla** actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales"* [3].

  La función de gestión corresponde normalmente a la Gerencia, encabezada por el Director Ejecutivo (CEO).

Fuentes: [3]

3.1.3 COBIT®5, auditoría y seguridad de la información

La relación de ISACA con la auditoría es fuerte, al tratarse de la entidad que ofrece la certificación sobre auditoría de sistemas de información más reconocida internacionalmente: CISA (*Certified Information Systems Auditor).*

Encontramos varias referencias relacionados con la auditoría a través de ISACA, destacando:

- ITAF: modelo de referencia de buenas prácticas para auditoría y control de sistemas de información. La última edición es la tercera, publicada en septiembre de 2014.
- COBIT: la función de auditoría y control de TI forma parte de la gobernanza corporativa de TI, por lo que COBIT 5 está alineado con estas funciones. Sirve como marco donde contextualizar otros estándares de auditoría y control relacionados, como ITAF, IPPF (*International Professional Practices Framework*) y SSAE (*Statement on Standards for Attestation Engagements*).

La visión de COBIT 5 sobre auditoría en TI se hace desde dos perspectivas:

- Perspectiva de función de **control** (aseguramiento, del inglés *assurance*): describe como los catalizadores contribuyen al control (aseguramiento)
- Perspectiva de **evaluación**: describe el asunto sobre el que se tiene que realizar el control, que en este caso es TI. Para realizar la función de evaluación, COBIT 5 define 3 procesos catalizadores principales:

Nº Proceso	Nombre
MEA01	Supervisar, evaluar y asegurar rendimiento y conformidad
MEA02	Supervisar, evaluar y asegurar el sistema de control interno
MEA03	Supervisar, evaluar y asegurar el cumplimiento con requerimientos externos

Tabla 3-1. Procesos de supervisión y evaluación COBIT 5

Por otra parte, ISACA define seguridad de la información dentro de lo que podríamos denominar una definición estándar:

"Ensures that within the Enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)".

"Asegura que dentro de la empresa, la información está protegida frente a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y la falta de acceso cuando sea necesario (disponibilidad)".

Los beneficios de utilizar COBIT 5 para gestionar la seguridad de la información son:

- Reducción de la **complejidad** e incremento de la **rentabilidad** debido a una integración de la seguridad de la información mejorada y sencilla, basada en estándares y buenas prácticas.
- Incremento de la **satisfacción del usuario** con la disposición de la seguridad de la información y los resultados obtenidos.
- Concienciación respecto a los **riesgos** y decisiones informadas de los mismos.
- Mejora en la **prevención**, **detección** y **recuperación**.
- Reducción de impacto de los **incidentes de seguridad**.
- Soporte mejorado para la **innovación** y la **competitividad**.
- Mejora en la **gestión de costes** relacionados con la función de seguridad de la información.
- Mejor **comprensión** de seguridad de la información.

La visión holística de COBIT 5 permite que se puedan utilizar los siete catalizadores para definir una buena gestión de la seguridad de la información. No obstante, enfocaremos la selección de controles en los procesos catalizadores ya que son los elementos donde se puede obtener información más precisa en cuanto a actividades a realizar para una buena gestión de TI y de su seguridad.

Además, debido a que COBIT 5 nace como marco para cubrir la empresa extremo a extremo (principio 2) no podemos olvidar la relación de este tipo de catalizador (proceso) con el resto:

- Los procesos necesitan políticas y procedimientos para asegurar una implementación y ejecución consistente.
- Los procesos necesitan estructuras organizativas y roles para operar.
- Los aspectos culturales y de comportamiento determinan la ejecución adecuada de los procesos.

- Los procesos producen y requieren capacidades de servicio: infraestructura y aplicaciones principalmente.
- Los procesos necesitan información que debe estar clasificada.

Haciendo una revisión de los procesos catalizadores (ver ANEXO II), podemos identificar los siguientes procesos como esenciales a la hora de tratar de definir controles para la seguridad de la información, destacando por encima de todos los procesos APO13 y DSS05, que son los referentes a seguridad:

Nº Proceso	Nombre
APO01	Gestionar el marco de gestión de TI
APO03	Gestionar la arquitectura empresarial
APO12	Gestionar el riesgo
APO13	Gestionar la seguridad
DSS02	Gestionar las peticiones y los incidentes del servicio
DSS04	Gestionar la continuidad
DSS05	Gestionar los servicios de seguridad

Tabla 3-2. Procesos COBIT 5 para seguridad de la información

De los procesos referentes a evaluación y supervisión: MEA01, MEA02 y MEA03, podemos destacar MEA02 y MEA03 en cuanto a control de seguridad de la información.

Nº Proceso	Nombre
MEA02	Supervisar, evaluar y valorar el sistema de control interno
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Tabla 3-3. Procesos COBIT 5 de evaluación en seguridad de la información

Además, en cualquier análisis de controles con COBIT 5, al englobarse la tarea en la gobernanza de TI, siempre hay que tener en cuenta los procesos de gobierno, que no veremos en este proyecto al considerar que están fuera del alcance del mismo:

Nº Proceso	Nombre
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno
EDM02	Asegurar la entrega de beneficios
EDM03	Asegurar la optimización del riesgo
EDM04	Asegurar la optimización de recursos
EDM05	Asegurar la transparencia hacia las partes interesadas

Tabla 3-4. Procesos COBIT 5 de gobernanza TI

A continuación se describen, a modo de resumen, los objetivos de control de los procesos involucrados con la seguridad de la información, así como los controles extraídos para una buena evaluación según COBIT 5. Nos centraremos más en los procesos APO13 (Gestión de la seguridad) y DSS05 (Gestión de los servicios de seguridad), ya que servirán como punto de referencia para el desarrollo de los siguientes puntos del proyecto.[5]

APO01. Gestionar el marco de gobierno de TI

En este proceso catalizador se tratan los aspectos generales de cualquier entorno de TI, de donde podemos extraer los controles de la tabla 3-5.

Id. Control	Control
APO01.1	Definición de la estructura organizativa, asignación de roles y responsabilidades.
APO01.2	Procedimientos de comunicación de los objetivos de dirección al resto de la organización.
APO01.3	Estudio de la ubicación de la función de TI.
APO01.4	Definición y clasificación de la información y del sistema.
APO01.5	Procedimientos de gestión para la continua mejora de los procesos.
APO01.6	Procedimientos de mantenimiento y cumplimiento de políticas y procedimientos del entorno y corporativos.

Tabla 3-5. Controles COBIT 5 de gestión de TI

[5] Aunque los controles han sido extraídos de COBIT 5, los identificadores son específicos de este documento.

APO03. Gestionar la arquitectura empresarial

La arquitectura empresarial se compone de todos los procesos de negocio, información, aplicaciones y arquitectura tecnológica. Es un elemento esencial para cualquier organización ya que establece el esquema base de módulos y relaciones sobre el que se apoyarán las estrategias y operaciones de la organización. Es fundamental tenerla en cuenta en cualquier proceso de control y auditoría, y su definición puede apoyarse en estándares como TOGAF®9. La gestión de la arquitectura empresarial es un punto extenso, pero de forma resumida los controles que podemos extraer se muestran en la tabla 3-6:

Id. Control	Control
APO03.1	Desarrollo de la visión de la arquitectura: definición del alcance y disposición alineados con los objetivos estratégicos de la organización
APO03.2	Establecimiento de un repositorio de arquitectura: donde se incluye la definición de la misma y todos los elementos de apoyo para obtener una visión general.
APO03.3	Revisión de la arquitectura periódica en base a los objetivos estratégicos.
APO03.4	Definición de un plan de implantación de la arquitectura, que incluya estudios de oportunidades y soluciones.
APO03.5	Desarrollo de guía de proyectos de implantación de los diferentes módulos de la arquitectura, así como supervisión de los mismos.

Tabla 3-6. Controles COBIT 5 de arquitectura empresarial

Es importante la relación que guarda este proceso con APO02.03 (Gestionar la estrategia), donde se establecen controles para identificar, evaluar soluciones y servicios de TI junto a los riesgos asociados, en línea con los objetivos y estrategia de negocio.

APO12. Gestionar el riesgo.

La gestión del riesgo es algo fundamental en cualquier ámbito relacionado con TI. La idea fundamental es hacer un análisis de riesgos, y en nuestro caso particular, riesgos relacionados con la seguridad de la información. Podemos determinar los siguientes controles:

Id. Control	Control
APO12.1	Análisis de riesgos
APO12.2	Procedimientos de comunicación de riesgos
APO12.3	Definición de una política de riesgos que incluya: portafolio de acciones para la gestión del riesgo y respuesta.

Tabla 3-7. Controles COBIT 5 de gestión de riesgos

APO13. Gestionar la seguridad

La gestión de la seguridad toma como elemento indispensable la existencia de un SGSI (Sistema de Gestión de la Seguridad de la Información). De esta forma, se puede mantener e incluso reducir el impacto de los incidentes de seguridad de la información en los procesos y objetivos de negocio. Podemos extraer los siguientes controles:

Id. Control	Control
APO13.1	Lo más importante es controlar que exista un SGSI implantado en la organización
APO13.2	Definición de un plan de gestión de riesgos de seguridad de la información: este control está directamente relacionado con los controles del proceso APO12 (ver punto anterior) y por tanto se puede incluir en la política de riesgos corporativa.
APO13.3	Elaboración y mantenimiento periódico de un inventario de activos relacionados con el SGSI.
APO13.4	Definición de métricas para calcular la efectividad de las prácticas de gestión seleccionadas.
APO13.5	Establecimiento de programas de formación y concienciación en seguridad de la información
APO13.6	Revisión periódica del SGSI: políticas, objetivos y buenas prácticas; por parte de los responsables y la dirección
APO13.7	Realización de auditorías internas y externas
APO13.8	Retroalimentación de resultado de auditorías y estudios de métricas en la supervisión y revisión del SGSI.
APO13.9	Registro de acciones y eventos con más impacto en el rendimiento del SGSI.

Tabla 3-8: Controles COBIT 5 de gestión de la seguridad

DSS02. Gestionar las peticiones e incidentes del servicio.

Este proceso está relacionado con la seguridad de la información en la medida que en cualquier entorno TI se producen incidentes, siendo unos de los más importantes y con más impacto los incidentes de seguridad. Podemos determinar los siguientes controles a tener en cuenta:

Id. Control	Control
DSS02.1	Definición y clasificación de incidentes, particularmente incidentes de seguridad.
DSS02.2	Existencia de un sistema de gestión de incidentes, que permita: • Registro, clasificación y priorización. • Procedimientos de verificación, diagnóstico y localización. • Resolución, recuperación y cierre de incidentes • Seguimiento de estado e informes.

Tabla 3-9. Controles COBIT 5 de gestión de incidentes

DSS04. Gestionar la continuidad

La seguridad de la información es un concepto clave a la hora de tratar la continuidad del negocio en caso de fallos y desastres. Los controles esenciales son:

Id. Control	Control
DSS04.1	Definición de un plan de continuidad del negocio, con sus objetivos y alcance. Las acciones que se deben llevar a cabo de forma iterativa sobre esta política son: • Desarrollo e implementación • Ejecución y pruebas • Revisión, mantenimiento y mejora. • Proporcionar formación. • Gestionar acuerdos de respaldo con partes implicadas ya sean internas o externas.

Tabla 3-10. Controles COBIT 5 de gestión de incidentes

DSS05. Gestionar los servicios de seguridad

Podemos considerar este proceso como uno de los más relevantes para el desarrollo de los siguientes puntos de este proyecto. Los controles extraídos de este proceso permiten establecer una relación directa con la técnica de sistemas y más concretamente con elementos técnicos de seguridad de la información.

Según COBIT 5 [20], se establecen siete áreas de control principales:

- Protección contra software malicioso.
- Seguridad de la red y conexiones.

- Seguridad de los puestos de usuario final.
- Gestión de identidades y acceso lógico.
- Gestión de acceso físico.
- Documentación sensible y dispositivos de salida.
- Gestión de eventos de seguridad.

Como ya se introdujo en el punto 2.3.1, el control de los accesos es posiblemente el punto más importante a nivel técnico en cuanto a seguridad de la información.

Controles para protección contra software malicioso

Id. Control	Control
DSS05.1.1	Procedimientos de prevención relacionados con concienciación al personal.
DSS05.1.2	Herramientas de protección contra software malicioso, y en relación a ellas: • Instalación en todas las ubicaciones • Actualización automática • Distribución centralizada
DSS05.1.3	Revisión periódica de nueva información relacionada con amenazas.
DSS05.1.4	Filtrado de tráfico entrante: correo electrónico, ficheros adjuntos y descargas.

Tabla 3-11. Controles COBIT 5 de protección contra software malicioso

Controles para gestión de la seguridad de la red y las conexiones

Id. Control	Control
DSS05.2.1	Política de seguridad para las conexiones.
DSS05.2.2	Configuración de dispositivos para forzar solicitud de credenciales.
DSS05.2.3	Procedimientos para permitir sólo el acceso a la red a dispositivos autorizados.
DSS05.2.4	Implementación de mecanismos de filtrado de red, cortafuegos y detección de intrusos.
DSS05.2.5	Cifrado de información transmitida, siempre que el tipo de información lo requiera por su clasificación.
DSS05.2.6	Configuración segura de los equipos de red.
DSS05.2.7	Implantar mecanismos de confianza para permitir transmisión segura de

	la información.
DSS05.2.8	Lanzamiento periódico de pruebas de intrusión y de seguridad de los sistemas.

Tabla 3-12. Controles COBIT 5 de seguridad en redes y conexiones

Controles para la seguridad de los puestos de usuarios

Id. Control	Control
DSS05.3.1	Configuración segura de los puestos de usuarios, incluyendo: • Bloqueo de dispositivos por inactividad. • Cifrado de información almacenada en base a la forma y tipo. • Gestión de acceso (lógico y físico) y control remoto. • Configuración de red de forma segura.
DSS05.3.2	Filtrado de tráfico de red en los dispositivos.

Tabla 3-13. Controles COBIT 5 de seguridad en puestos de usuario

Controles para la gestión de identidades y control de acceso lógico

Id. Control	Control
DSS05.4.1	Gestión de identidades y derechos de acceso de acuerdo a los requisitos de negocio, basada en el principio de menor privilegio.
DSS05.4.2	Identificación unívoca en cualquier actividad de acceso a la información llevada a cabo por todo el personal: interno, externo y temporal.
DSS05.4.3	Autenticación de todo acceso a los activos de información, en línea con los requisitos de negocio
DSS05.4.4	Administración de identidades: creación, modificación y eliminación; bajo autorización de los responsables.
DSS05.4.5	Gestión independiente de cuentas de usuario privilegiadas y sus accesos.
DSS05.4.6	Revisión periódica de cuentas y derechos de acceso.

Tabla 3-14. Controles COBIT 5 de gestión de identidades y control de acceso lógico

Controles para la gestión de acceso físico

Id. Control	Control
DSS05.5.1	Procedimientos de gestión para los accesos a las instalaciones de la organización.
DSS05.5.2	Autorización de accesos por parte del responsable, y registro de los mismos
DSS05.5.3	Revisión y actualización de los perfiles de acceso.
DSS05.5.4	Visibilidad en todo momento de la acreditación del personal.
DSS05.5.5	Escoltar a visitantes y alertar a Seguridad en caso contrario.

Tabla 3-15. Controles COBIT 5 de gestión de acceso físico

Controles para la gestión de documentos y dispositivos de salida sensibles

Id. Control	Control
DSS05.6.1	Existencia de procedimientos para el tratamiento de documentos y dispositivos sensibles, que incluyan: • Recepción, utilización y eliminación de formularios especiales. • Asignación de privilegios. • Creación de un inventario específico.

Tabla 3-16. Controles COBIT 5 de gestión de documentos y dispositivos

Controles relacionados con la supervisión de eventos de seguridad

Id. Control	Control
DSS05.7.1	Registro de eventos de seguridad, en línea con la política de riesgos.
DSS05.7.2	Definición y comunicación de incidentes potenciales
DSS05.7.3	Revisión de los registros de eventos de seguridad.
DSS05.7.4	Integración de los incidentes de seguridad dentro del sistemas de gestión de incidentes corporativo (relacionado con el proceso DSS02).

Tabla 3-17. Controles COBIT 5 de supervisión de eventos de seguridad

MEA02. Supervisar, evaluar y valorar el sistema de control interno.

Este proceso está relacionado directamente con la función de auditoría de TI. El objetivo es implementar procedimientos para la evaluación continua del control interno. Esto ayuda a la dirección a detectar deficiencias e ineficiencias, impulsando la mejora constante en los procesos de TI. Los principales controles que podemos extraer son:

Id. Control	Control
MEA02.1	Procedimientos de supervisión interno.
MEA02.2	Revisión de la efectividad de los controles sobre los procesos de negocio.
MEA02.3	Autoevaluaciones de control: auditoría interna.
MEA02.4	Procedimientos para la identificación y comunicación de deficiencias.
MEA02.5	Garantizar auditorías externas independientes y cualificadas.
MEA02.6	Impulso de iniciativas de aseguramiento, que incluyan: • Planificación • Estudio • Ejecución

Tabla 3-18. Controles COBIT 5 de supervisión y evaluación del sistema de control

MEA03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

El objetivo de este proceso es establecer procedimientos que permitan a la organización estar alineada con su entorno: sector, regulación según zona geográfica, etc. Para ello, podemos extraer los siguientes controles:

Id. Control	Control
MEA03.1	Identificación de requisitos externos de cumplimiento.
MEA03.2	Optimización de la respuesta a requisitos externos.
MEA03.3	Confirmación del cumplimiento con los requisitos externos.

Tabla 3-19: Controles COBIT 5 de supervisión y evaluación de cumplimiento con regulaciones

Por último, en el punto 3.3 se verá el alineamiento de estos controles básicos con el estándar ISO/IEC 27002:2013, así como la organización de los mismos según los criterios de clasificación establecidos en el punto 2.3.3 (Niveles de control).

Fuentes: [3]**,** [20]

3.2 ISO/IEC 27002:2013

3.2.1 Historia y evolución de ISO/IEC 27002

Desde 1901 la Institución Británica de Estándares (BSI, *British Standards Institution*) se ha encargado de la normalización a nivel mundial, siendo la primera entidad dedicada a tal fin. Entre algunas de sus normas más importantes se encuentran la BS5750, relativa a la calidad, publicada en 1979 y ahora renombrada a ISO 9001); y la BS7750, dedicada al medio ambiente desde 1992 y renombrada como ISO 14001.

La historia de la seguridad de la información con BSI comienza en 1995 con la publicación de la norma BS7799, un código de buenas prácticas para la gestión de la información. A esta norma le sigue en 1998 la publicación de BS7799-2, una especificación para los sistemas de gestión de la seguridad de la información (SGSI). En 1999 se realiza una revisión de ambas normas fijándolas como BS7799-1:1999 y BS7799-2:1999. Como consecuencia de esta revisión, en el año 2000 la primera parte se adopta como estándar internacional por ISO/IEC, con el nombre de ISO/IEC 17799:2000.

En España se adoptan ambas normas como UNE-ISO/IEC 17799:2002 para la primera parte (año 2002) y UNE 71502 en el año 2004 (aún sin estándar internacional relacionado) para la segunda parte de la norma.

Ya en el 2005, se revisa y se renombra BS7799-2 para adoptarla a la estructura de ISO, con lo que se crea la ISO/IEC 27001:2005. A su vez, en el mismo año se revisa ISO/IEC 17799, obteniendo como resultado ISO/IEC 17799:2005 que en el año 2007 es renombrada como ISO/IEC 27002:2007. Es por esto que el contenido de la ISO 27002 es el mismo que ISO 17799:2005, cuya estructura, visión y controles serán los que se expondrán en este capítulo.

En 2013 se ha hecho una revisión del estándar para adaptarlo a los cambios realizados en ISO/IEC 27001:2013, y por tanto la denominación última es ISO/IEC 27002:2013.

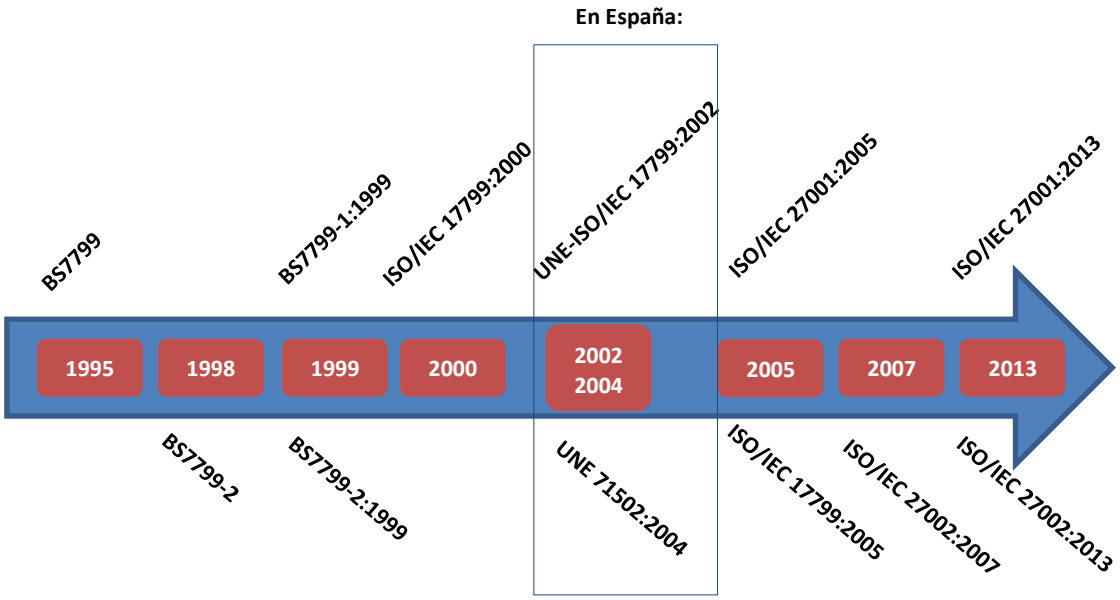


Figura 3-3: Evolución de ISO/IEC 27002

3.2.2 Entender ISO/IEC 27002

El estándar establece que para lograr una protección adecuada de la información se necesita realizar la implantación de un modelo de seguridad lo más formal posible, definiendo un sistema de seguridad para el que existen dos tipos de medios de implementación:

- Medios técnicos, que son limitados y que necesitan del apoyo fundamental de los otros medios (de gestión).
- Medios de gestión, en los que participan accionistas, proveedores, clientes y otros grupos de interés para el mantenimiento de la seguridad de la información.

Analizando el estándar, podemos establecer cuatro fases principales para el proceso de implementación del modelo de seguridad (ver figura 3-4):

1. Evaluación de riesgos.
    a. Identificación de los requisitos de seguridad
    b. Determinar la acción de gestión adecuada
2. Selección de controles adecuados
3. Implementación de controles

4. Monitorización, evaluación y mejora.

El primer paso fundamental, y del que depende la eficacia del modelo de seguridad, es la evaluación de riesgos. Los actores principales en esta fase son los medios de gestión, debido a su capacidad de decisión e influencia dentro de las organizaciones. Deben realizar las tareas principales:

- Identificar los requisitos de seguridad, que se alimenta de tres fuentes:
    - Identificación de amenazas y su impacto.
    - Requisitos legales, regulatorios, estatutarios y contractuales.
    - Definición particular de principios, objetivos y requisitos comerciales.
- Determinar la acción de gestión apropiada, para lo que es importante:
    - Buscar un equilibrio entre el coste de establecer controles de seguridad y el posible daño comercial de no implementarlos.

Existen diferentes opciones en cuanto a las acciones a determinar:

- Aplicar controles apropiados para reducir riesgos.
- Aceptar riesgos conscientemente, siempre que se cumpla con la política de la organización.
- Evitar riesgos, no permitiendo acciones que podrían causar que el riesgo ocurra.
- Transferir riesgos asociados a otros grupos, como aseguradoras u otros proveedores.

Una vez realizada la evaluación de riesgos, hay que tener en cuenta que en las fases de selección e implementación de controles ningún conjunto de controles puede lograr la seguridad completa, por lo que se hace necesario implementar una gestión complementaria de monitorización, evaluación y mejora de la eficiencia de los controles de seguridad; de ahí la existencia de la cuarta fase en el proceso. Esta fase se desarrolla en paralelo con la fase de implementación de controles.

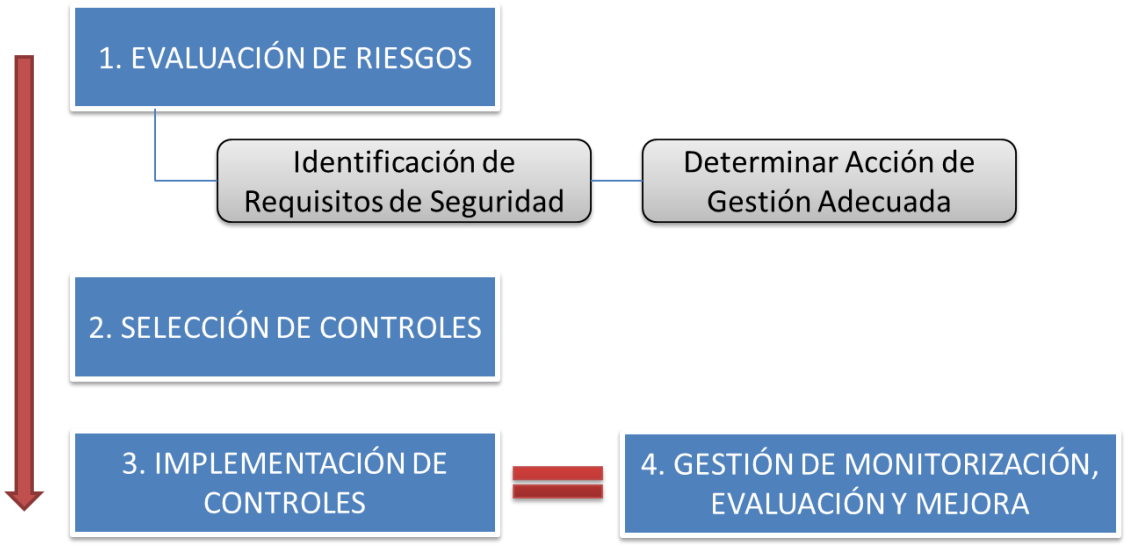


Figura 3-4: Fases según ISO/IEC 27002:2013

A modo de resumen, la estructura del estándar se divide en 14 dominios de seguridad que contienen 35 objetivos de control y 114 controles. Los dominios son:

1. Políticas de seguridad (sección 5).
2. Aspectos organizativos de la seguridad de la información (sección 6).
3. Seguridad ligada a los recursos humanos (sección 7).
4. Gestión de activos (sección 8).
5. Control de accesos (sección 9).
6. Cifrado (sección 10).
7. Seguridad física y ambiental (sección 11).
8. Seguridad en la operativa (sección 12).
9. Seguridad en las telecomunicaciones (sección 13).
10. Adquisición, desarrollo y mantenimiento de los sistemas de información (sección 14).
11. Relaciones con proveedores (sección 15).
12. Gestión de incidentes en la seguridad de la información (sección 16).
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio (sección 17).
14. Cumplimiento (sección 18).

Fuentes: [21]

3.2.3 Selección de controles

El estándar ISO/IEC 27002:2013 es un estándar algo extenso, por lo que resultaría inabarcable su exposición en un proyecto de estas características. Además, la finalidad de cualquier marco o estándar es servir de herramienta para una correcta implantación de procesos y/o prácticas. Por este motivo, haremos una descripción de los principales puntos en base a la clasificación de controles descrita en el punto 2.3.3 (Niveles de control).

Se mostrará la referencia a los objetivos de control de la norma en cada categoría, así como un resumen de los controles extraídos. Este trabajo de análisis del estándar permitirá concluir que tanto COBIT 5 como ISO/IEC 27002:2013 se pueden alinear y completar para una puesta en práctica de controles en cuanto a seguridad de la información. El alineamiento de ambos marcos se introducirá en el punto 3.3 'Alineamiento COBIT 5 – ISO/IEC 27002:2013'.

Apartado ISO/IEC 18.1. Cumplimiento

Los temas relativos a cumplimiento con requisitos externos se tratan bajo el dominio de 'Cumplimiento', que se localiza en la sección 18 del estándar. Podemos extraer los controles en el objetivo de control 18.1 'Cumplimiento de los requisitos legales y contractuales', mostrados de forma genérica en la tabla 3-20.

Id. Control	Control
ISO18.1.1	Definir política de cumplimiento de derechos de propiedad intelectual.
ISO18.1.2	Herramienta de gestión de inventario: monitorizar, auditar y controlar activos (hardware, software y otros).
ISO18.1.3	Gestión de licencias: control anti-pirateo, control de copias no permitidas.
ISO18.1.4	Procedimiento de clasificación e identificación de registros: asociando el periodo de retención de los mismos. Cumplimiento de normas estatutarias, contractuales y legales del entorno.
ISO18.1.5	Mecanismos de protección.
ISO18.1.6	Definir política de protección de datos: en España la LOPD y el reglamento que la desarrolla.

Tabla 3-20. Controles ISO/IEC 27002 de cumplimiento normativo

Apartado 5.1 Políticas de seguridad

El objetivo de establecer políticas de seguridad es proporcionar directrices en cuanto a la seguridad de la información en línea con los requisitos de negocio. Este tema se trata en la sección 5 del estándar. Podemos extraer los controles que se muestran en la tabla 3-21.

Id. Control	Control
ISO5.1.1	Definir política de seguridad: DOCUMENTO DE LA POLÍTICA DE SEGURIDAD (aprobado por diferentes niveles y comunicado a todos los empleados). El contenido mínimo establecido por el estándar es: • Definiciones • Declaración de intenciones • Marco de referencia • Responsabilidades • Explicación breve de políticas • Referencias a documentación de apoyo

Tabla 3-21. Controles ISO/IEC 27002 de política de seguridad

Apartado ISO/IEC 6.1. Organización interna

La organización de las personas y sus responsabilidades es vital para el buen funcionamiento de la empresa. Estos conceptos se tratan en el apartado 6.1 del estándar. Podemos extraer los controles que se muestran en la tabla 3-22.

Id. Control	Control
ISO6.1.1	Establecer un marco de referencia para controlar la implementación: organigrama y niveles de responsabilidad.
ISO6.1.2	Definir activos y procesos de seguridad de cada sistema, asignar un responsable y establecer niveles de autorización y delegación.

Tabla 3-22. Controles ISO/IEC 27002 de organización interna

Apartado ISO/IEC 7.2.2. Concienciación, educación y capacitación

Un punto también relacionado con las personas es su concienciación y formación en temas relativos a seguridad. El estándar sólo relaciona esta cuestión durante la contratación de recursos humanos en el apartado 7.2.2, dejando sin cubrir detalladamente la formación al personal de posibles proveedores o suministradores de servicios. De forma resumida, los controles extraídos se muestran en la tabla 3-23.

Id. Control	Control
ISO7.2.1	Existencia de procesos de formación y capacitación en temas de seguridad a empleados y personal externo: formación previa al acceso y formación continua (actualización).

Tabla 3-23. Controles ISO/IEC 27002 de educación y capacitación

Apartado ISO/IEC 8.2. Clasificación de la información

El estándar trata las cuestiones relativas a clasificación de la información en el apartado 8.2. Los controles extraídos se muestran en la tabla 3-24.

Id. Control	Control
ISO8.2.1	Clasificación de la información según su valor, requisitos legales, sensibilidad y grado crítico.
ISO8.2.2	Procedimientos para el etiquetado de la información y el manejo seguro para cada nivel de clasificación.

Tabla 3-24. Controles ISO/IEC 27002 de clasificación de la información

Apartado ISO/IEC 16.1 Gestión de incidentes

Algo también fundamental, la gestión de incidentes, se trata en el estándar en el apartado 16.1. En este caso, la selección de controles es algo más detallada al tratarse de un punto muy importante, ya que los incidentes tienen impacto en los niveles de servicio y operaciones de la organización. Los controles extraídos se muestran en la tabla 3-25.

Id. Control	Control
ISO16.1.1	Definición de responsabilidades asociados a los incidentes
ISO16.1.2	Procedimientos para gestionar cada tipo de incidente, en base a los incidentes habituales identificados: pérdida de servicio, código malicioso, negación de servicio, violaciones de integridad y confidencialidad, etc.
ISO16.1.3	Procedimientos para cubrir información de análisis de la causa de los incidentes, la contingencia aplicada, el proceso de comunicación y la notificación a las autoridades oportunas.
ISO16.1.4	Mecanismos de cuantificación y monitorización de los tipos de incidentes.
ISO16.1.5	Procedimientos que permitan recolectar el máximo de información posible (recolección de evidencias) utilizando propiedades como: • Admisibilidad: si una evidencia puede ser utilizada en un tribunal. • Peso: calidad e integridad de la evidencia.

Tabla 3-25. Controles ISO/IEC 27002 de gestión de incidentes

Apartado ISO/IEC 17.1. Gestión de la continuidad del negocio

Otro de los aspectos esenciales, y relacionado con posibles incidentes e interrupciones, es la gestión de la continuidad del negocio. El estándar trata este punto en el apartado 17.1. La selección de controles generales se muestra en la tabla 3-26.

Id. Control	Control
ISO17.1.1	Identificación de eventos que puedan causar interrupciones en las operaciones.
ISO17.1.2	Existencia de un plan de continuidad del negocio para seguridad de la información con las siguientes propiedades: - Incluido en un marco global, dentro un plan de continuidad general de la organización - Desarrollado e implementado de acuerdos a los niveles y tiempos establecidos. - Probado, mantenido y revisado de forma periódica.

Tabla 3-26. Controles ISO/IEC 27002 de gestión de la continuidad del negocio

Apartado ISO/IEC 12.4. Registro de actividad y monitorización

Los temas de registro de eventos, actividad y su monitorización se tratan en el apartado 12.4 del estándar. Los controles que hemos extraído de forma genérica se muestran en la tabla 3-27.

Id. Control	Control
ISO12.1	Establecimiento del nivel de monitorización en base al análisis de riesgos. Habilitación de registro de eventos en función de los niveles de monitorización establecidos y con la información mínima esencial.
ISO12.2	Registro independiente de eventos de administrador y operador, así como del registro de errores.
ISO12.3	Sincronización de los relojes de todos los equipos de la red de la organización

Tabla 3-27. Controles ISO/IEC 27002 de registro de actividad y monitorización

Apartado ISO/IEC 12.7. Consideraciones de auditoría

Id. Control	Control
ISO12.4	Planificación y acuerdo con la dirección de auditorías, minimizando el riesgo de interrupciones.
ISO12.5	Protección de las herramientas de auditoría de los sistemas de información.

Tabla 3-28. Controles ISO/IEC 27002 de auditoría

Apartado ISO/IEC 12.6. Gestión de la vulnerabilidad técnica

La vulnerabilidad técnica se refiere al hecho de que no existe ningún software totalmente seguro, y por tanto hay que realizar una gestión adecuada de sus vulnerabilidades. Estas vulnerabilidades son tratadas y solventadas en muchos casos por los fabricantes. Un resumen de los controles extraídos del apartado 12.6 del estándar se muestra en la tabla 3-29.

Id. Control	Control
ISO12.6.1	Establecimiento de responsabilidades asociadas a la gestión de la vulnerabilidad técnica: monitorizaciones, evaluaciones de riesgos, etc.
ISO12.6.2	Procedimientos de identificación y notificación de vulnerabilidades. Control de inventario y seguimiento de publicaciones de vulnerabilidades de fabricantes y centros de respuesta a incidentes
ISO12.6.3	Aplicación de parches, previo análisis de riesgos y seguimiento de la acción según el plan de gestión de cambios o gestión de incidentes de seguridad.

Tabla 3-29. Controles ISO/IEC 27002 de gestión de la vulnerabilidad técnica

Apartado ISO/IEC 12.2. Protección contra código malicioso

La protección contra el software y código malicioso la hace el estándar en el punto 12.2. En este sentido, también es muy importante el control de uso de software con licencias (en contraposición a la obtención ilegal de software). En la tabla 3-30 se muestra un resumen de los controles a tener en cuenta sobre esta cuestión.

Id. Control	Control
ISO12.2.1	Procedimientos de prevención, detección y recuperación. Dentro de los procedimientos se incluyen todas las herramientas a valorar para el control del software malicioso.
ISO12.2.2	Existencia de política de prohibición de uso de software no autorizado que incluya revisión y chequeo regular del software, archivos, adjuntos de correo y páginas web.

Tabla 3-30. Controles ISO/IEC 27002 de protección contra código malicioso

Apartado ISO/IEC 12.3. Gestión de copias de seguridad

Toda organización debe mantener copias de seguridad de los activos de información más importantes para el cumplimiento de los requisitos de negocio. El estándar trata esta cuestión en el apartado 12.3. De forma resumida, los controles a tener en cuenta se muestran en la tabla 3-31.

Id. Control	Control
ISO12.3.1	Procedimientos de respaldo, que incluya copias de seguridad de información y software en base a unos criterios mínimos.

Tabla 3-31. Controles ISO/IEC 27002 de gestión de copias de seguridad

Apartado ISO/IEC 8.3. Gestión de medios

Los medios de soporte de la información son importantes ya que normalmente tienen asociados riesgos en cuanto a su uso y distribución. Por ello es necesario establecer controles en cuanto a uso y gestión. En el apartado 8.3 del estándar se puede encontrar información relativa a tal cuestión. En la tabla 3-32 se muestran de forma resumida los controles a tener en cuenta.

Id. Control	Control
ISO8.3.1	Procedimientos para identificar, seleccionar y eliminar de forma segura los medios no necesarios para la organización. Utilización de registros siempre que sea posible.
ISO8.3.2	Procedimientos para manipular, procesar, almacenar y comunicar la información, estableciendo niveles de acceso independientemente del tipo de soporte.
ISO8.3.3	Establecimiento de listas de control por parte de los propietarios de la documentación del sistema.

Tabla 3-32. Controles ISO/IEC 27002 de gestión de medios

Apartado ISO/IEC 13.1. Gestión de la seguridad de la red

Las redes son los medios a través de los que se transmite la información de una organización. Es vital realizar una gestión adecuada de la misma, estableciendo controles en cuanto a su uso controlado y verificado por parte de usuarios autorizados. El estándar trata estas cuestiones en el apartado 13.1. En la tabla 3-33 se muestra un resumen de los posibles controles a implementar.

Id. Control	Control
ISO13.1.1	Procedimientos de gestión y control de la red que aseguren la integridad, confidencialidad y disponibilidad de la información, en línea con los niveles de servicio acordados.
ISO13.1.2	Autenticación de dispositivos conectados a la red.
ISO13.1.3	Monitorización del tráfico de red según niveles de riesgo analizados.

Tabla 3-33. Controles ISO/IEC 27002 de gestión de la seguridad en red

Sección ISO/IEC 9. Control de accesos

Posiblemente, el control de acceso sea el concepto más importante en cuanto a seguridad de la información se refiere, ya que a través de los sistemas de control de acceso se abre o cierra la puerta a los usuarios para que puedan acceder, usar y manipular información de la organización. Este tema se trata ampliamente en la sección 9 del estándar. No obstante, en la tabla 3-34 se muestra un resumen de los controles a tener en cuenta.

Id. Control	Control
ISO9.1	Existencia de una política de control de accesos (físicos y lógicos) implantada, documentada y revisada en línea con los requisitos de negocio.
ISO9.2	Existencia de una política de acceso a la red en línea con la política de accesos, que establezca el uso en base a la autorización asignada a los usuarios. Esta política debe contener procedimientos, mecanismos de autenticación y monitorización.
ISO9.3	Procedimientos para el alta y baja de usuarios con identificadores únicos dentro de la organización.
ISO9.4	Procedimientos y mecanismos centralizados para la gestión de permisos a usuarios y roles, con revisión periódica de derechos por parte de los propietarios de la información. Eliminación de los derechos de acceso cuando se produzcan cambios en la relación con el usuario.
ISO9.5	Procedimientos y mecanismos de asignación de derechos de acceso con privilegios de forma restringida y controlada, así como las herramientas que hagan uso de estos privilegios para su correcto funcionamiento.
ISO9.6	Procedimientos de gestión de la información secreta para la autenticación (i.e. contraseñas), que incluyan firma de documentos de responsabilidad por parte del usuario.
ISO9.7	Obligar al usuario a seguir las prácticas de uso de información secreta para la autenticación: cambio de contraseña, longitud y estructura de contraseñas, no mantener información secreta a la vista, etc.
ISO9.8	Procedimientos y mecanismos seguros de autenticación de usuarios en todos los sistemas que lo requieran, en línea con la política de control de accesos y los niveles de seguridad establecidos.
ISO9.9	Existencia de un sistema de gestión de contraseñas interactivo y que asegura contraseñas de calidad.

Tabla 3-34. Controles ISO/IEC 27002 de control de accesos

Sección ISO/IEC 10. Controles criptográficos

Los controles criptográficos son cada vez más necesarios a la hora de compartir información y documentación, ya que aseguran los cuatro principios de la seguridad de la información: confidencialidad, integridad, disponibilidad y no repudio. El tema se trata en la sección 10 del estándar y se muestra un resumen de los controles en la tabla 3-35.

Id. Control	Control
ISO10.1	Existencia de una política de uso de controles criptográficos, en línea con la dirección y el análisis de riesgos realizado, y que incluya la definición de responsabilidades en cuanto a uso y gestión de claves criptográficas.
ISO10.2	Procedimientos de gestión de claves criptográficas, que incluyan: generación, almacenamiento, distribución, archivado, recuperación y destrucción

Tabla 3-35. Controles ISO/IEC 27002 de controles criptográficos

Fuentes: [21]

3.3 Alineamiento COBIT 5 – ISO/IEC 27002:2013

Tabla de correspondencia de controles

Debido a que las últimas versiones de COBIT e ISO/IEC 27002 son relativamente recientes (2012 y 2013 respectivamente), no existe aún una referencia bien definida en cuanto al alineamiento entre los dos marcos.

No obstante, ISACA ofrece una guía de alineamiento entre COBIT 4.1, ITILv3 e ISO 27002:2005, publicada en 2008 [22].

A través de la guía de alineamiento y con la ayuda de la guía de procesos de COBIT 5 y el estándar ISO/IEC 27002:2013 podemos obtener una correspondencia entre ambos marcos en relación a los controles más importante según la clasificación del punto 2.3.3 ‘Niveles de control’.

Como se puede observar en la tabla 3.37, existen algunos puntos que, o bien COBIT o bien ISO/IEC 27702 no cubren completamente, por lo que se puede afirmar que, aun siendo marcos de referencia bastante completos, el uso combinado de los dos ofrece un acercamiento y tratamiento todavía más integral de la seguridad de la información enmarcada en el gobierno corporativo de la función de TI.

NIVEL	SUBNIVEL	CONTROL GENÉRICO	Localización COBIT 5	Localización ISO/IEC 27002:2013
General	Esencial Legislativo	Derechos de propiedad intelectual	MEA03	18.1
		Protección de registros de la organización	MEA03	18.1
		Protección de datos y privacidad de información personal	MEA03	18.1
	Prácticas Comunes	Conjunto de políticas de seguridad	APO13	5.1
		Organización y asignación de responsabilidades en cuanto a seguridad de la información	APO01/APO13	6.1
		Cultura y capacitación en seguridad	APO13	7.2
		Clasificación de la información	APO01	8.2
		Planificación de la arquitectura empresarial y del SGSI	APO03/APO13	n/a
		Gestión de incidentes y mejoras en seguridad	DSS02	16.1
		Gestión de la continuidad del negocio	DSS04	17.1
		Monitorización	MEA02 / MEA03	12.4
		Auditoría	MEA02	12.7
Técnico	Técnico Común	Gestión de la vulnerabilidad técnica	n/a	12.6
		Protección contra código malicioso	DSS05	12.2
		Gestión de copias de respaldo o back-up	n/a	12.3
		Gestión de medios	DSS05	8.3

		Gestión de seguridad de la red	DSS05	13.1
		Control de acceso a varios niveles: físico, red, sistema operativo, aplicaciones, información	DSS05	9
		Controles criptográficos	DSS05	10

Tabla 3-36: Alineamiento de controles estándar con COBIT 5 e ISO/IEC 27002:2013

Buenas prácticas de control de accesos y gestión de identidades

En cuanto a la seguridad relacionada con el control de accesos lógicos y gestión de identidades, COBIT 5 trata el tema desde una perspectiva de alto nivel en el proceso **DSS05 'Gestionar Servicios de Seguridad'**, más concretamente **DSS05.04 'Gestionar la identidad del usuario y el acceso lógico'** [20], estableciendo los controles vistos en el punto 3.1.3.

Por otra parte, ISO/IEC 27002:2013, trata estos conceptos en el punto **9.4 'Control de acceso a sistemas y aplicaciones'**, más concretamente a través de cinco controles que incluyen guías de implementación precisas:

- 9.4.1. Restricción del acceso a la información.
- 9.4.2. Procedimientos seguros de inicio de sesión.
- 9.4.3. Gestión de contraseñas de usuario.
- 9.4.4. Uso de herramientas de administración de sistemas.
- 9.4.5. Control de acceso al código fuente de los programas.

Un concepto fundamental en seguridad de la información, y en general en el dominio de la informática, es el **principio de menor privilegio** y hay que tenerlo presente a la hora de tratar cualquier punto relacionado con controles de acceso.

Este principio afirma que cualquier objeto del sistema (usuario, administrador, aplicación, servicio) debe tener tan solo los privilegios necesarios para llevar a cabo su tarea y ninguno más.

Podemos identificar los siguientes conceptos claves en cuanto a controles de acceso lógico y gestión de identidades:

- Definición y organización de roles y responsabilidades sobre los diferentes sistemas y la información que manejan.
- Definición y documentación de la arquitectura de la información.
- Cuentas e identificación de usuarios:
    - Revisión periódica de gestión de todas las cuentas y privilegios.
    - Gestionar de forma centralizada las cuentas de usuarios.
    - Asegurar la identificación unívoca de los usuarios y roles en los sistemas, en línea con la definición y organización de los mismos. Esto

permite identificar cualquier actividad en los procesos de monitorización y auditoria.

- Separar y administrar cuentas de usuarios y cuentas con privilegios de forma independiente.
- Obligar al usuario a la elección de contraseñas de calidad.
- Obligar al cambio de contraseña en primera sesión y de forma regular.
- Mantener histórico de contraseñas por usuario y evitar reutilización.
- Almacenar ficheros de contraseñas separados de los sistemas de aplicación.
- Almacenar y transmitir de forma protegida las contraseñas (cifrado). No mostrar contraseñas en claro.

- Autenticación e inicio de sesión:
  - Determinar tipos de verificación: débil / normal / fuerte; y utilizar método de autenticación acorde al tipo de verificación.
  - Usar métodos de autenticación: contraseñas, métodos criptográficos, *smart cards*, *tokens*, métodos biométricos, etc.
  - Autenticar todos los accesos a los sistemas.
  - Minimizar la oportunidad de fracaso en la autenticación.
  - En el proceso de inicio de sesión:
    - No mostrar información del sistemas/aplicación hasta un inicio de sesión correcto y completo, ni ayuda a la autenticación.
    - Proceso completo, esto es, mostrar al usuario sólo si el proceso ha sido satisfactorio o insatisfactorio.
    - Protegido contra ataques de fuerza bruta.
    - Registrar todos los intentos de acceso: satisfactorios e insatisfactorios.
    - Lanzar incidente de seguridad si se detecta brecha de autenticación potencial o verificada.
- Derechos de acceso:
  - Aplicar el principio de menor privilegio en la asignación de permisos a las cuentas de usuario.
  - Tipos de permisos: lectura, escritura, borrado, ejecución.
  - Asociar permisos por aplicaciones, funcionalidades y datos en los sistemas y aplicaciones.

- Administrar y revisar de forma periódica la asignación de permisos a las cuentas.
- Controlar la salida de información de los sistemas y aplicaciones: informes, imprimir, etc.
- Aislar sistemas, aplicaciones y datos sensibles.
- Controlar los permisos para el uso de herramientas de sistemas.
    - Asignación de privilegios al número mínimo de usuarios.
    - Autorización ad-hoc e inicio de sesión obligatorio.
    - Limitación de tiempo en el uso de los privilegios.
    - No disponibilidad de herramientas de sistemas a usuarios de aplicación.
    - Eliminación de herramientas de sistemas innecesarias.

Fuentes: [20], [21]

4 Interoperabilidad y Adopción de Estándares

La necesidad de aprovechar (y reducir) la inversión en infraestructura tecnológica de las empresas implica que los departamentos de sistemas deban conocer dicha infraestructura y mantener y mejorar la interconexión entre sus distintos elementos, tomando especial importancia y preocupación si la infraestructura está formada por plataformas distintas que cubren multitud de servicios de la empresa.

En la actualidad existen multitud de plataformas para según qué fin se quiera dar al uso de las TIC, por lo que se hace realmente crítica la gestión de estos entornos heterogéneos. Además, el grado de penetración de la computación en la nube empieza a ser alto, existiendo una tendencia hacia el uso de servicios prestados por terceros en lugar de implantar infraestructura, lo que añade complejidad a la cuestión.

Pero primero es necesario aclarar la situación que se está tratando. Partimos de una situación inicial donde hay que plantearse qué camino seguir:

a) Aquel en el que se busca homogeneizar los sistemas buscando la máxima integración con los requisitos de negocio dentro de las posibilidades que ofrece ese mundo homogeneizado.

b) Una adecuación de sistemas independientes (en principio) y heterogéneos que satisfacen de forma más precisa y eficaz la consecución de los objetivos de negocio.

Es evidente que en la primera opción no es necesario plantearse la problemática de integrar todos los sistemas, aunque seguramente existan otros problemas asociados.

En el segundo caso los departamentos de administración de sistemas se enfrentan a la elección entre dos opciones para tratar la problemática asociada:

1. Realizar migraciones de los sistemas para lograr un entorno homogéneo

2. Mantener un entorno heterogéneo, buscando soluciones para que la interconexión sea lo más eficaz posible.

Podemos decir que la opción de homogeneizar los entornos es un escenario teórico, siendo muy difícil encontrar en la práctica. Se podría pensar en esta opción sólo en casos donde el entorno implique muy pocos sistemas: catálogo de servicios mínimos; algo que a priori sólo ocurriría en entidades donde no existe una apuesta clara por las tecnologías, o simplemente no merece la pena afrontar esta problemática.

No obstante, la migración de sistemas incluso en entornos tan pequeños puede ser muy costosa para la empresa, un coste que se traduce en tiempo, recursos humanos y búsqueda de conocimientos. Es lógico pensar que lo más sensato es intentar buscar la viabilidad y eficacia de los entornos mixtos.

Por otra parte, en escenarios de grandes organizaciones, encontramos que normalmente se dividen en unidades de negocio independientes, cada una de ellas tomando sus propias decisiones en cuanto a arquitectura empresarial y tecnológica, y por tanto encontrando sistemas heterogéneos que posiblemente sea necesario integrar en algún momento.

Para alcanzar el grado de satisfacción máximo en la utilización de entornos mixtos es necesario tener muy claro un concepto básico y esencial en informática: la interoperabilidad (del inglés *interoperability*). Según los objetivos de este proyecto, es necesario buscar mecanismos que logren la interoperabilidad entre las plataformas Windows y Linux, y más allá, entre los diferentes entornos y servicios ofrecidos por la computación en la nube en caso de optar por este modelo de infraestructura.

En este capítulo se hablará de la interoperabilidad, de cómo lograrla con el uso de estándares, y de los servicios más importantes en la implantación de sistemas con entornos mixtos, así como de protocolos y tecnologías que facilitan la interoperabilidad en entornos Windows/Linux, principalmente en los servicios asociados a la gestión de usuarios e identidades.

4.1 Servicios de empresa

En el ámbito de este proyecto, cuando hablamos de un entorno mixto o heterogéneo nos referimos a un entorno donde los servicios centralizados de una empresa pueden ser ofrecidos tanto por uno como por otro sistema operativo.

Por otra parte, es necesario diferenciar entre servicios internos ofrecidos a usuarios empresariales y servicios ofrecidos a clientes. Según el caso, podría ser una buena práctica separar los dos ambientes para no interferir las operaciones con la actividad de los clientes. En este caso, nos centraremos en los servicios utilizados por los usuarios empresariales. Dentro de estos, los más importantes son de forma general:

a) **Servicios de cuentas de usuario conectados a la red corporativa**: el concepto de dominio, desde el punto de vista de administración de sistemas, se denomina como el conjunto de equipos interconectados que comparten información administrativa centralizada. En un dominio se trabaja con toda la información de usuarios, grupos y contraseñas asociados al mismo. Esta forma de organización es necesaria para poder gestionar de una forma clara y sencilla la conectividad de los usuarios de una entidad. Esta gestión se realiza utilizando una serie de servicios específicos en los sistemas, tanto en Windows como en Linux, utilizando en ambos casos protocolos específicos diseñados para tal fin.
b) **Servicios de gestión de la infraestructura**: dentro de una red corporativa existen protocolos que sirven para mantener la infraestructura que posibilita la conectividad entre los distintos usuarios. Los servicios que ofrecen la utilización de estos protocolos son utilizados por los sistemas centralizados y el usuario suele abstraerse de su uso y existencia.
c) **Servicios de correo electrónico**: toda red corporativa tiene servicios de correo electrónico, siendo el medio de comunicación entre personas más utilizado hoy en día. No obstante, cada vez es más normal externalizar este servicio.
d) **Servicios de archivos e impresión de documentos**: en una red corporativa siempre es necesario que existan servicios que permitan a los usuarios tener acceso a los archivos y documentos que necesiten, así como la posibilidad de imprimirlos, sin que los ficheros se encuentren físicamente en sus puestos de trabajo sino distribuido a lo largo de toda la red. No obstante, la visión de este tipo de servicio ha cambiado con la introducción de modelos de computación en

la nube, siempre que cumpla con los requisitos de seguridad establecidos en la organización.

e) **Servicios de gestión de certificados**: los certificados digitales son equivalentes a las licencias en el mundo real. Son archivos electrónicos que sirven como un pasaporte en línea. A través de los certificados se asegura que existen garantías, ofrecidas por un tercero (autoridad de certificación) de que la identidad del usuario está relacionada con la clave pública utilizada. Debido a que se relacionan los certificados con claves públicas, es necesario llevar una gestión de dichas claves y los certificados asociados, a través de servicios que ofrecen características de Infraestructura de Clave Pública o PKI (del inglés *Public Key Infrastructure*).

f) **Servicios de redes privadas virtuales y acceso remoto**: algo importante cuando se crea y administra una buena red corporativa es dar a los usuarios la posibilidad de tener acceso a recursos de la misma desde puestos que no se encuentran en las instalaciones de la empresa. Para poder ofrecer este servicio es necesario ser muy riguroso con la seguridad, y asegurar que se ofrece de forma exclusiva a los usuarios de la red y nadie externo a la empresa pueda tener acceso a la red corporativa interna.

g) **Servicios de gestión de contenidos multimedia**: actualmente es importante poder ofrecer servicios bajo demanda de contenidos multimedia ya que permiten una mejor conectividad entre usuarios a través de multi-conferencias tanto de audio como video y visualización de seminarios, cursos y otros eventos.

A pesar de que existen estos y otros servicios que son ofrecidos por los sistemas de una organización, se puede asegurar que el más importante es el de **gestión de las cuentas de usuarios y su autenticación en la red**, al ser el punto de partida desde el que se puede acceder al resto de servicios dentro de una red empresarial.

El conjunto de protocolos y estándares existentes para integrar cuentas de usuarios y otros servicios a través de Windows y Linux es: **LDAP + Kerberos + DNS + Samba + NFS + SAML**. Además, si se ofrecen servicios a usuarios externos a la organización es importante el uso de **PKI**.

La **autenticación** es la técnica utilizada para mantener a salvo cualquier recurso en la red: puestos de trabajo, aplicaciones, impresoras y archivos; manteniéndolos a salvo de accesos no permitidos.

En cualquier organización se puede elegir entre varias opciones a la hora de decidir el motor que gestiona la autenticación de los usuarios. Siempre se puede optar por un entorno de red homogéneo con un sistema único y que facilita la administración, o se puede optar por un entorno heterogéneo para poder satisfacer el mayor número de requisitos de negocio a pesar del incremento del grado de complejidad en la tarea de administración y mantenimiento.

Para tener el mayor número de funcionalidades que cumplan con los requisitos de la organización, y a la vez minimizar el coste de administración y mantenimiento de un sistema heterogéneo, la mejor solución suele pasar por integrar el sistema de gestión de cuentas de usuario de todos los sistemas a uno en concreto (que sea un estándar en la industria).

4.2 Interoperabilidad

A pesar de que interoperabilidad no es una palabra reconocida por el diccionario, sí es un término muy utilizado hoy en día en el ámbito de la informática, debido a la variedad de plataformas, aplicaciones y servicios disponibles en el mercado, y a la necesidad de que todos estos elementos consigan trabajar juntos y "hablar" el mismo idioma.

La finalidad principal de un entorno mixto es alcanzar el mayor grado de interoperabilidad posible (también podemos expresarlo como compatibilidad).

Interoperabilidad se puede definir como la capacidad de diferentes productos y servicios de TI para intercambiar y usar datos e información, con el objetivo de funcionar juntos en un entorno conectado en red. La interoperabilidad debe cumplir tres características principales:

1. Viable: a pesar de que siempre hay que buscar la interoperabilidad entre las plataformas, ésta debe implementarse siempre que sea factible y asequible.

2. Segura: hay que buscar siempre una interoperabilidad que garantice los requerimientos de seguridad de la empresa y sus procesos.

3. De fácil mantenimiento: la interoperabilidad es aplicable siempre y cuando se pueda llevar a cabo un mantenimiento eficaz y aceptable, en caso contrario no sería rentable buscar dicha interoperabilidad.

Para alcanzar la interoperabilidad de los sistemas es necesario seguir un camino sólido y que esté disponible para todas las plataformas. El camino adecuado para una buena interoperabilidad es la adopción de estándares en tecnología.

Los estándares consisten en definiciones, formatos o procesos que han sido aprobados por determinadas organizaciones de estandarización o simplemente aceptados por la industria como tales debido a su uso y expansión. Los estándares se pueden clasificar según varias taxonomías: estándares **abiertos y propietarios**; estándares **permisivos y exclusivos**; estándares **según su carácter legal**.

La definición de estándares en tecnología es fundamental ya que sin ellos sería prácticamente imposible que los diferentes sistemas existentes se comunicasen y

pudieran intercambiar la información necesaria para llevar a cabo sus tareas (hablar un mismo lenguaje).

Por otra parte, dependiendo del enfoque y ámbito, el uso de estándares tiene consecuencias, tanto positivas como negativas. Algunas de estas consideraciones son:

1. Generan efectos de red: cuando se genera una primera base de usuarios de un estándar y éste se extiende a otros usuarios de forma exponencial, puede ser contraproducente si en un futuro se realizan cambios en su utilización, debidos por ejemplo a la aparición de otro estándar mejor.
2. Alteran la naturaleza de la competencia: cuando en la industria se sigue un estándar puede provocar limitaciones a las empresas en la investigación y desarrollo de nuevas especificaciones que no se contemplan en el estándar.
3. Reducen la incertidumbre: si se utiliza un estándar, se tiene más certidumbre sobre el uso de lo adquirido en el futuro.
4. Afectan a los costes de cambio: se reducen los costes de adquisición o utilización de tecnologías basadas en un estándar. Además, si el estándar es abierto permite una mayor compatibilidad.

4.2.1 Estándares abiertos

IEEE define interoperabilidad como '*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*" [23].

"La capacidad de dos o más sistemas o componentes de intercambiar información y utilizar la información intercambiada" y lo relaciona directamente con el concepto de compatibilidad".

Según esta definición, la información recogida por el programa ISA (del inglés *Interoperability Solutions for European Public Administrations)* de la Comisión Europea, y algunas ideas revisadas por algunos países, un estándar abierto es aquel que cumple las siguientes características:

- Está publicado y su especificación y documentación completas están disponibles de forma gratuita o al precio de coste de distribución.
- Su propiedad intelectual se ofrece de forma irrevocable libre de regalías, de cualquier otro derecho de explotación de la propiedad intelectual, y no sujeto a

patentes o contratos que restrinjan su uso y reutilización directa o indirectamente.

- Existe al menos una implementación de referencia que desarrolla todas las funcionalidades de la especificación, que está disponible bajo una licencia que permite que sea usada para cualquier propósito, y que puede ser copiada, estudiada, mejorada y distribuida libremente, con o sin cambios.

Los estándares abiertos son los adecuados para permitir la interoperabilidad en un mercado de libre competencia entre múltiples implementaciones de hardware y software. No obstante, la convivencia con los estándares propietarios existe y no debe rechazarse, aunque sí primar la utilización de estándares abiertos sobre propietarios.

Algunos estándares abiertos populares son: HTML, HTTP, TCP/IP, 802.11, XML, SOAP.

Existen diversas entidades en diferentes ámbitos que se ocupan de la definición de estándares. En el caso de la ingeniería, sistemas de información, tecnologías y protocolos, algunas de las más importantes son:

- IEEE (*Institute of Electrical and Electronics Engineers)*
- IETF (*Internet Engineering Task Force*)
- OASIS (*Organization for the Advancement of Structured Information Standards*)
- W3C (*World Wide Web Consortium*)

4.2.2 Estándares propietarios

Los estándares propietarios son especificaciones técnicas desarrolladas y mantenidas por una sola entidad, y que son ofrecidas comercialmente bajo acuerdos de licencias sujetos a Propiedad Intelectual, regulando de esta forma el alcance de uso de los mismos.

A pesar de que los estándares abiertos son los apropiados para conseguir la interoperabilidad entre sistemas, los estándares propietarios son importantes en cuanto a la aportación que realizan en algunas ocasiones a la industria.

Estos estándares son consecuencia directa de las aportaciones en I+D financiadas por compañías que perciben ventajas en sus inversiones, de modo que a pesar de que su objetivo principal es obtener un beneficio propio del desarrollo y

expansión de las mismas, no hay que olvidar que si se consigue un avance tecnológico importante es lógico que al final consigan el reconocimiento de estándar debido a su uso. Y es este reconocimiento, sumado a la utilización de la tecnología lo que facilita y estimula la interoperabilidad.

Además, pueden darse casos en los que un estándar propietario pueda llegar a ser abierto, facilitando aún más la interoperabilidad a través del mismo y su posible evolución, véase el caso de la decisión de Sun Microsystems cuando liberalizó Java, o el formato de documento PDF, desarrollado por la empresa Adobe y lanzado como estándar abierto en 2008.

4.3 Protocolos y estándares en implantación de entornos mixtos

A la hora de crear, administrar y mantener entornos mixtos Windows-Linux existen una serie de protocolos básicos y fundamentales que facilitan la tarea de unificar los servicios.

La mayoría de los estándares que se plantean a partir de este punto sirven como referencia a una organización para satisfacer los requisitos de negocio que se establecen a través de los marcos COBIT e ISO 27002, más concretamente en los controles relacionados con la gestión de identidades y acceso lógico (ver punto 3.3).

Profundizaremos en aquellos protocolos que se utilizan en el proceso de autenticación y control de identidades de los usuarios y su acceso a los recursos de la red, y en consecuencia, los protocolos que permiten el desarrollo e implantación de estos servicios, como LDAP y Kerberos, el protocolo SMB y otros relacionados con la distribución de recursos y ficheros a través de la red como NFS.

4.3.1 LDAP

Protocolo Ligero de Acceso a Directorio, LDAP (del inglés *Lightweight Directory Access Protocol,*) es un protocolo de tipo cliente-servidor, definido en un principio en [24], que permite el acceso por parte de un puesto de cliente a un servicio de directorio estructurado según el estándar X.500, simplificando el modelo DAP (del inglés *Data Access Protocol*) y utilizando básicamente comunicaciones sobre TCP. LDAP se utiliza principalmente como método de **autenticación** y **autorización**, aunque para autenticación se puede complementar con los servicios de Kerberos. La versión actual es LDAPv3 [25].

De forma genérica, se puede definir un directorio como un listado de información sobre objetos distribuidos en algún orden que da detalles sobre cada uno de los objetos.

En términos de informática, un directorio es una base de datos especializada que almacena información relacionada con objetos de forma ordenada y basada en los tipos de estos objetos. A modo de resumen, un directorio, y en concreto un directorio LDAP, tiene las siguientes características principales:

- Permite a usuarios y aplicaciones encontrar recursos con características necesarias para una tarea particular.

- Los directorios tienen un número mucho mayor de accesos que de actualizaciones/modificaciones. Están optimizados para la lectura, no siendo apropiados para almacenar información que cambia rápidamente. Es por esto que son muy rápidos en la lectura de registros.
- La mayoría de implementaciones no soportan transacciones. Aunque LDAP soporta transacciones, están limitadas a transacciones internas.
- Los directorios normalmente implementan su propio protocolo de acceso simplificado y optimizado, en contraposición al uso de SQL en las bases de datos de propósito general.
- Funciona sobre TCP/IP y SSL, lo que facilita que la mayoría de aplicaciones dispongan de soporte para LDAP.
- Permite replicar el servidor de forma sencilla y económica.
- Estructura de directorio LDAP sencilla y jerarquizada, ya que dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.
- Un directorio LDAP se basa en una estructura de árbol llamada DIT (del inglés *Directory Information Tree*) que contiene una colección de entradas.
    - Una entrada es una colección de atributos que tienen un Nombre Distintivo (DN, *Distinguished Name*) que es único y global en todo el árbol del directorio. Cada atributo de una entrada posee un tipo y uno o más valores. Los tipos suelen ser palabras nemotécnicas (del estilo "cn" para *common name* o "*mail*" para la dirección de correo). Los datos se representan mediante pares de atributo y su valor.
    - Los atributos se organizan en clases de objetos. En la clase de objeto se define la colección de atributos que pueden usarse para definir una entrada. Una entrada puede pertenecer a más de una clase de objetos. El estándar LDAP proporciona los siguientes tipos de objetos básicos: **grupos**, **emplazamientos**, **organizaciones** y **personas**.
- Ofrece un formato de fichero utilizado para importar y exportar información de directorio entre servidores de directorios. Estos ficheros LDIF (*LDAP Data Interchange Format*) almacenan la información en jerarquías de entradas orientadas a los objetos definidos. Normalmente está representado en un fichero de texto plano.

Es importante tener en cuenta el control de accesos al servidor LDAP. Aunque el control de accesos no es parte del estándar y se deja libertad a cada implementación de servidor, existen modelos que se usan de forma común.

Fuentes: [24], [25], [26]

4.3.2 Kerberos v.5

Kerberos es un protocolo de tipo cliente-servidor, desarrollado desde la década de 1980 (inicios en 1983) por el Instituto Tecnológico de Massachusetts (MIT Massachusetts Institute of Technology). En 1993 apareció la versión 5 del protocolo, presentada por el MIT y diseñada por John Kohl y Clifford Neuman. Dicha versión se definió en [27], aunque ha quedado obsoleta y sustituida por [28].

Kerberos se utiliza como método de **autenticación** en redes de ordenador abiertas (o desprotegidas). Está basado en parte en el protocolo de autenticación de Needham-Schroeder, el cual establece la necesidad de un tercero de confianza en la comunicación entre dos partes. Se implementa básicamente en los siguientes procesos: login, acceso a otros servidores y acceso a sistemas de ficheros. El funcionamiento de Kerberos y sus principales características son:

- Asume las siguientes condiciones en la red:
    - Se pueden leer, modificar y añadir paquetes de datos a través de la red.
    - No depende de la seguridad de los sistemas de la red, ni en las direcciones de los mismos, ni en la seguridad física de los mismos.
- Utiliza criptografía convencional DES (clave secreta compartida), aunque puede utilizar criptografía de clave pública en situaciones donde sea necesario mediante el uso de extensiones. Se ha definido el uso del protocolo AES para integrarlo con Kerberos 5 (RFC 3962).
- Existe un servidor Kerberos (KDC) que provee tres servicios fundamentales:
    - Servicio de Autenticación (AS, *Authenticated Service*): Autentica inicialmente a los clientes y les proporciona un ticket para comunicarse con el servidor de tickets.
    - Servicio de Tickets (TGS, *Ticket Granting Service*): proporciona a los clientes las credenciales necesarias para comunicarse con un servidor final.

  - Repositorio de clientes y claves privadas: guarda las claves de cada cliente de forma que sólo son conocidas por el servidor y el propio cliente.

- La arquitectura de Kerberos está basada en tres objetos de seguridad:
  - Clave de sesión: es una clave secreta generada por Kerberos y expedida a un cliente para su uso con un servidor durante una sesión. Se utilizan para minimizar el uso de las claves secretas de los diferentes clientes, esto es así ya que la validez de las claves secretas es mucho mayor en el tiempo, por lo que conviene minimizar su uso para prevenir reducir el número de ataques.
  - Ticket: es un testigo expedido a un cliente de Kerberos para solicitar los servicios de un servidor específico. Garantiza que un cliente ha sido autenticado recientemente por lo que lleva una marca de tiempo (timestamp).
  - Autenticador: es un testigo formado por el cliente y enviado a un servidor para probar su identidad y la actualidad de la comunicación. Sólo se utiliza una vez y está cifrado con la clave de sesión, el nombre del cliente y una marca de tiempo (timestamp).
- El funcionamiento básico del protocolo es el siguiente:
  - Un cliente envía una petición al servidor de autenticación (AS) solicitando credenciales para un determinado servidor.
  - El servidor de autenticación responde con las credenciales cifradas en la clave del cliente. Las credenciales se forma con el ticket y la clave de sesión.
  - El cliente transmite el ticket al servidor. El servidor envía al cliente la prueba de actualidad cifrada con la clave secreta de la sesión y es validado para poder utilizar los servicios.
- Aunque Kerberos es un protocolo bastante robusto, es importante tener en cuenta algunos problemas al utilizarlo:
  - Cambios en la implementación de las aplicaciones: cualquier programa que utilice Kerberos debe ser modificado para poder funcionar correctamente, lo que implica cambios en el código fuente de las aplicaciones. Esto genera dos inconvenientes principales: disponibilidad del código fuente e inversión en tiempo para realizar las modificaciones.

- Centralización del sistema: se ha de disponer en todo momento del servidor Kerberos. Además, si el servidor que mantiene la base de datos de claves ve su seguridad comprometida, la red estará amenazada.
- Uso de marcas de tiempo (timestamps): obliga a que todas las máquinas que ejecutan servicios autenticados mantengan sus relojes sincronizados, por lo que se hace necesario el uso de servidores de tiempo.

Actualmente, tanto el servidor de directorio de Microsoft (Active Directory) como OpenLDAP se integran con Kerberos v.5.

Fuentes: [27], [28], [29]

4.3.3 DNS

El Sistema de Nombres de Dominio (DNS, *Domain Name System*) es el servicio de directorio de Internet. DNS es la forma en que los nombres de dominio se traducen a direcciones IP, así como también permite controlar la distribución del correo electrónico.

La especificación base que define DNS se encuentra en las RFCs [30] y [31], no obstante, existen alrededor de 114 RFCs relacionadas con DNS desde sus inicios, muchas de ellas ya obsoletas (alrededor de 20), y otras que actualizan las citadas anteriormente.

De forma resumida, el sistema DNS permite a los ordenadores encontrar sitios web y resolver los destinatarios de los correos electrónicos. Consta de tres componentes principales:

- Espacio de nombres de dominio y registros de recursos: son especificaciones para un espacio de nombres estructurado en forma de árbol y la información asociada con los nombres. Cada nodo y hoja del árbol del espacio de nombres de dominio identifica (etiqueta) un conjunto de información, y las consultas de las operaciones intentan extraer tipos específicos de información de cada conjunto.
- Servidores de nombre: son servidores que guardan información sobre la estructura del árbol de dominios y sus grupos de información relacionada. Normalmente un servidor de nombres guarda información completa sobre un subconjunto de espacio de nombres.

- Sistema de resolución: son programas que extraen información de los servidores de nombres en respuesta a peticiones de clientes.

Estos componentes corresponden a las tres capas de los sistemas de dominio:

- Capa de usuario: se accede al sistema de dominios mediante una llamada (a nivel de sistema operativo) al sistema de resolución local. El espacio de dominios consiste en un árbol sencillo donde el usuario puede solicitar información de cualquier sección del árbol.
- Capa de sistema de resolución: el sistema de dominios se compone de un número desconocido de servidores de nombres. Cada servidor de nombres tiene un subconjunto de toda la información del árbol de dominios, tratándola de forma estática.
- Capa de servidor de nombres: el sistema de dominios consiste en conjuntos separados de información local, llamadas zonas. Cada servidor de nombres tiene una copia local de alguna de las zonas. El servidor de nombres debe refrescar periódicamente sus zonas desde una copia maestra o desde servidores de nombres ajenos a él. Además, el servidor de nombres procesa de forma concurrente las peticiones que le llegan desde sistemas de resolución.

El flujo normal de DNS es el siguiente:

1. Existen miles de millones de registros de recursos que son separados en millones de archivos llamados Zonas.
2. Las zonas se mantienen en servidores autorizados que se distribuyen a lo largo de todo Internet. Los servidores autorizados responden a las consultas basadas en los registros de recursos almacenados en las zonas de los que ellos mismos tienen copias.
3. Los servidores de almacenamiento intermedio (*caching servers*) consultan a otros servidores sobre la información y la guardan para posibles peticiones repetidas.
4. La mayoría de los servidores de nombres están autorizados para algunas zonas y desarrollan funciones de almacenamiento intermedio para la demás información DNS.

Fuentes: [30], [31]

4.3.4 SMB/CIFS

SMB (*Server Message Block*) es un protocolo de red dentro de la capa de aplicación que permite compartir archivos e impresoras. Puede implementarse sobre diversos protocolos como TCIP/IP, NetBEUI o IPX/SPX. Tanto en el caso de Samba como de Windows se implementa habitualmente sobre NetBIOS sobre TCP/IP.

SMB fue desarrollado inicialmente por IBM a principios de los años 80. Microsoft, entre otros, ha ido ampliando su funcionalidad hasta el punto de rebautizar el protocolo en 1998 como CIFS (*Common Internet File System*), que incluye soporte para enlaces simbólicos, enlaces duros y mayores tamaños de archivo. Debido a otras evoluciones también se habla de SMB en los siguientes protocolos: Core Protocol, DOS Lan Manager, LAN Manager, NTLM, y por último **Samba**, que es una implementación libre del protocolo con las extensiones de Microsoft incluidas.

SMB es un protocolo de tipo cliente/servidor, donde el servidor ofrece recursos que pueden ser utilizados de forma remota por los clientes. Los recursos son procesados y devueltos al cliente tras una petición al servidor. Trabajar con redes SMB es diferente a trabajar con redes TCP/IP de Unix. Podemos tratar tres temas principales:

- Conceptos básicos de una red SMB
- Implementaciones de Microsoft
- Servicios principales de Samba

El eje central sobre el que se mueve Samba es NetBIOS (*Network Basic Input/Output System*). NetBIOS es una API creada por IBM en 1984 cuya utilidad es conectar por red las computadoras. Proporcionaba un diseño rudimentario para que una aplicación se conectara y compartiera información con otras computadoras. Se puede pensar en NetBIOS API como extensiones a las llamadas estándar de BIOS API.

Con el paso de los años, NetBIOS se tuvo que adaptar a los tipos de redes utilizadas, terminando por implementar la API sobre TCP/IP y UDP/IP que llegaron a ser los tipos de redes más extendidas.

Debido a que NetBIOS utiliza nombres y TCP/IP utiliza direcciones (192.168.1.1) surgió un problema al unir ambos protocolos, que se resolvió en 1987 cuando el IETF publicó la serie de estándares 1001/1002 (hoy en día todavía en uso).

Este estándar, conocido como NetBIOS sobre TCP/IP o NBT describe una serie de servicios en una red:

- Servicio de nombres: permite resolver nombres a direcciones (al estilo DNS en Internet)
- Dos servicios de comunicaciones. Protocolos de comunicación secundarios :
    a) Datagramas (datagrams)
    b) Sesiones (sessions)

Conceptos básicos de una red SMB

Los conceptos elementales que se manejan al hablar de una red que utiliza SMB son:

- Registro de nombres en redes NetBIOS:
    - Con servidor de nombres NetBIOS (NBNS): la gestión de los nombres es centralizada.
    - Sin servidor de nombres NetBIOS: cada máquina envía (*broadcast*) la petición de nombre en espera de si alguna máquina deniega al existir ya dicho nombre. En el registro de nombre se producen dos acciones principales: registro y resolución.
- Existen cuatro estrategias que definen el tipo de nodo dentro de una red NetBIOS:
    a) b-node: sólo broadcast para registro y resolución
    b) p-node: sólo point-to-point para registro y resolución
    c) m-node: broadcast para registro. Si es satisfactorio notifica al NBNS el resultado. Broadcast para resolución. Utiliza el NBNS si el broadcast no es satisfactorio
    d) h-node (hybrid): utiliza NBNS para registro y resolución. Utiliza broadcast si el NBNS no responde o está inoperativo. Este tipo fue desarrollado por Microsoft y no está incluido en la RFC 1001/1002
- Estructura de nombre NetBIOS:
    - Existe un nombre único para representar una máquina con NetBIOS (no existen nombres cualificados y/o segmentados como en DNS.
    - Un nombre NetBIOS sólo puede tener 15 caracteres: (a-z, A-Z, 0-9) y los caracteres especiales más comunes.

  - Normalmente el nombre DNS para un servidor Samba se utiliza como nombre NetBIOS. Por ejemplo, en berlioz.uc3m.es se utiliza BERLIOZ como nombre NetBIOS.
  - La estructura de un nombre NetBIOS se representa con 16 bytes: 15 para el nombre y el último para definir el tipo de recurso que es.
- En SMB, Las máquinas o recursos pertenecen a grupos. En el mundo Windows, un Grupo de Trabajo y un grupo SMB son lo mismo.
- Aunque el modelo SMB define los dos primeros niveles de seguridad, en la actualidad Samba ofrece hasta cuatro (incluidos los dos básicos):
  a) Nivel compartido (share)
  b) Nivel usuario (user)
  c) Nivel de servidor
  d) Nivel de dominio

Fuentes: [32]

Implementaciones de Microsoft

Un concepto importante antes de hablar de las implementaciones de Microsoft es la navegación para acceder a los sistemas. La navegación concebida en sistemas Windows permite examinar el contenido de una red utilizando una interfaz gráfica (GUI), de forma que no es necesario conocer el nombre del equipo o recurso compartido a utilizar. La búsqueda o navegación en una red SMB puede ser de dos tipos:

a) Búsqueda en una lista de equipos y recursos compartidos
b) Búsqueda del recurso compartido de un equipo específico

Microsoft introdujo una serie de mejoras en las redes SMB para su integración con Windows, a las que llamó Windows para Grupos de Trabajo y Dominios de Windows.

- Los **Grupos de Trabajo** de Windows se asemejan a los grupos en el protocolo SMB, añadiendo algunas características como la navegación. Básicamente, un grupo de trabajo es una colección de ordenadores donde cada uno mantiene su propia información de seguridad. De esta forma, cada servidor (equipo) se encuentra con un nivel de seguridad compartido. Se puede decir que la seguridad está distribuida y no centralizada.

- Un **Dominio** es un conjunto de equipos que comparten una base de datos de directorio común. Este directorio común permite que la seguridad esté centralizada. Cada dominio tiene uno o más controladores de dominio, siendo habitual la existencia de un controlador de dominio principal y algunos controladores de dominio de respaldo. Los controladores de dominio mantienen la información relativa a las cuentas de usuario: nombre de cuentas, contraseñas cifradas, horas de uso permitidas, grupos a los que pertenece el usuario, etc.

  Por su propia naturaleza un dominio suele ser más seguro que un grupo de trabajo debido a que las contraseñas están cifradas y son monitorizadas por el servidor de dominio.

  Aunque se detallarán más adelante cuando se hable de Active Directory, el uso de dominios permite conseguir los siguientes objetivos:

- Delimitar la seguridad
- Replicar información
- Aplicar políticas (o directivas) de grupo
- Delegar permisos administrativos

En los últimos años, Microsoft ha trabajado en la mejora del protocolo, introduciendo en 2006 SMB2 como mejora del protocolo original, y SMB3 a partir de las últimas versiones de Windows 8 y Windows Server 2012.

Se puede encontrar más información actualizada sobre los protocolos SMB y CIFS en [33], [34].

Servicios principales de Samba

Como se ha comentado, Samba es una implementación libre del protocolo SMB con las extensiones de Microsoft incluidas. Con el paso del tiempo, se ha convertido en un paquete completo de funcionalidades y servicios para dar capacidades de integración completas entre sistemas Windows y Linux, especialmente en el mundo de la centralización y gestión de cuentas de usuario, autentificación y recursos compartidos.

La última versión de Samba (mayor) es la 4.1, publicada en octubre de 2013. Podemos decir que los servicios más importantes que ofrece Samba son los siguientes (tanto a nivel de servidores como para máquinas clientes):

- Servidor de ficheros
- Servidor de impresión
- Servidor de Microsoft DFS
- Controlador de Dominio Principal (PDC)
- Controlador de Dominio de Respaldo (BDC)
- Controlador de Dominio de Active Directory
- Autenticación Windows NT/2000/XP/Vista/7/8
- Buscador Local Maestro
- Buscador Local de Respaldo
- Buscador de Dominio Maestro
- Servidor WINS principal
- Servidor WINS secundarios
- Winbind

Fuentes: [32]

4.3.5 NFS

NFS *(Network File System)* es un servicio de red que permite a un ordenador cliente montar y acceder a un sistema de archivos remoto, exportado por un sistema servidor.

NFS es un protocolo diseñado y desarrollado por Sun Microsystems en 1984 orientado principalmente a sistemas UNIX y surgido de la necesidad de estos sistemas de montar sistemas de ficheros en el propio núcleo para poder acceder a ellos. No obstante, se puede utilizar un sistema Windows como cliente y servidor NFS mediante el uso de los Servicios de Windows para Unix (SFU, *Windows Services for Unix*).

La versión más actual del protocolo es la 4, definida en [35]. La RFC es una revisión de las anteriores versiones: NFS v2 (RFC 1094) y NFS v3 (RFC 1813). Las características principales de NFS son:

- Está dividido en dos partes: un servidor y uno o más clientes. Los clientes acceden de forma remota a los datos que hay almacenados en el servidor.
- Centralización de los datos en el servidor, lo que permite que los puestos de trabajo utilicen menos espacio de disco local. Además, la centralización de los datos permite que no sea necesario replicar la información para varios usuarios.

- Se elimina la necesidad de un directorio "*home*" en cada máquina de la organización para cada usuario.
- Se pueden compartir otros dispositivos de almacenamiento como unidades DVD, entre otros. También es útil para ubicar software en un solo sitio de la red y compartirlo.
- Todas las operaciones sobre ficheros son síncronas, lo que garantiza la integridad de los ficheros.
- Un servidor NFS puede exportar más de un directorio y atender simultáneamente varios clientes
- Un cliente NFS puede montar directorios remotos exportados por diferentes servidores.
- Cualquier sistema UNIX puede ser a la vez cliente y servidor NFS

El funcionamiento básico de NFS está basado en la API RPC (*Remote Procedure Call*) ya que permite realizar llamada a procedimientos que se ejecutan en otra máquina, para lo que el cliente envía un mensaje de petición al servidor con los parámetros de la llamada y espera una respuesta con los resultados.

Es muy importante tener en cuenta la seguridad en un servidor NFS ya que al configurar una máquina como tal se está compartiendo un sistema de ficheros con diferentes máquinas clientes. Para mejorar el sistema de seguridad en NFS, a partir de la versión 4 se utilizan diferentes módulos que se integran con KerberosV5 lo que permite tener mecanismos orientados a la autenticación de usuarios individuales y no a máquinas clientes, como lo hacía las versiones anteriores (NFSv2 y NFSv3).

Fuentes: [35], [36]

4.3.6 SAML

SAML (*Security Assertion Markup Language*) es un estándar abierto definido por el Comité Técnico de Servicios de Seguridad de OASIS y liberado en 2005. SAML define un esquema XML para el intercambio de información de autenticación y autorización. Es un protocolo flexible y extensible, actualmente se ha convertido en el estándar de referencia al hablar de gestión de identidades federadas.

La primera versión de SAML 1.0 apareció en 2002. Durante unos años, el trabajo de OASIS se realizó en paralelo con otras iniciativas como *Shibboleth* y el *Identity*

Federation Framework (ID-FF) de la *Liberty Alliance*, lo que dio lugar a una convergencia en SAML 2.0 en 2005.

SAML surge para dar respuesta al uso creciente de la web, y el uso de servicios a través de diferentes aplicaciones basadas en web. Al encontrar escenarios cada vez más heterogéneos, se hacía necesario proporcionar un mecanismo que permitiera estandarizar el intercambio de información de seguridad

SAML está relacionado directamente con los conceptos de *Single Sign-On e Identity Federation*. El principal objetivo de SAML es conseguir el intercambio de credenciales entre diferentes entidades, típicamente, proveedores de servicios y proveedores de identidades y autorizaciones.

De forma resumida, SAML se construye sobre cuatro conceptos:

- Aserciones: representan las características o atributos de las entidades: información de autenticación, atributos detallados del usuario, permisos asociados al usuario.
- Protocolos: definen la forma de las peticiones y respuestas de la información mediante protocolos basados en esquemas XML.
- Mapeos: para determinar la forma de traducir la información a los siguientes niveles de transporte: SOAP, HTTP, etc.
- Perfiles: tipos de combinaciones entre los elementos anteriores según el escenario de uso.

Fuentes: [37]

4.3.7 Otros protocolos y tecnologías

Los protocolos hasta ahora expuestos son los más importantes a la hora de integrar sistemas en entornos heterogéneos, principalmente en tareas de gestión de la autenticación y centralización de cuentas de usuario. No obstante, existen muchos protocolos orientados a establecer comunicaciones a través de la red más seguras. Algunos de estos protocolos más importantes se exponen a continuación.

IPSec

IPSec (*Internet Protocol Security*): es un conjunto de protocolos del nivel de red pensados para asegurar las comunicaciones, autenticando y cifrando cada paquete IP en un flujo de datos a través de la red. Está basado en un modelo de seguridad extremo a

extremo, esto quiere decir que sólo los equipos que envían y reciben los paquetes son los únicos que tienen que conocer la protección. Cada equipo controla la seguridad en su extremo, suponiendo que el medio de comunicación no es seguro.

Existen muchas RFCs relacionadas con IPSec pero las más elementales son [38], [39] y [40].

IPSec consta de dos protocolos principales: *Authentication Header* (AH) y *Encapsulating Security Payload* (ESP). El primero proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados. El segundo proporciona confidencialidad, autenticación y protección de integridad. Algunos algoritmos criptográficos para usar con IPSec son: HMAC, SHA-1, Triple DES-CBC y AES-CBC.

No se recomienda el uso de IPSec para servidores miembros de un dominio así como tampoco para controlar todo el flujo de una red local. Se recomienda el uso de IPSec en las siguientes situaciones:

- Servidores de seguridad con acceso a Internet.
- Segmentos o subredes que requieran un grado extra de seguridad en sus comunicaciones
- Servidores y sistemas con información sensible y altamente protegida, por ejemplo en la comunicación entre algunos servidores web y bases de datos.
- Uso de túneles L2TP/IPSec, tanto para conexiones VPN (*Virtual Private Networks*) como otro tipo de interoperabilidad. Este es uno de los usos más habituales de IPSec.

Fuentes: [38], [39] y [40]

TLS/SSL

TLS (*Transport Layer Security*) es un protocolo del nivel de transporte que se utiliza para cifrar los segmentos de red en la comunicación entre dos aplicaciones. Está basado en el protocolo SSL (*Secure Socket Layer*). Proporciona autenticación y privacidad entre extremos sobre Internet mediante el uso de criptografía. El uso de TLS/SSL implica el despliegue de una infraestructura de claves públicas (PKI) para los clientes. El uso del protocolo previene de ataques por escucha (*eavesdropping*) y

falsificación de identidad del remitente (*phishing*). La última especificación de TLS (1.2) se encuentra en [41].

En cuanto a las fases en que se divide la comunicación con TLS/SSL son básicamente tres:

- Negociar entre las partes el algoritmo que se utilizará para la comunicación.
- Intercambiar las claves públicas y realizar la autenticación basándose en certificados digitales. Los protocolos utilizados para la criptografía de clave pública son: RSA, Diffie-Hellman, DSA o Fortezza.
- Cifrar el tráfico basándose en cifrado simétrico. Los protocolos que se pueden utilizar para el cifrado son: RC2, RC4, IDEA, DES, Triple DES o AES.

Fuentes: [41]

PKI

Algo muy importante en seguridad es el concepto de Infraestructura de Clave Pública (PKI, *Public Key Infrastructure*). Una infraestructura PKI es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.

Un usuario o entidad posee un par de claves (pública y privada) y un certificado asociado a su clave pública. De esta forma, los usuarios se pueden autenticar frente a otros usuarios usando la información de los certificados para cifrar y descifrar mensajes, firmar digitalmente información, etc.

El uso de tecnología PKI se da principalmente en los siguientes escenarios:

- Autenticación de usuarios y sistemas.
- Identificación de interlocutores.
- Cifrado de datos digitales.
- Firma digital de datos como documentos, software y otros.
- Asegurar las comunicaciones (como ya se ha expuesto en el uso del protocolo TLS/SSL).
- Garantizar el no repudio (rechazar una transacción que tuvo lugar).

En una infraestructura PKI es muy importante el uso y la gestión de certificados. Existen diferentes tipos de certificados en función de la información que contienen:

personales, de empresa, de representante, de persona jurídica, etc. Debe existir un sistema capaz de verificar la validez y dar legitimidad a la relación de una clave pública con la identidad de un usuario o servicio, que conceptualmente se denomina como tercero de confianza. Los principales componentes que actúan como terceras partes son: autoridad de certificación, autoridad de registro y otras terceras partes como autoridades de sellado de tiempo.

Algunos de los servicios ofrecidos por una infraestructura PKI son los siguientes:

- Registro de claves: emisión de certificados para una clave pública.
- Revocación de certificados: cancelación de un certificado previamente emitido.
- Selección de claves: publicación de la clave pública de los usuarios.
- Evaluación de la confianza: determinación sobre si un certificado es válido y qué operaciones están permitidas para dicho certificado.
- Recuperación de claves: posibilidad de recuperar las claves de un usuario.

Debido al uso de certificados es importante tener en cuenta el uso de certificados X.509, el cual es un protocolo estándar para infraestructuras PKI que especifica, entre otras cosas, el formato estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. El protocolo X.509 está definido en la RFC 5280.

OpenID

OpenID es un estándar abierto de identificación digital distribuido y descentralizado. El objetivo de OpenID es permitir al usuario autenticarse en diferentes páginas y aplicaciones web sin necesidad de mantener un identificador diferente para cada una de ellas. Para ello es necesario que el servicio ofrezca soporte para el protocolo.

OpenID nació en 2005, desarrollado por Brad Fitzpatrick. En 2006 se publicó la versión 2.0 y en 2007 se creó la OpenID Foundation.

OpenID deja del lado del proveedor del servicio la implementación del mecanismo de autenticación. Está orientado a la web y se está convirtiendo en el estándar para la identificación unificada de los usuarios en los diferentes servicios que existen en Internet. OpenID está basado en estándares y tecnología web como DNS, HTTP, SSL, Diffie-Hellman, etc.

Algunas compañías que soportan OpenID son: Google, Microsoft, Yahoo, VeriSign, WordPress, que además realizan la función de proveedor de identidades.

A pesar de que facilita la gestión de identidades al usuario, conlleva ciertos riesgos, ya que si la cuenta del proveedor de identidad se ve comprometida, el usuario puede ver comprometida toda su identidad digital en todos los servicios que pueda utilizar.

En otras alternativas a tener en cuenta, encontramos OpenID Connect que unifica el uso de OpenID con OAuth como marco de autorización.

Fuentes: [42], [43]

OAuth

OAuth (*Open Authorization*) es un protocolo abierto que permite autorización segura a través de un método simple y estándar para entornos y aplicaciones web, móviles y de escritorio. La última especificación es OAuth 2.0, y su definición se encuentra en las RFCs [44], [45] y [46].

OAuth comenzó a implementarse en 2006 después de que varios desarrolladores intentaban implementar OpenID, principalmente para Twitter. Después del interés mostrado por varias compañías, en octubre de 2007 se publicó la primera versión del protocolo. En 2008 fue adoptado por el IETF, y en 2010 fue publicada la primera RFC (5849). Ya en 2012 se publicó la versión OAuth 2.0 que es la última versión, y que más que un protocolo establece un marco abierto de autorización descentralizado.

Al igual que OpenID, el protocolo se basa en el concepto de redireccionamiento, existiendo proveedores de permisos asociados a un usuario y proveedores de servicios que necesitan acceder a dichos permisos para verificar si un usuario tiene accesos a funcionalidades, contenidos, etc.

Algunas compañías que utilizan e implementan OAuth son: Amazon, Facebook, Google, Microsoft y Yahoo.

Fuentes: [44], [45], [46], [47]

5 Entornos Mixtos

5.1 Control de accesos. Gestión de identidades

La Gestión de Identidades y Control de Accesos (IAM, *Identity and Access Management*) se puede definir como "conjunto de procesos de negocio, tecnologías, infraestructura y políticas que permite realizar la gestión de las identidades de usuario y controlar el acceso de éstas a los diferentes recursos organizacionales" [48].

El control de accesos y la gestión de identidades son elementos críticos en cualquier negocio y organización. Es la llave que permite abrir las puertas a la información que se maneja en una entidad. Toda acción de gestión, operación y mantenimiento debe pasar por este proceso si se quiere cumplir con los estándares en seguridad.

Encontramos otros términos como IdM (*Identification Management*) e IAG (*Identification and Access Governance*), que podemos tratar como sinónimos, aunque existe cierto debate respecto a algunos matices que los pueden diferenciar. Otro concepto que se encuentra en la literatura es el de Sistema de Gestión de la Identidad (*Identity Management System)*, que podríamos definir como el sistema o tecnología específica utilizada para la gestión de identidades y accesos.

Dentro del conjunto de elementos que forman IAM, es importante manejar los siguientes conceptos:

- Identidad: objeto que contiene atributos que identifican a un usuario.
- Autenticación: proceso de verificación de que una identidad es auténtica.
- Autorización: proceso de comprobación de los derechos de acceso a recursos y funcionalidades asociados a una identidad.
- Roles: conjunto de funciones que se asignan a una identidad.
- Privilegios: derechos que tiene una identidad sobre los recursos y funcionalidades.

Por otra parte, es importante conocer los modelos formales de control de acceso más habituales [49], [50]. De forma resumida:

a) Control de Acceso Discrecional (DAC, *Discretionary Access Control*): el acceso a los objetos está gestionado por su propietario y los grupos a los que pertenece. El propietario puede transmitir sus permisos a otro sujeto. Es el tipo de control típico de un sistema de ficheros UNIX. Es un método descentralizado.

b) Control de Acceso Mandatorio (MAC, *Mandatory Access Control*): está basado en políticas. Se establecen reglas de acceso (basada en niveles) para establecer relaciones entre las acciones sobre los objetos y usuarios. Es el sistema (y responsable del sistema) y no el propietario quien gestiona los permisos sobre los objetos. El origen de este tipo de control es militar, y lo podemos encontrar en tecnologías como AppArmor y SELinux. Es un método centralizado.
c) Control de Acceso Basado en Roles (RBAC, *Role Based Access Control*): basado en funciones. Los derechos se asignan a las funciones o roles que existen en el sistema, normalmente de forma estructurada. El usuario sólo puede acceder a un objeto si tiene asignado un rol que tiene asociados permisos para el objeto. Es un modelo centralizado, y el más popular en la actualidad.
d) Modelo de "Originador" Controlador (ORCON, *Dissemination and Extraction of Information Controlled by Originator*): pensado para el control de la distribución de documentos confidenciales (y otro material). Está basado en el concepto de consentimiento para copias o divulgación de la información. Un sujeto de una organización que recibe una copia de un objeto (o derecho sobre él) no puede distribuir la información a otra organización sin el consentimiento de la primera. Los sistemas DRM se basan en los conceptos de ORCON, aunque es difícil implementar tecnológicamente ya que se basa en la información contenida en los documentos o materiales y no en las entidades u objetos.
e) Control de Acceso Basado en Atributos (ABAC, *Attribute Based Access Control*): modelo reciente en el que el control de acceso evalúa en base a los atributos de las entidades: sujeto y objeto. Este modelo ha surgido gracias a la aplicación del lenguaje XML al dominio del control de acceso, generando lenguajes como XACML (*eXtensible Access Control Markup Language*).

Aunque no es objetivo del proyecto tratarlos, no podemos olvidar los modelos clásicos de control de accesos que han servido como base: modelo Bell-La Padula, modelo Biba, modelo Clark-Wilson, modelo de la Muralla China.

Como es lógico, ha existido una evolución en cuanto al tratamiento del problema de gestión de identidades y control de accesos. La identidad y sus privilegios siempre van asociados a un entorno concreto, ya sea nuestra identidad como personas en nuestro entorno: empresa, ciudad, país, continente; como nuestra identidad en el mundo virtual: aplicaciones, computadoras, empresas, redes sociales, Internet, etc.

En el ámbito de la informática, todo empezó por la necesidad de identificarnos en las computadoras y las redes de las empresas. A continuación, en las diferentes aplicaciones que se utilizaban en los ordenadores y servidores de una red. Después, el problema se trasladó a la web cuando se hizo necesaria la identificación en las nuevas aplicaciones basadas en web y los diferentes servicios que ofrecían al usuario. Por último, llegaron las redes sociales, y actualmente, con tal diversidad y complejidad, uno de los objetivos es definir un marco donde cada persona posea y gestione una única identidad digital que pueda utilizar en cualquier sitio de Internet.

El reto a cualquier nivel (red, empresa o Internet) es tratar de unificar los diferentes perfiles o identidades que pueda tener una persona, usuario o recurso, y que mediante un único proceso de autenticación se pueda acceder a cualquier servicio al que se tengan derechos de acceso sin necesidad de repetir el proceso de autenticación. Esta tarea, cuando hablamos de Internet, es complicada (aunque se está avanzando en este sentido), sin embargo, a nivel de empresa existen soluciones planteadas como IAM, donde a través de la centralización de estos procesos y servicios podemos alcanzar el objetivo.

De la necesidad anterior surge el concepto de Sistema Centralizado de Autenticación y Autorización (*Single Sign-on*), en adelante SSO, que habilita al usuario para autenticarse una única vez y tener acceso a diferentes servicios asociados al proveedor de identidad. Las ventajas de utilizar SSO son:

- Reduce los costes operacionales
- Reduce el tiempo de acceso a la información
- Mejora la experiencia del usuario
- Introduce un sistema de seguridad avanzada en los sistemas
- Alivia la carga sobre los desarrolladores
- Permite una gestión centralizada de usuarios y roles
- Permite auditorías detalladas
- Asegura el cumplimiento con las normativas

Algunas de las tecnologías más populares para implementar sistemas *Single Sign-On* está descritas en el punto 4.3: LDAP, Kerberos, Active Directory.

Dependiendo del escenario, de las necesidades a cubrir y de la arquitectura empresarial definida, podemos elegir el tipo de SSO, de entre varios:

- Enterprise SSO (E-SSO), también llamado Legacy SSO
- SSO por sesión
- Web SSO o Web Access Management (WAM)
- SSO de varios dominios
- SSO federado

En el punto 5.4 se verá el escenario objetivo del proyecto de entre varios posibles, pero es importante hacer hincapié en que, aunque la infraestructura tecnológica debe tender al uso de sistemas SSO en cuanto a control de accesos se refiere, el elemento central de cualquier AIM es el sistema de control y gestión de identidades. Y entre los sistemas de gestión de identidades encontramos por una parte a **Microsoft Active Directory** como actor destacado, y por otra parte a **OpenLDAP** y **Samba** como sus alternativas libres. Otros productos también relacionados que podemos encontrar en el mercado son: NetIQ eDirectory, IBM Tivoli Identity Manager y Oracle Identity Management, entre otros.

Centrándonos en la autenticación y control de accesos de ambos sistemas, antes de Windows 2000, los controladores de dominios Windows NT proporcionaban servicios de autenticación a los clientes utilizando el protocolo NTLM (NT LAN Manager). No obstante, aunque el protocolo ayudaba a resolver el problema de mantener cuentas duplicadas en varios servidores a través de la red, no era tan seguro como se pensó en sus orígenes. Es por esto que, a partir de Windows 2000, Microsoft cambió de NTLM a Active Directory con los servicios de autenticación de Kerberos integrados. Al utilizar Kerberos se conseguía un entorno más seguro y escalable, además de utilizar un estándar utilizado también en sistemas Linux y UNIX.

Por otra parte, los sistemas Windows conceden o deniegan el acceso a los recursos basándose en listas de control de acceso (ACLs, *Acess Control Lists*) las cuales utilizan los SIDs (*Security Identifier*) para identificar a los usuarios y grupos miembros de las listas. El SID es un nombre único, una cadena de caracteres alfanuméricos, que asigna una autoridad de seguridad (como un controlador de dominio) durante el proceso de acceso al sistema (*login*), y que se utiliza para identificar el objeto, ya sea un usuario o grupo de usuarios.

En cuanto a Linux, en sus orígenes no se implementó para tener un mecanismo de autenticación para las aplicaciones único. Normalmente, los desarrolladores tenían que

implementar su propio esquema de autenticación utilizando básicamente el fichero de nombres y contraseñas /etc/passwd. Pero en 1995 Sun Microsystems propuso un mecanismo llamado PAM (*Pluggable Authentication Modules*), cuyo propósito era separar la implementación de la gestión de privilegios de los programas, basándose en esquemas de autenticación apropiados y seguros. De esta forma, PAM proporciona un conjunto de librerías de funciones que cualquier aplicación puede utilizar para gestionar su propia autenticación en el sistema.

Sun Microsystems también desarrolló el sistema NSS (*Name Service Switch*) para la resolución de nombres: usuarios, máquinas, etc. NSS junto a PAM forman el sistema básico de autenticación en los sistemas Linux modernos.

Por otra parte, en Linux, a diferencia de Windows, no se utiliza la propiedad SID en los recursos, sino que los usuarios llevan asociado un UID (*User Identifier*), que es un número entero de 32 bits, y cuyo valor está limitado a la propia máquina. Los grupos se identifican por un GID (*Group Identifier*) que sigue el mismo patrón que el UID.

Uno de los principales problemas de la integración de entornos Windows-Linux es la correspondencia de identificadores (SID – UID/GID) entre los diferentes sistemas, para lo cual podemos utilizar Samba, que a través de su módulo Winbind, facilita la resolución de problemas de correspondencia de los identificadores.

5.2 Microsoft Active Directory

5.2.1 Conceptos básicos

El mundo alrededor de Active Directory es muy amplio, y en las organizaciones es normal encontrar equipos del departamento de TI dedicados exclusivamente a ello (dependiendo del tamaño de la organización). A continuación ofrecemos una breve introducción a algunos conceptos básicos a tener en cuenta sobre Active Directory. Existe mucha literatura al respecto de esta tecnología como [51], [52] y [53].

Windows Server 2012 Active Directory puede adquirir cinco roles principales (entre paréntesis el acrónimo utilizado según sus siglas en inglés):

- Servicios de **dominio** de Active Directory (AD DS)
- Servicios de **directorio ligero** de Active Directory (AD LDS)
- Servicios de **certificados** de Active Directory (AD CS)
- Servicios de **administración de derechos** de Active Directory (AD RMS)
- Servicios de **federación** de Active Directory (AD FS)

Al implantar un sistema Windows Server 2012 con el rol de dominio de Active Directory (AD DS) se convierte a dicho sistema en Controlador de Dominio (DC, *Domain Controller*).

La información que reciben los clientes de Active Directory es aquella relacionada con cuentas de usuario, grupos y equipos, así como también los perfiles de usuario y equipo, directivas de seguridad y servicios de red. Esto convierte a Active Directory en una herramienta fundamental en la administración de toda la organización, en línea con los objetivos de centralización de la gestión de identidades.

Además, Active Directory separa la estructura lógica de la organización (dominios) de la estructura física (topología de red), lo que implica mayor independencia para la administración de ambos entornos.

De entre todos los estándares con los que Active Directory ofrece compatibilidad: DHCP, DNS, SNTP, LDAP, Kerberos V5, Certificados X.509; es imprescindible conocer los detalles de la relación entre DNS y el Active Directory, ya que el grado de dependencia de este con DNS es muy grande. En versiones anteriores, la funcionalidad que ofrece DNS también era implementada por servidores WINS, aunque ya no se

recomienda su uso debido a la poca aceptación por parte de la industria y que no es un estándar, y se empieza a dejar como uso residual y por motivos compatibilidad.

Básicamente, Windows Server 2012 utiliza DNS para localizar equipos y controladores de dominio. Una estación de trabajo o servidor miembro busca un controlador de dominio preguntando a DNS. Esta búsqueda es posible gracias a los registros publicados en un Controlador de Dominio con Active Directory a través de DNS *Service Location* (SRV).

Además, un dominio de Windows Server 2012 se identifica unívocamente mediante un nombre DNS (por ejemplo, *miuniversidad.com*) y cada equipo que forma parte de un dominio tiene un nombre DNS cuyo sufijo es el nombre DNS de dicho dominio (por ejemplo, *miequipo.miuniversidad.com*). El concepto más importante a tener en cuenta es que dominios y equipos se representan como objetos en Active Directory y como nodos en DNS. Aunque esto puede llevar a confusión, se puede diferenciar en que: DNS almacena zonas y registros de recursos y Active Directory guarda dominios y objetos del dominio. Active Directory utiliza DNS para tres funciones principales:

a) Resolución de nombres: DNS permite realizar la resolución de nombres al convertir los nombres de host a direcciones IP.
b) Definición del espacio de nombres: Active Directory utiliza las convenciones de nomenclatura de DNS para asignar nombre a los dominios.
c) Búsqueda de los componentes físicos Active Directory: para iniciar una sesión de red y realizar consultas en Active Directory se debe encontrar primero un controlador de dominio para procesar la autenticación. La base de datos DNS almacena información acerca de qué equipos realizan estas funciones

Fuentes: [51], [54]

5.2.2 Estructura lógica

La estructura lógica de Active Directory se centra en la administración de los recursos de la red organizativa, independientemente de la ubicación física de dichos recursos, y de la topología de las redes. La estructura lógica de Active Directory se basa en el concepto de dominio explicado en el punto 4.3. El uso de dominios permite conseguir los siguientes objetivos:

- **Delimitar la seguridad.** Un dominio define un límite de seguridad. Las directivas de seguridad, los derechos administrativos y las listas de control de acceso (Access Control Lists, ACLs) no se comparten entre los dominios.
- **Replicar la información**. Un dominio es una partición del directorio, que son unidades de replicación. Cada dominio almacena sólo la información sobre los objetos localizados en este dominio. Active Directory utiliza un modelo de replicación con varios maestros, de forma que todos los controladores de dominio reciben y pueden replicar los cambios.
- **Aplicar políticas/directivas de grupo**. Un dominio define un posible ámbito para las políticas. Al aplicar un objeto de política de grupo (GPO) al dominio, se establece como se configuran y se usan los recursos de dicho dominio.
- **Delegar permisos administrativos**. Se puede delegar a medida la autoridad administrativa tanto para unidades organizativas (OUs, *Organizacional Units*) individuales como a dominios individuales, lo que reduce el número de administradores necesarios. Los permisos administrativos se limitan al dominio.

Independientemente de la forma de organizar Active Directory dentro de la organización, la práctica adecuada es que dentro de un dominio siempre existan Unidades Organizativas. Una **Unidad Organizativa** es un objeto de Active Directory que puede contener a otros objetos del directorio. El objetivo de las unidades organizativas es estructurar u organizar el conjunto de los objetos del directorio, agrupándolos de forma coherente.

A la hora de implantar Active Directory en una organización, en función del tamaño de la misma y de las necesidades se puede optar por:

a) Utilizar un modelo con un dominio único y realizar un diseño adecuado de las unidades organizativas y los objetos contenidos en ellas.
b) Estructurar la organización en varios dominios. En este caso es necesario aplicar los conceptos de árbol, bosque y relaciones de confianza.

Al instalar el primer controlador de dominio en una organización el primer dominio que se genera se denomina dominio raíz, y contiene la configuración y esquema del bosque. Se pueden agregar dominios a este dominio raíz de dos formas: como subdominios, lo que da lugar a un árbol de dominios; o bien como dominios "hermanos" al mismo nivel, lo que da lugar a un bosque de dominios. Los dominios se

vinculan mediante relaciones de confianza entre dominios. Algunos conceptos importantes en el manejo de Active Directory con múltiples dominios son:

- **Árbol**: conjunto de uno o más dominios que comparten un espacio de nombres contiguo. Si existe más de un dominio, estos se disponen en estructuras de árbol jerárquicas. La relación padre-hijo entre dominios en un árbol es simplemente una relación de confianza.
- **Bosque**: grupo de árboles que no comparten un espacio de nombres contiguo, conectados a través de relaciones de confianza bidireccionales y transitivas.
- **Relación de confianza**: es una relación establecida entre dos dominios de forma que permite a los usuarios de un dominio ser reconocidos por los controladores de dominio de otro dominio. Estas relaciones permiten a los usuarios acceder a los recursos de otro dominio y a los administradores definir los permisos y derechos para los usuarios del otro dominio. En función de sus características, las relaciones de confianza se pueden clasificar en:
    a) Implícitas o explícitas. Las relaciones de confianza implícitas se crean de forma automática mientras que las explícitas son creadas de forma manual.
    b) Unidireccionales o bidireccionales. En una relación de confianza unidireccional un usuario de un dominio A puede utilizar recursos de un dominio B, pero no al revés. Al contrario ocurre en las relaciones de confianza bidireccionales donde los recursos son accesibles en ambos sentidos.
    c) Transitivas o no transitivas. Las relaciones de confianza transitivas permite heredar la relación entre dominios no heredados directamente. Una relación de confianza transitiva permite que si un dominio (A) confía en otro (B), y éste confía en un tercero (C), el primero (A) confía en éste último (C).

5.2.3 Estructura

La estructura física de Active Directory se utiliza para configurar y administrar el tráfico de red. Se compone de sitios y controladores de dominio. A través de la definición de la estructura física se establece dónde y cuándo se producen tanto el tráfico de replicación como el inicio de sesión. Los conceptos básicos son:

- **Sitio**: es una combinación de una o varias subredes IP que están conectadas por un vínculo de alta velocidad. Se puede asemejar a sedes físicas. Los sitios se crean principalmente para optimizar el tráfico de replicación y para permitir que los usuarios se conecten a un controlador de dominio mediante una conexión confiable.
- **Controlador de dominio** (Domain Controller, DC): es un equipo (normalmente ejecuta Windows Server 2012) que almacena una réplica de la información del directorio. Esta información se divide en varias categorías o particiones:
    - Categoría de esquema: contiene los tipos de objetos y atributos (comunes a todos los dominios en el bosque) que pueden ser creados en el Directorio Activo. Esta información se replica a todos los controladores de dominio del bosque.
    - Categoría de dominio: contiene los objetos del directorio para este dominio. La información se replica a todos los controladores de ese dominio pero no a otros dominios.
    - Categoría de configuración: contiene la estructura de los dominios y la topología de replicación. Esta información es común a todos los dominios en el bosque y se replica a todos los controladores de dominio.
    - Categoría de aplicaciones: las aplicaciones y los servicios pueden utilizar las particiones de directorio de aplicaciones para almacenar datos específicos de una aplicación. Pueden contener cualquier tipo de objeto, salvo entidades principales de seguridad (e.g. usuarios, grupos y equipos).
    - Catálogo global: es un controlador de dominio que almacena toda la información de las categorías anteriores, así como las copias parciales de sólo lectura de las demás categorías.

Todos los controladores de dominio admiten cambios en la información que gestionan, y aunque estos cambios se replican a todos los controladores de dominio, no es práctico que algunas de estas modificaciones se realicen en múltiples maestros debido al tráfico de replicación y a los posibles conflictos en las operaciones básicas. Por esta razón, la función de servidor de catálogo global y las operaciones de maestro único se asignan a determinados controladores de dominio.

5.2.4 Objetos y uso compartido de recursos

Los principales tipos de objetos que representan a las entidades o recursos que existen en un dominio son: usuarios, grupos, equipos y unidades organizativas.

Usuarios globales

En los sistemas Windows actuales es necesario crear cuentas de usuario y de grupo (de forma local) que sirven para identificar y autentificar a las personas que pueden acceder al sistema, así como para poder administrar los permisos que permiten aplicar el control de acceso adecuado a dichos usuarios en el sistema.

Este método local está disponible a través de la base de datos local llamada SAM (*Single Account Manager*). A través de una cuenta SAM se puede administrar los usuarios y grupos del sistema, pudiendo asignar políticas de seguridad mediante la herramienta *gpedit.msc*. La administración SAM crea por defecto dos cuentas: *Administrador* e *Invitado* (deshabilitada inicialmente por razones de seguridad). La cuenta de Administrador es la que se utiliza para crear y administrar nuevos usuarios en el sistema local. El principal problema de la protección local es que si una persona necesita trabajar en varios ordenadores, deberá poseer una cuenta de usuario en cada uno de ellos.

Por esta razón, en un dominio de Windows se pueden crear cuentas de *usuario global* (entendiendo global como global al dominio). Los datos de una cuenta de usuario global se almacenan en la base de datos de Active Directory: NTDS.DIT (*New Technology Directory Services*), y por tanto, son conocidos por todos los ordenadores del bosque al que pertenece el dominio. Esta cuenta es única, asociándole un identificador distintivo llamado SID.

Grupos

Los grupos son contenedores de otros tipos de objetos como usuarios y equipos. Cuando se asignan permisos de seguridad a un grupo en la lista de control de accesos (ACL) sobre un recurso, todos los miembros del grupo reciben dichos permisos.

Al igual que los usuarios globales, los grupos son visibles desde todos los ordenadores del dominio. Existen dos grupos principales: *grupos de distribución* y *grupos de seguridad*. Los primeros se utilizan exclusivamente para crear listas de distribución de correo electrónico, mientras que los grupos de seguridad se utilizan con

fines administrativos para asignar los permisos de acceso a los recursos de la red. Los grupos de seguridad son los más importantes.

Existen tres clases de grupos de seguridad según su ámbito. Según el nivel funcional del dominio, los siguientes grupos albergan distintos tipos de objetos:

- **Grupos locales del dominio**: sólo son visibles en el dominio en que se crean. Se utilizan para conceder permisos y derechos en cualquiera de los equipos del dominio.
- **Grupos globales**: son visibles en todos los dominios del bosque. Se utilizan para clasificar a los usuarios en función de las tareas que realizan.
- **Grupos universales**: Son visibles en todo el bosque y pueden contener cuentas de usuario y grupos globales, así como otros grupos universales de cualquier dominio del bosque.

La regla recomendada a la hora de la utilización de grupos y asignación de recurso es la siguiente:

- Asignar usuarios globales a grupos globales, según las labores que desempeñen en la organización
- Incluir usuarios y/o grupos globales en grupos locales (del equipo o del dominio) según el nivel de acceso que vayan a tener.
- Asignar permisos y derechos únicamente a estos grupos locales (del equipo o del dominio).

Equipos

Además de usuarios y grupos, la base de datos del Directorio Activo recoge información de *cuentas de equipo* por cada uno de los sistemas miembro de un dominio.

En cada cuenta de equipo se almacena el nombre de equipo y el identificador único y privado (análogo al SID) que identifica al equipo unívocamente en la red. Este identificador sólo lo conocen los controladores de dominio y el propio sistema miembro. Al ser un dato interno del sistema operativo ni siquiera el administrador puede cambiarlo, es por ello que se denomina un principal de seguridad (*security principal*).

Existen dos protocolos de autenticación principales entre los equipos miembros de un dominio y los controladores de dominio:

- NTLM: protocolo que se utiliza en versiones iguales o anteriores a Windows NT.
- Kerberos V5: este protocolo expuesto en el punto 4.3.2 presenta numerosas ventajas respecto a NTLM, pero sólo es viable si todas las máquinas del dominio utilizan sistemas operativos con versiones superiores a Windows NT. Hoy en día, debido a su antigüedad, es poco frecuente encontrar sistemas Windows NT, por lo que Kerberos es el método estándar de facto.

Unidades organizativas

Las unidades organizativas son contenedores de objetos de Active Directory. La utilidad principal de las unidades organizativas es la de poder delegar la administración de sus objetos a otros usuarios distintos del administrador del dominio, pudiendo personalizar el comportamiento de los usuarios y equipos mediante la aplicación de directivas de grupo. Esto se aplica habitualmente en dominios con un tamaño considerable donde es necesario diversificar las tareas de gestión del mismo.

Para diversificar las tareas de gestión se suele utilizar la delegación de la administración. Para delegar la gestión basta con selección la acción "Delegar el control…" en el menú contextual de una unidad organizativa.

La delegación de control se puede hacer de forma completa, ofreciendo control total sobre la unidad, o de forma parcial, permitiendo la lectura, modificación y/o borrado de objetos. La delegación de control de forma parcial ofrece muchas posibilidades al poder establecer permisos sobre cada uno de los atributos de cada tipo de objeto.

Uso de recursos compartidos

Cualquier sistema Windows (servidor o estación de trabajo) puede compartir carpetas. En Windows Server 2012 se pueden compartir carpetas tanto locales como de equipos pertenecientes a la red utilizando el complemento de "Archivos Compartidos". De forma local, se puede compartir una carpeta desplegando el menú contextual desde una ventana del explorador de archivos y seleccionando la opción "Compartir…"

Es importante tener en cuenta que existe diferencia al compartir una carpeta si reside en un sistema de ficheros FAT o NTFS. En el primero sólo existe la opción de decidir los usuarios que pueden acceder al recurso, mientras que utilizando un sistema NTFS se pueden establecer además los permisos sobre la carpeta. Además, no hay que olvidar que al acceder a un recurso de red se accede desde un equipo que también debe tener el derecho concedido para obtener la lista de recursos.

Cuando se comparten recursos dentro de un dominio de Windows, se deben realizar las siguientes acciones:

- Compartir físicamente el recurso/carpeta.
- Publicar el recurso en el directorio. Esto se hace creando un objeto nuevo en la unidad organizativa del tipo *recurso compartido,* al que se le asocia un nombre simbólico. El administrador debe ser responsable de compartir y publicar un recurso de forma correcta ya que no se comprueba su existencia, aunque existe la opción de compartir en el directorio desde la carpeta para crear automáticamente el objeto en el directorio.

Además, hay que tener en cuenta que cuando se une un equipo a un dominio, se crean de forma automática y por defecto los siguientes recursos (que no se deben modificar ni prohibir):

RECURSO	**DESCRIPCIÓN**
Unidad$	Se crea un recurso compartido por cada partición existente en el equipo (e.g: C$, D$)
ADMIN$	Recurso utilizado por el propio sistema durante la administración remota
IPC$	Recurso que agrupa las colas de mensaje utilizadas por los programas para comunicarse entre ellos. Se utiliza durante la administración remota
NETLOGON$	Recurso que exporta un controlador de dominio para proporcionar a los ordenadores miembros del dominio el servicio de validación de cuentas globales a través de la red (Net Logon Service).
SYSVOL	Recurso que exporta cada controlador de dominio de un dominio Windows. Contiene información de Active Directory que debe replicarse en todos los controladores de dominio.

Tabla 5-1: Recursos compartidos habituales en Windows

Los comandos utilizados para compartir y utilizar recursos en la red son:

- **net share:** para crear, eliminar y mostrar recursos compartidos
- **net use:** para conectar y desconectar un equipo de un recurso compartido. También se utiliza para mostrar información acerca de las conexiones del equipo.

5.2.5 Novedades en la versión 2012

La tendencia actual en las organizaciones es que los usuarios/empleados solicitan cada vez más acceso a los datos corporativos desde varios dispositivos, incluidos dispositivos personales, lo que podemos ver como un nuevo nivel de productividad en las empresas. Para cubrir esta necesidad y a la vez permitir a los administradores de TI mantener el control sobre los recursos, Windows Server 2012 Active Directory incluye cambios y mejoras principalmente enfocadas a la federación de identidades (AD FS, de *Active Directory Federation Services*). De esta forma se avanza en los nuevos modelos de Single Sign-On ofrecidos tanto en la red interna como fuera de la red corporativa. Esto es especialmente útil, más si cabe, con los nuevos modelos de computación en la nube, donde se despliegan multitud de servicios, distribuidos en nubes y servicios diferentes que necesitan arquitecturas preparadas para esta heterogeneidad.

Las mejoras y cambios con mayor impacto que ofrece la versión 2012 de Active Directory son:

- Permitir a los administradores de TI asociar dispositivos a Active Directory y utilizar esta asociación como mecanismo de autenticación de segundo nivel.
- Permitir a usuarios usar SSO desde los dispositivos asociados.
- Permitir a los usuarios conectar a aplicaciones y servicios desde cualquier lugar con *Web Application Proxy*.
- Administrar los riesgos de que los usuarios trabajen desde cualquier lugar, accediendo a información protegida con *Multi-Factor Acces Control* y *Multi-Factor Authentication*.

Destacamos los siguientes elementos y tecnologías subyacentes a estos cambios:

- *Workspace Join*
- *Device Registration Service*
- *Multifactor Authentication*: el usuario debe proporcionar credenciales y el dispositivo debe estar registrado.

- Control de acceso a recursos sobre: **aplicación, usuario, dispositivo y localización;**
- *Web Application Proxy*
- Control de acceso condicional
- Métodos de autenticación

De los dos últimos ofrecemos una breve descripción.

Control de acceso condicional (Conditional Access Control)

Sobre las aplicaciones, usuarios, dispositivos y localizaciones se aplican **reglas** de solicitud. Los beneficios del control de accesos condicional son:

- Ofrece políticas de autorización flexibles por aplicación.
- Permite crear reglas de autorización de emisión para aplicaciones de confianza.
- Experiencia de interfaz gráfica rica.
- Soporte para PowerShell y lenguaje de reglas de solicitud para escenarios avanzados.
- Permite personalizar mensajes de "Acceso Denegado" para aplicaciones de confianza.

Métodos de autenticación

Los métodos de autenticación que ofrece AD FS en función de desde donde se hace el acceso a los recursos:

- Fuera de la red corporativa:
    - *Forms Authentication* (método por defecto)
    - *Certificate Authentication* (smarcards y certificados de usuario)
- Red interna:
    - *Windows Authentication* (método por defecto): cuando se utiliza este método a través de navegador hay que tener en cuenta que no todos los navegadores lo soportan.
    - *Forms Authentication*
    - *Certificate Authentication*

AD FS puede utilizar varios protocolos para suministrar los tokens a los solicitantes: WS-Trust, WS-Federation y SAML (ver punto 4.3.6), lo que le permite tener una buena capacidad de integración con otros proveedores y servicios.

Fuentes: [55]

5.2.6 Escenarios y configuraciones

Los roles que adopta un servidor Windows Server 2012 con Active Directory (ver punto 5.2.1) determina los posibles escenarios de despliegue de este tipo de servicio, entre los que podemos destacar:

- Escenario empresarial
- Escenario de directorio ligero
- Escenario de infraestructura de clave pública
- Escenario de servicios federados

Escenario empresarial

Es el escenario tradicional que también sirve de base para otros escenarios. En este escenario existe un servidor Active Directory donde se centraliza toda la gestión de identidades y control de accesos para todos los dispositivos pertenecientes a la red corporativa, a través del ya introducido concepto de dominio. Es necesario diseñar e implementar la organización del directorio: árboles de directorio, bosques, etc. En función del esquema organizacional de la empresa. Además, la gestión se basa en el uso de herramientas administrativas para Políticas de Grupos (GPO). Este escenario ofrece capacidades para:

- Auditoría (registro de cambios)
- Establecer políticas de contraseña no restringidas a una única política global.
- Políticas de Kerberos y políticas de clave pública única por dominio.
- Política de recuperación de sistema de ficheros cifrados única por dominio.
- Definición de zonas globales y resolución de nombres a través de DNS.
- Parada y reinicio del directorio

El rol de servidor necesario para implementar este escenario es AD DS. Se puede implementar una arquitectura de replicación donde existe un controlador de dominio principal (que permite lectura y escritura de propiedades sobre los objetos) y otro controlador de dominio de sólo lectura (RODC).

Escenario de directorio ligero

Escenario donde no hay necesidad de mantener un dominio, y todo su conjunto de funcionalidades, sino que es suficiente con mantener un directorio de objetos al que acceden diferentes aplicaciones preparadas para integrarse con Active Directory. Este escenario ofrece básicamente capacidades LDAP a aplicaciones cliente y es especialmente útil cuando no existe necesidad de implantar un dominio pero existen aplicaciones empresariales como CRM (*Customer Relationship Management*), ERP (*Enterprise Resource Planning*) que acceden a un almacén común de usuarios, clientes, proveedores, etc.

El rol de servidor para implementar este escenario es AD LDS.

Escenario de infraestructura de clave pública (PKI)

Escenario donde Active Directory hace las funciones de autoridad de certificación y por lo tanto puede incluirse dentro de una infraestructura de clave pública dentro de la organización. Algunas funciones que puede adoptar Active Directory en este tipo de escenario son:

- Emisión y admisión de certificados
- Protección de datos cifrados frente a pérdidas
- Comprobación y revocación de certificados
- Mecanismo de autenticación para servidores web con certificados (hhtps)
- Aumento de la seguridad de la red inalámbrica mediante uso de certificados
- Refuerzo de la administración de identidades con el uso de tarjetas inteligentes (que incluyen certificados).
- Protección de derechos de propiedad intelectual

Los roles de servidor para implementar estos escenarios son: AD CS Y AD RMS, este último en el caso de funcionalidades para protección de derechos de propiedad intelectual.

Escenario de servicios federados

Escenario donde la arquitectura AIM sirve además como suministrador de servicios de identificación y autenticación fuera de los límites de la red corporativa permite el uso de tecnologías de Single Sign-On web.

5.2.7 Identificadores y proceso de autenticación

Al tratar el tema de los identificadores en Active Directory es esencial comprender tres conceptos similares pero con diferencias sutiles: GUID (*Global Unique Identifier*), SID (*Security Identifier*) y RID (*Relative Identifier*). Como ya se introdujo en el punto 5.1, la gestión de los identificadores es uno de los puntos que más problemas generan al tratar de integrar entornos Windows y Linux, ya que el modelo de seguridad de cada sistema operativo es diferente en este sentido (entre otros).

Lo más importante es que todos los objetos contenidos en Active Directory son identificables de forma unívoca a través del GUID.

Un GUID es un identificador alfanumérico de 128 bits, cuyo valor es único en una organización, y en la práctica se puede decir que también único en el mundo. El rango de valores es de 2^{128}. Es la implementación de Microsoft del estándar UUID.

El GUID se utiliza internamente para identificar objetos en Active Directory, se localiza a través de la propiedad "objectGUID", y se publica en el catálogo global.

Por otro lado, el SID es un valor único de longitud variable utilizado para identificar un sujeto confiable en Windows. Cada cuenta (de usuario, grupo, etc) tiene un SID único emitido por una autoridad, que habitualmente es SAM o un controlador de dominio, y almacenado en una base de datos segura (Active Directory). Cada vez que el usuario accede al sistema, éste obtiene el SID del usuario desde la base de datos y lo asocia al token de acceso de ese usuario para la sesión. El sistema utiliza el SID para identificar al usuario en todas las interacciones posteriores que realice. El SID no puede ser el mismo para distintos usuarios o grupos. El modelo de seguridad de Windows utiliza el SID en tres elementos principales:

- Descriptores de seguridad. Los descriptores de seguridad contienen la información de seguridad asociada a un objeto asegurable.
- Entradas de control de acceso (ACE, *Access Control Entry*). Las entradas de control de acceso definen qué usuarios y grupos tiene derechos de acceso concedidos o denegados en un objeto asegurable.
- Tokens de acceso. Son objetos que guardan la información del contexto de seguridad asociado al usuario que inicia una sesión.

La información en un token de acceso incluye la identidad y los privilegios de la cuenta de usuario asociados con el proceso de autenticación (ver tabla 5-1):

ELEMENTOS DE UN TOKEN DE ACCESO
Identificador de Seguridad (SID) de la cuenta de usuario.
SID de los grupos de los que el usuario es miembro.
SID de login (logon SID) que identifica la sesión de inicio actual.
Lista de los privilegios que tiene el usuario y los grupos de los que es miembro.
SID de propietario.
SID del grupo primario.
DACL que el sistema utiliza cuando el usuario crea objetos con seguridad sin especificar un descriptor de seguridad. DACL (Discretionary Access Control List) es una lista que identifica los sujetos confiables a los que se permite o deniega el acceso al objeto con seguridad.
Origen del token de acceso.
Si el token es primario o de suplantación.
Lista opcional de SID restringidos.
Niveles actuales de suplantación.
Otras estadísticas.

Tabla 5-2: Información de Token de inicio de sesión Windows

El SID se representa en formato alfanumérico como una cadena S-R-X-Y-RID, donde:

- **S**: Indica que la cadena corresponde a un SID
- **R**: Nivel de revisión
- **X**: Valor de la autoridad del identificador
- **Y**: Identificador de sub-autoridad(es)
- **RID**: *Relative Identifier;* es un valor auto-generado por la autoridad encargada de mantener los identificadores. Esta autoridad puede ser el sistema local a través de SAM, o un controlador de dominio Active Directory. El valor de RID es único sólo a nivel de dominio.

La característica que hay que tener en cuenta del SID y que lo diferencia del GUID, es que el SID puede cambiar. Aunque los SID de grupos no cambian, un SID de

una persona puede ser diferente ya que las personas se pueden mover dentro de la organización (cambiar de dominio) y con ellas sus cuentas. Al cambiar de dominio, el RID que se genera en cada uno puede ser diferente y por tanto cambiar el SID actual del usuario. Por este motivo, en Active Directory existe la propiedad SIDHistory, que almacena el conjunto de SID que ha tenido una cuenta de usuario durante su vida útil.

Acceso interactivo a dominio

Otros conceptos a tener en cuenta están relacionados con el acceso del usuario a través de un dominio:

- Este tipo de acceso concede al usuario tanto acceso local como acceso a recursos de red en el dominio.
- El usuario debe tener una cuenta en Active Directory.
- El equipo debe tener una cuenta (también denominado ingresar) en el dominio de Active Directory, además de tener conexión de red para poder realizar las comunicaciones.

El esquema del proceso de autenticación se puede ver en la figura 5-1. La secuencia de acciones es la siguiente:

1. El usuario inicia el sistema o presiona la secuencia SAS (CTRL+ALT+DEL).
2. Winlogon recibe la SAS y se pone en contacto con los proveedores de credenciales para obtener el listado de los diferentes tipos de credenciales disponibles en el sistema.
3. Winlogon procesa las credenciales aportadas por el usuario y las envía al subsistema LSA.
4. LSA utiliza el paquete Negotiate. Intenta el proceso de autenticación utilizando el protocolo Kerberos. Al ser una autenticación mediante usuario de Active Directory, el protocolo Kerberos se comunica con la máquina que realiza la función de controlador de dominio.
5. En el controlador de dominio, el subsistema LSA utiliza Kerberos para validar las credenciales de usuario, verificando la información almacenada en la base de datos de Active Directory.
6. El controlador de dominio devuelve al subsistema LSA de la máquina local el resultado de la autenticación.

7. Si las credenciales son válidas, el subsistema LSA de la máquina local devuelve un token de acceso a Winlogon y se inicia un nuevo proceso de creación de Shell de usuario y escritorio, mediante el ejecutable explorer.exe.

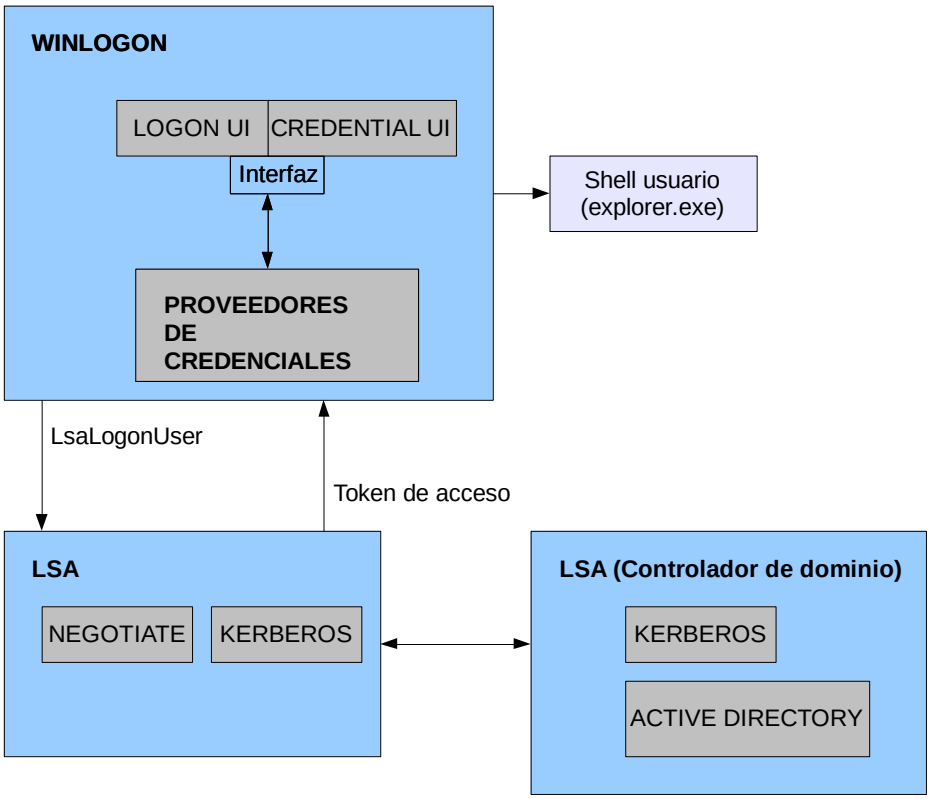


Figura 5-1: Proceso de autenticación desde Windows a Active Directory

5.3 Samba y OpenLDAP

Tradicionalmente en los entornos UNIX se utiliza el servidor NIS (*Network Information System*) para la resolución de nombres y la distribución de información a través de la red. Mediante NIS, toda la configuración contenida en los ficheros del directorio /etc y los subdirectorios group, hosts, mail, netgroup, networks, passwd, printcap, protocols, rpc y servicios, se distribuyen por la red de forma fácil al tratarse de ficheros texto.

No obstante, el manejo de grandes cantidades de información se vuelve complicado sin la existencia de una estructura organizada. NIS está diseñado exclusivamente para plataformas UNIX por lo que no resulta adecuado para servicios de administración centralizados y heterogéneos, aunque en el caso de interacción con sistemas Microsoft se podría pensar en la implementación de sistemas Windows que hagan uso de los SFU, los cuales implementan servicios de integración con NIS.

Con el uso de LDAP se solucionan los problemas de escalabilidad de NIS ya que no está restringido a redes UNIX y, como ya se ha dicho, Active Directory es un servicio de directorio que soporta el uso de LDAP.

Dentro de las implementaciones más comunes de LDAP se encuentra OpenLDAP, que es un paquete completo de aplicaciones y herramientas de desarrollo basadas en una implementación libre del protocolo.

Por otra parte, aunque el uso de OpenLDAP sería el adecuado en entornos UNIX, debido a que se está tratando en todo momento de entornos heterogéneos completamente integrados, para conseguir tal objetivo es necesario el uso de Samba, ya que es el sistema específico para cumplir la tarea de controlador de dominios típicos Windows (Active Directory) en entornos no Windows. De esta forma, tanto clientes Windows como clientes Linux tendrán un sistema único de autentificación y centralización de cuentas.

Ahora bien, existen dos opciones para la implantación de un servidor Samba, según el sistema de respaldo (*backend*) utilizado como base de datos de información de cuentas. Versiones anteriores a la 3 del paquete Samba permitían varios sistemas de almacenamiento de cuentas y acceso, aunque a partir de la versión 3 sólo se soportan tres tipos:

- **Smbpasswd**: este sistema está dejando de utilizarse y sólo almacena cuentas de usuario Samba.
- **Tdbsam**: sistema basado en un fichero de formato binario tdb. TDB es un tipo de base de datos bastante trivial y muy pequeña que permite escritura simultánea y gestión sencilla de interbloqueos en las operaciones. Tdbsam sólo almacena cuentas de usuario Samba.
- **Ldapsam**: sistema que almacena tanto información de cuentas de usuario y grupo de Samba como POSIX (UNIX) en un repositorio único

Podemos educir que la implantación del servidor Samba se puede hacer utilizando tdbsam o ldapsam. A continuación se ofrece una explicación más detallada de ambas opciones. En el caso de utilizar ldapsam entra en juego además la implantación del servidor OpenLDAP ya que será el que ofrezca a Samba la información de las cuentas. En la figura 5-1 se muestran las posibilidades de implantación de arquitectura de Samba.

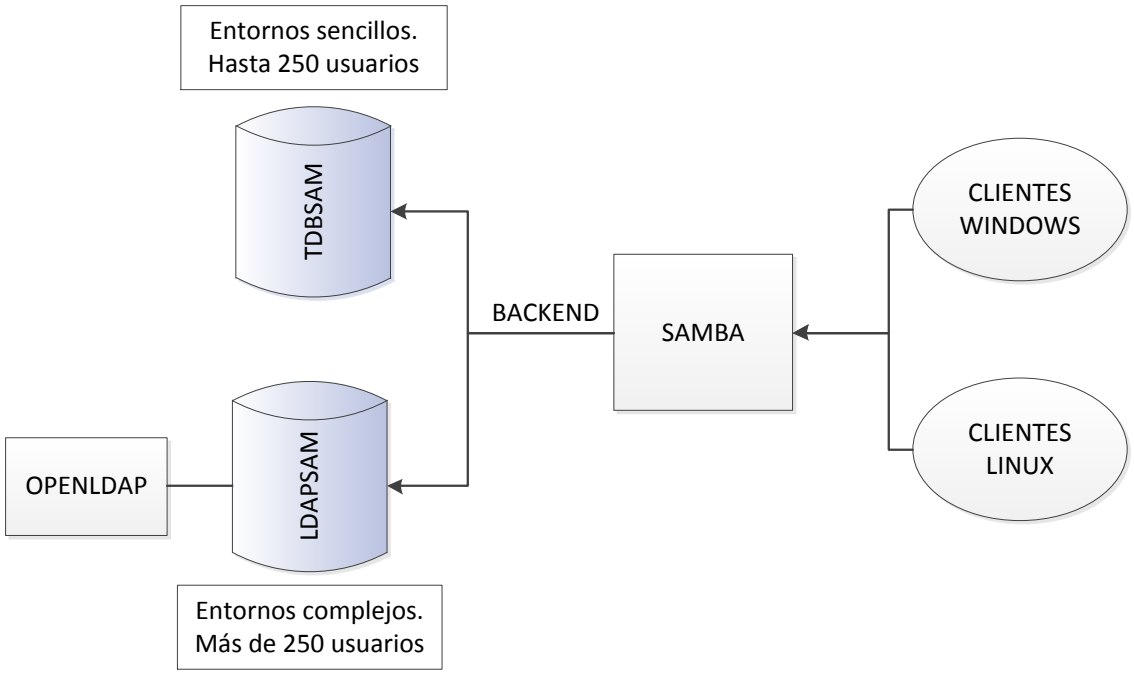


Figura 5-2: Arquitectura de Samba

Como ya se introdujo en el punto 4.3.4 relativo al protocolo SMB/CIFS, Samba es un paquete de servicios que empezó su desarrollo para dar soporte a ficheros e impresoras pero que hoy día ofrece un amplio conjunto de funcionalidades, tanto para servidores como para clientes, utilidades de migración, así como otras herramientas para

mejorar la interoperabilidad con Microsoft Windows. Samba es compatible con clientes a partir de Windows 7 desde las versiones 3.3.7 y 3.4.0.

Se puede encontrar información más completa sobre Samba en [56], [32]. [57]. Referencias de OpenLDAP sobre Suse se pueden encontrar en [58], [59].

5.3.1 Configuración del servidor Samba con tdbsam en OpenSuse

El sistema tdbsam proporciona una base de datos para servidores locales únicos (PDC) donde no se necesita un controlador de dominio de respaldo (BDC), ya que no está soportado. Tdbsam está recomendado para un máximo de 250 usuarios.

Tdbsam almacena tanto la información que se almacena con un sistema smbpasswd como la información extendida en las cuentas SAM de Windows NT/20xx. La implementación de tdbsam responde a las necesidades de usuarios que no requieren un entorno complejo implementado con OpenLDAP.

El software necesario para poder implantar un servidor samba y poder utilizar todas las funcionalidades es: *samba* y *samba-client*.

En el caso de utilizar tdbsam es importante tener en cuenta que la gestión de los usuarios debe hacerse primero en el sistema local, es decir, se deben dar de alta los usuarios Linux (cuentas POSIX) antes de darlos de alta en el servidor Samba. La gestión de usuarios se hace desde la herramienta *Gestión de usuarios y grupos* en la categoría *Seguridad y Usuarios* de YAST.

Por otra parte, como bien se ha expuesto, en Active Directory existen tres tipos de cuentas principales: usuarios, grupos y equipos. En el caso de Linux con Samba, no existen cuentas específicas para los equipos, por lo que se crean dichas cuentas como usuarios normales con el símbolo $ al final de su nombre de usuario.

Configuración del servidor Samba

Una vez creadas las cuentas de usuario necesarias, la configuración del PDC se realiza desde la herramienta *Servidor Samba* dentro de la categoría *Servicios de Red* de YAST. Dentro de la herramienta se configuran las siguientes opciones dentro de las cinco pestañas presentes:

- Inicio: en esta pestaña se seleccionan las opciones:
    - *Inicio del servicio - Durante el arranque* para que Samba funcione automáticamente al arrancar la máquina.

  - *Valores de configuración del cortafuegos – Puerto abierto en el cortafuegos.* Al seleccionar esta opción se abren los puertos necesarios en el cortafuegos para habilitar las conexiones a Samba.

- Recursos compartidos: en esta pestaña aparece un listado de los recursos compartidos configurados en el servidor Samba. Se deben habilitar y deshabilitar los recursos que el administrador considere. Además se puede habilitar a los usuarios para que compartan sus directorios.

- Identidad: esta pestaña es la más importante para la configuración del servidor Samba como PDC. Simplemente hay que realizar la siguiente configuración:

  - *Nombre de grupo de trabajo o dominio*: es el nombre para el dominio (p.ej. miuniversidad.com).

  - *Controlador de dominio*: seleccionar *Primario (PDC).* En caso de encontrarse en un entorno distribuido se podría configurar un servidor como *Secundario (BDC).*

  - *Nombre de host de NetBIOS*: nombre de máquina del servidor que se utilizará para el protocolo y la red de Microsoft.

  - *Compatibilidad con servidor WINS*. Se establece esta opción en caso de que el servidor tenga que funcionar como servidor WINS.

- Dominios de confianza: en esta pestaña se pueden establecer otros dominios con los que establecer relaciones de confianza al estilo de Active Directory cuando se está trabajando en un bosque.

- Configuración LDAP: esta pestaña es útil sólo cuando se utiliza OpenLDAP (o cualquier otro servidor LDAP) como sistema de gestión de cuentas. Este apartado se explica en el siguiente punto relativo a la configuración de Samba con OpenLDAP.

Creación de usuarios y grupos

Una vez configurado el servidor Samba (cuyos valores se ven reflejados en el fichero de configuración /etc/samba/smb.conf) el siguiente paso es añadir los usuarios

existentes en el sistema al propio Samba. Para ello se utiliza el siguiente comando para cada usuario:

```
pdbedit –a nombreusuario
```

Por último, es necesario realizar la correspondencia de los grupos UNIX a grupos Windows para facilitar la integración de los mismos en ambos sistemas. Lo más habitual es manejar los grupos: administradores, usuarios e invitados. Para realizar la correspondencia se ejecutan los siguientes comandos:

```
net groupmap add ntgroup=”Domain Admins” unixgroup=root rid=512
net groupmap add ntgroup=”Domain Users” unixgroup=users rid=513
net groupmap add ntgroup=”Domain Guests” unixgroup=nobody rid=514
```

Además, se asignan los privilegios específicos al grupo de administradores del dominio para que puedan unir máquinas al dominio y tareas propias de administración. De esta forma se puede crear un usuario de nombre *Administrador* perteneciente a este grupo para añadir máquinas Windows al dominio:

```
net –S localhost –U root rpc rights grant “servidor\Domian Admins” SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege
```

Fuentes: [59]

5.3.2 Configuración del servidor Samba con ldapsam en OpenSuse

El sistema ldapsam proporciona un directorio de gestión completo para una instalación que requiera un entorno distribuido. Es el sistema adecuado cuando es necesario utilizar un controlador de respaldo: PDC + BDC y está recomendado para más de 250 usuarios.

Como ya se ha explicado en el punto 4.3.1, el protocolo LDAP se basa en una estructura de árbol llamada DIT (*Directory Information Tree*) en la que existen entradas, identificadas por su nombre distintivo (DN) y que pueden ser de diferente tipo.

Los tipos de entradas u objetos que acepta un directorio LDAP se establecen mediante esquemas de directorio. Los tipos de objeto se determinan mediante una clase de objeto (*object class)* en el fichero de definición de esquema, donde se establecen los atributos que le corresponden a dicha clase. El esquema debe contener definiciones de todas las clases de objetos y atributos. Los esquemas más comunes están definidos en

las RFCs 2252 y 2256, así como LDAP RFC 4519. A partir de la versión 3 de Samba se establece un formato de esquema específico que se puede encontrar en el directorio *examples/LDAP* de la distribución de Samba.

La implementación libre de LDAP es OpenLDAP, que es la más utilizada en las distribuciones Linux. El software necesario para la instalación de un servidor Samba con soporte OpenLDAP es:

- En la parte del servidor: yast2-ldap-server, openldap2 y samba.
- En la parte del cliente: samba-client, openldap2-client, pam-ldap, nss-ldap.

Con una configuración de red correcta, donde es muy importante realizar una configuración adecuada de la resolución de nombres (servidor DNS), la implantación del servidor Samba-OpenLDAP se realiza básicamente utilizando las siguientes herramientas de YAST:

- Servidor LDAP
- Servidor Samba
- Cliente LDAP

Fuentes: [59]

Configuración del servidor LDAP

La recomendación que da Samba es realizar primero toda la configuración del servidor OpenLDAP y después realizar la integración de Samba con dicho servicio. Dentro de la herramienta *Servidor LDAP* las opciones principales que hay que configurar son:

- Configuración general: habilitar para que el servicio se inicie automáticamente al arrancar la máquina en la opción Iniciar el servidor LDAP, y abrir los puertos correspondiente seleccionando la opción Puerto abierto en el cortafuegos.
- Configuración de base de datos: en la configuración de base de datos hay que introducir:
    - Tipo de base de datos: la base de datos debe ser del tipo *hdb*. Una base de datos *hdb* es una variante del sistema *bdb* con un diseño jerárquico que permite cambiar el nombre de los subárboles del directorio.
    - DN base: nombre distintivo del dominio. Por ejemplo, *miuniversidad.com* tendría como DN: *dc=miuniversidad, dc=com*.

  - DN del administrador y su contraseña: nombre distintivo del administrador del dominio (p.ej. *cn=administrador*). Es necesario añadir el DN base para completar el DN del administrador: *cn=administrador, dc=miuniversidad, dc=com*. También es necesario introducir una contraseña para el usuario administrador.
  - Directorio de base de datos: se puede ver donde está localizada en el disco la base de datos del directorio LDAP. La opción *Usar esta base de datos como base por defecto para los clientes OpenLDAP* hace que se escriba como nombre de host "localhost" y el DN base introducido antes en el archivo de configuración para los clientes OpenLDAP que está en */etc/openldap/ldap.conf*.
  - Una vez configurada la base de datos los conceptos a los que se debe prestar más atención en el directorio son:

- Esquemas: en el caso de integración con Samba es importante seleccionar el esquema samba3 dentro de la opción *Archivos de esquema* del servidor LDAP.
- TLS: como ya se ha explicado en el punto 4.3.7. TLS es un protocolo de cifrado surgido como evolución y sustituto de SSL. Permite realizar comunicaciones seguras a través de red por la que habilitar este protocolo en el servidor LDAP permite comunicación segura entre el servidor y los clientes LDAP. Hay que tener en cuenta que el funcionamiento de TLS está basado en el uso de certificados. La configuración de TLS se realiza en *Valores globales de configuración – Configuración de TLS*, dentro del árbol de opciones de configuración del servidor LDAP. El uso de certificados para TLS en LDAP puede realizarse de dos formas:
  - Importando un archivo de certificados específico.
  - Utilizando un servidor de certificados común: en este caso se puede configurar un servidor de certificados a través de la herramienta *Gestión de CA* dentro de la categoría *Seguridad y Usuarios* de *YAST*. Se puede encontrar más información acerca de la gestión de certificados X.509 en la guía de seguridad de OpenSuse.
- Directivas de contraseñas: dentro de la base de datos de directorio creada es importante habilitar las directivas de contraseñas para obtener un entorno lo más seguro posible. La configuración de las directivas de contraseña se realiza en la opción *Configuración de las directivas de contraseñas*. Es necesario establecer

un nombre distintivo (DN) al objeto de directivas. En las directivas se establecen las políticas de cambio, antigüedad y bloqueo de contraseñas: comprobar calidad de contraseña, si el usuario puede o no puede cambiar la contraseña, antigüedad mínima y máxima de la contraseña, bloqueo de contraseña, etc.

Configuración de cliente LDAP

Es necesario configurar la máquina como cliente LDAP ya que el servidor Samba utilizará esta capacidad para poder conectar con el directorio LDAP configurado anteriormente. La configuración de cliente LDAP se realiza desde la herramienta *Cliente LDAP* de los *Servicios de red* en *YAST*. Lo más importante en esta herramienta de configuración es habilitar el uso de LDAP e introducir los valores del servidor LDAP: dirección IP del servidor y el DN base del directorio. En caso de que se haya habilitado en el servidor el uso de TLS/SSL también es necesario habilitarlo en el cliente.

Es habitual seleccionar la casilla *Crear directorio personal al iniciar sesión* ya que permite crear una carpeta en la máquina al iniciar sesión con un usuario del directorio.

Existen otros aspectos de configuración avanzada que escapan al alcance de este proyecto pero que en la mayoría de casos son importantes, principalmente para habilitar la modificación de información en el servidor LDAP como administrador, así como permitir la gestión de grupos y usuarios. Si la máquina no va a realizar tareas administrativas en LDAP no es necesario llevar a cabo esta configuración. En caso contrario, será necesario acceder a la *Configuración avanzada* dentro de la herramienta *Cliente LDAP* y establecer los valores oportunos de DNs de grupos, usuarios y contraseñas, así como el del administrador.

Configuración del servidor Samba

Una vez completada toda la configuración del servidor LDAP hay que llevar a cabo la implantación del servidor Samba y su integración con LDAP. La configuración de Samba es la misma en cuanto a servicio, cortafuegos, identidad, recursos compartidos y dominios de confianza vista en el apartado de Configuración de Samba con tdbsam (a través de la herramienta *Servidor Samba*). El único punto que difiere es en la pestaña *Configuración LDAP*, donde hay que habilitar el uso de LDAP y realizar la configuración de las siguientes opciones:

- *Usar sistema secundario para contraseñas de LDAP*: hay que habilitar esta opción e introducir la URL del servidor LDAP para utilizar el directorio LDAP como proveedor de contraseñas. Si el servidor LDAP y el servidor Samba se encuentran en la misma máquina basta con introducir la URL ldap://127.0.0.1.
- *Usar sistema secundario Idmap de LDAP*: hay que habilitar esta opción e introducir la URL del servidor LDAP correspondiente para utilizar el directorio LDAP como sistema para realizar la correspondencia de identificadores. Si el servidor LDAP y el servidor Samba se encuentran en la misma máquina basta con introducir la URL ldap://127.0.0.1.
- *DN de base de búsqueda*: en este campo es necesario introducir el DN del directorio configurado en LDAP (p.ej. *dc=miuniversidad, dc=com*).
- Autenticación: para poder realizar las tareas oportunas de gestión de grupos y usuarios hay que identificar al usuario administrador (DN completo) de la base de datos del directorio (p.ej. cn=administrador, dc=miuniversidad, dc=com)

Si la configuración del servidor LDAP, el cliente LDAP y el servidor Samba es correcta, al realizar la prueba de conexión entre Samba y LDAP el resultado deberá ser satisfactorio. Por otra parte, si se habilita el uso de TLS en LDAP habrá que configurarlo también en Samba accediendo a los *Valores de configuración avanzada*.

Creación de usuarios y grupos

Una vez realizada la implantación de los servidores OpenLDAP y Samba el siguiente paso es dar de alta los usuarios y grupos.

Al igual que en la configuración de Samba con tdbsam, la gestión de usuarios se realiza mediante la herramienta *Gestión de usuarios y grupos* en la categoría *Seguridad y usuarios* de *YAST*. La única diferencia con el caso anterior es que en el caso de usuarios y grupos de un directorio se utilizan los filtros *Usuarios LDAP* y *Grupos LDAP*.

Lo más importante en este punto es crear los grupos LDAP y la correspondencia de dichos grupos con los grupos Windows más comunes para facilitar la integración de los mismos en ambos sistemas (al igual que se hace en la configuración de Samba con tdbsam). La creación de los grupos y la correspondencia se hace desde la herramienta de gestión de usuarios.

Utilizando el filtro Grupos LDAP se crean tres grupos que se recomienda tengan las siguientes propiedades:

Nombre de grupo	**Id de grupo (GID)**	**Nombre grupo Samba**	**RID (EN sambaSID)**
ntadmins	10000	Domain Admins	512
ntusers	10001	Domain Users	513
ntguests	10002	Domain Guests	514

El *nombre del grupo* y el *ID del grupo (GID)* se editan desde la propia ventana de creación/edición del grupo.

El nombre de grupo Samba se establece desde la pestaña Plug-in o Complementos, ejecutando el complemento *Administrar el atributo Samba de grupos LDAP*.

El RID son los últimos 5 dígitos del atributo *sambaSID*. Para editar el atributo *sambaSID* es necesario ejecutar el complemento *Editar atributos LDAP restantes*.

De esta forma se consigue que los grupos LDAP *ntadmins, ntusers y ntguests* correspondan a los grupos *Domain Admins, DomainUsers y Domain Guests* respectivamente en Samba, que son los habituales en entornos Windows. Para comprobar la correspondencia de grupos se puede utilizar el siguiente comando (como usuario root):

```
net groupmap list
```

Por último, es necesario asignar los privilegios necesarios al grupo *Domain Admins* (al igual que en la configuración de Samba con tdbsam) y que, de esta forma, puedan agregar máquinas al dominio:

```
net –S localhost –U root rpc rights grant "servidor\Domian Admins" SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege
```

5.4 Escenarios de entornos mixtos

Los escenarios posibles en cuanto al control de accesos son muy variados en función de las necesidades de la organización, la arquitectura empresarial definida, el modelo de infraestructura utilizado y los perfiles de las aplicaciones y usuarios.

Por una parte, y tomando como base la necesidad de implantar un sistema Single Sign-On (ver punto 5.1), podemos definir varios tipos de SSO que utilizarán un sistema de soporte a la gestión de identidades (IAM) que podrá ser: Active Directory, Samba, OpenLDAP, entre otros. En la figura 5-1 se muestra un esquema de integración de las diferentes partes.

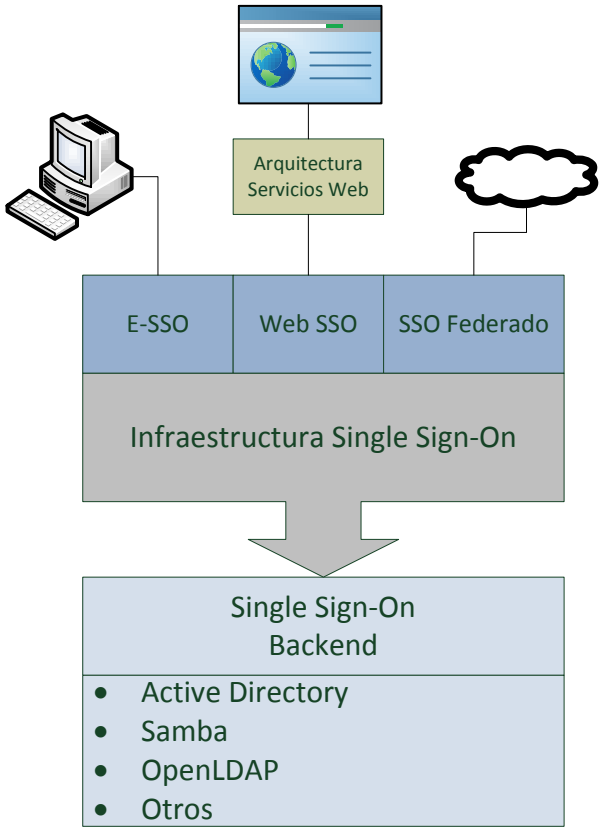


Figura 5-3: Escenarios Single Sign-on

El escenario objetivo de este proyecto es un **escenario empresarial,** que en términos de Single Sign-On denominaríamos E-SSO, donde existe una entidad encargada de centralizar la gestión de las identidades y autorizaciones, a la que los diferentes clientes (Windows, Linux) se conectan para poder acceder a los recursos de la red.

Por otra parte, tenemos que tener en cuenta las posibilidades de despliegue de la infraestructura (ver figura 5-4): centro de datos físico tradicional, modelo de computación en nube. En función del tipo de infraestructura, el proceso de auditoría posterior será diferente en cuanto a controles a considerar según las capas involucradas en el despliegue.

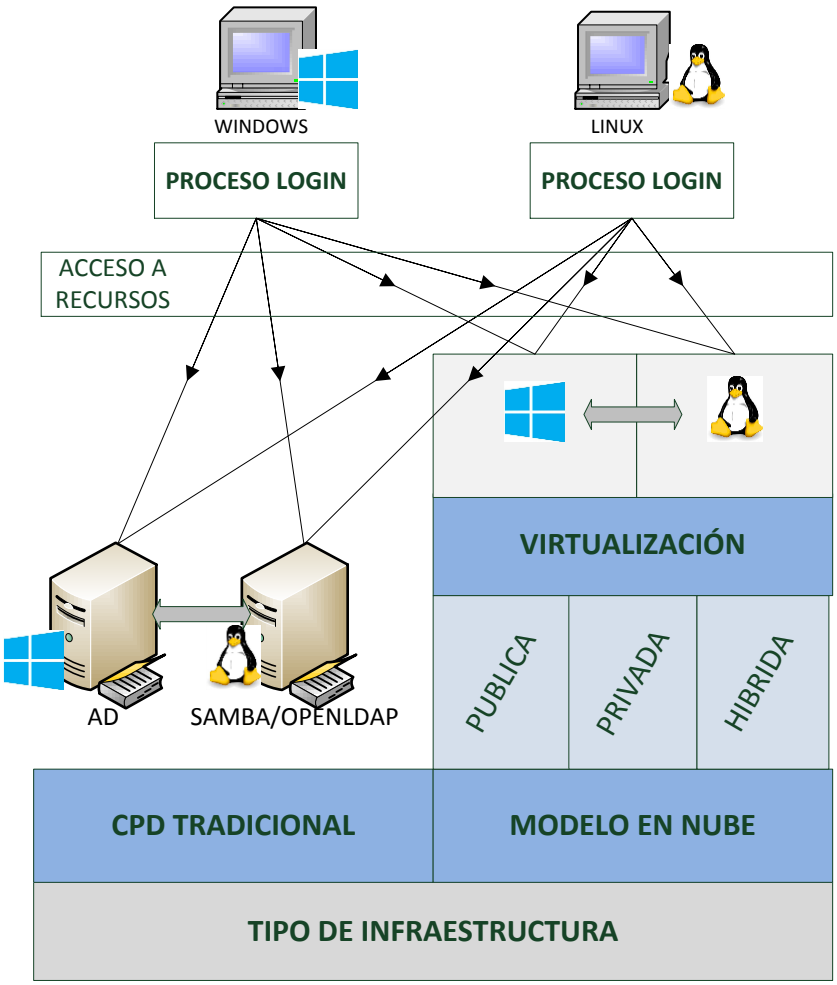


Figura 5-4: Escenarios de entornos mixtos

5.4.1 Integración de clientes Windows en servidor Active Directory

La integración de clientes Windows en un dominio de Active Directory no requiere configuraciones extra una vez el controlador está configurado, con la única salvedad de que es necesario añadir al cliente en el dominio para poder acceder a los sistemas de la red:

Autenticación

Es importante tener en cuenta la diferencia entre los métodos de autenticación: de forma **local** y sobre un **dominio**. Cuando la autenticación se hace sobre la propia máquina (de forma local) se utiliza siempre la base de datos de la cuenta SAM (*Single Account Manager*). Sin embargo, cuando la autenticación se hace sobre un dominio, el método de autenticación en Windows Server 2012 es por defecto Kerberos versión 5 (esto es así desde Windows Server 2003, en versiones anteriores la autenticación de clientes se realizaba con el protocolo NTLM – NT LAN Manager).

Como requisito previo para unirse a dominios Windows es necesaria una edición de cliente de Windows habilitada para ello. En función de la versión de Windows utilizada, podemos encontrar:

- **Windows 8 / 8.1**: ediciones Pro y Enterprise (las ediciones RT y para uso particular no permiten unirse a un dominio).
- **Windows 7**: ediciones Professional y Ultimate (las ediciones Starter y Home Premium no permiten unirse a un dominio).
- **Windows Vista**: ediciones Business y Ultimate (las ediciones Home Basic y Home Premium no permiten unirse a un dominio).
- **Windows XP**: edición Professional (la edición Home no está habilitada para unirse a dominios)

Con una edición de Windows válida, para cambiar el método de autenticación de tipo local a tipo dominio basta con:

- Tener configurada en Active Directory una cuenta de **usuario** y de **equipo** para tener acceso al dominio.
- Acceder de forma local al puesto cliente con una cuenta local con los permisos necesarios para realizar los cambios oportunos de unión al dominio.
- Localizar la pestaña de propiedades de nombre de equipo que se encuentra en: Panel de control – Sistema.
- Hacer clic sobre el botón “Cambiar” e introducir los valores oportunos en el campo “Dominio”. El sistema pide reiniciar el equipo, tras lo que ya se estará en condiciones de acceder al equipo utilizando una cuenta del dominio.

Acceso a recursos

El acceso a recursos y carpetas dentro del dominio es el propio de Active Directory y Windows, a través del Explorador de Archivos.

5.4.2. Integración de clientes Linux OpenSuse en servidor Active Directory

El objetivo de integrar sistemas Linux es que puedan ser clientes de un dominio del Directorio Activo como si fueran sistemas Windows miembros del dominio. Esto permite tener una única base de datos de usuarios y grupos con la posibilidad de iniciar sesión en cualquier sistema cliente (Windows y Linux), sin necesidad de tener cuentas de usuario locales en los clientes.

Históricamente, la integración de clientes Linux sobre dominios de Active Directory no es una tarea fácil para el administrador de sistemas, donde el punto fundamental a tener en cuenta es el método de autenticación a utilizar. De forma genérica, existen tres estrategias principales de autenticación que se pueden implantar en las máquinas clientes con Linux. No obstante, desde la aparición del método Winbind esta tarea se ha facilitado, aún más en OpenSuse donde existen opciones específicas para unir el sistema a Active Directory.

Utilizar autenticación LDAP

Esta estrategia es la más sencilla de implantar ya que sólo requiere configurar PAM para utilizar LDAP como método de autenticación. En la figura 5-5 se muestra el esquema básico de la integración.

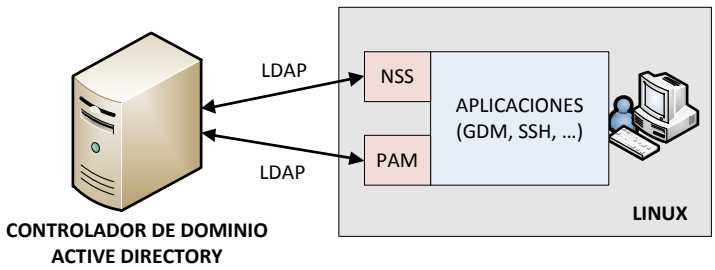


Figura 5-5. Integración cliente Linux en AD – Autenticación LDAP

Este método tiene una serie de características que ofrecen una serie de desventajas:

- Aunque Active Directory es un servicio LDAP, los clientes Windows utilizan Kerberos como método de autenticación (y no LDAP) por lo que en este caso es necesario realizar un enlace LDAP en Active Directory.
- La autenticación LDAP (LDAP binding) transmite el usuario y la contraseña en claro a través de la red. Esto se traduce en un método inseguro e inaceptable en la mayoría de los casos.
- Para mitigar el problema anterior se puede cifrar el canal de comunicación utilizando algún protocolo como SSL. Esto implica añadir carga administrativa al ser necesario gestionar los certificados SSL tanto en el Controlador de Dominio como en la máquina Linux.
- El módulo PAM LDAP no permite cambiar contraseñas reseteadas o caducadas.

Utilizar LDAP y Kerberos

Esta estrategia implica configurar PAM para utilizar Kerberos y NSS para que realice las búsquedas en LDAP. En la figura 5-6 se muestra el esquema básico de integración.

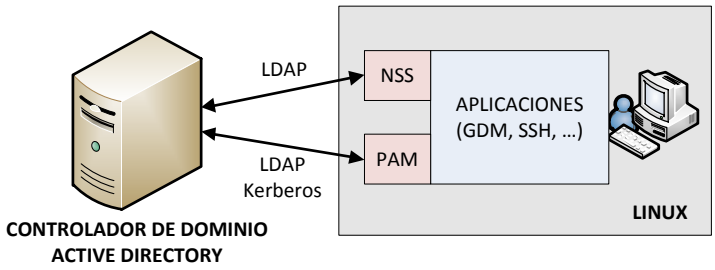


Figura 5-6. Integración cliente Linux en AD – Autenticación LDAP/Kerberos

Las características de este método de integración son las siguientes:

- Es un método más seguro que el anterior debido al uso de Kerberos.
- No tiene la ventaja de utilizar los registros publicados en Active Directory a través de DNS Service Location (SRV) en el Controlador de Dominio. Esto obliga a elegir un conjunto específico de controladores de dominio para la autenticación.
- No proporciona una manera muy intuitiva de administrar contraseñas de Active Directory caducadas.

Utilizar Winbind

Winbind es el servicio más importante ofrecido por Samba para la integración de sistemas Linux en dominios Active Directory.

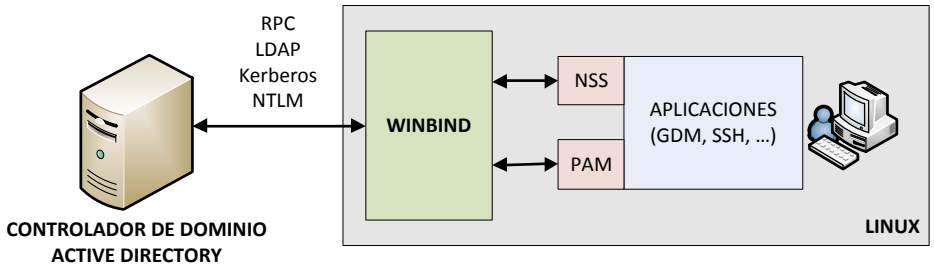


Figura 5-7. Integración cliente Linux en AD – Winbind

Winbind es un componente de la suite de interoperabilidad Samba que da solución al problema de unificación en el proceso de login entre Windows y Linux, debido a la diferencia en el método de autenticación nativo de cada sistema.

Winbind utiliza una implementación UNIX de las llamadas a procedimientos remotos de Microsoft (RPC), Pluggable Authentication Method (PAM) y Name Service Switch (NSS), para permitir a usuarios de dominios Windows NT y Active Directory estar presentes y operar como usuarios UNIX en máquinas UNIX. Tres son las bases de Winbind:

- Autenticación de credenciales de usuario a través de PAM. Esto hace posible hacer login en una máquina UNIX/Linux utilizando cuentas de usuarios y grupos Windows NT4 y/o Active Directory.
- Resolución de identidades a través de NSS. Se utiliza NSS para la resolución de los nombres de cuenta ya que es el método por defecto en una máquina Linux cuando no se usa Winbind.
- Mantiene una base de datos llamada *winbind_idmap.tdb* donde se almacenan las correspondencias entre los UIDs y GIDs de UNIX y los SIDs de Windows. Si se establece otro método de obtención de correspondencias (a través del parámetro de configuración "idmap backend") se ignora la base de datos local y se obtiene la información del sistema correspondiente.
- La importancia de implementar las llamadas a procedimientos remotos de Microsoft (MSRPC) radica en que estas llamadas se utilizan en entornos de red con sistemas Windows para realiza muchas operaciones importantes de interacción entre máquinas, como por ejemplo administración remota,

autenticación de usuarios, gestión de colas de impresión y cambio de contraseñas de usuarios.

Algunas de las características más importantes que ofrece Winbind son:

- Servicio/demonio que se ejecuta en clientes Samba. El demonio relacionado con winbind se llama *winbindd*.
- Actúa como proxy entre PAM-NSS y Active Directory
- Utiliza Kerberos como método de autenticación en Active Directory
- Utiliza LDAP como mecanismo para obtener información de usuarios y grupos.
- Ofrece habilidad para localizar controladores de dominio utilizando un algoritmo similar a DCLOCATOR en Active Directory.
- Ofrece habilidad para resetear contraseñas de Active Directory utilizando RPC
- Soluciona algunos problemas que no se solucionan utilizando simplemente Kerberos con PAM.

Configuración de Linux con Winbind

Para integrar clientes Linux OpenSuse en un dominio Active Directory hay que seguir una serie de pasos frecuentes en la máquina Linux. Se ha utilizado como sistema para los pasos a seguir un sistema OpenSuse, siendo fundamental el uso de la herramienta de configuración de esta distribución YAST.

Esta configuración funciona, al igual que un cliente Windows, siempre y cuando exista una cuenta de **equipo** en Active Directory así como los **usuarios** correspondientes que tendrán acceso al dominio desde la máquina Linux.

Software necesario

En OpenSuse es necesario instalar los paquetes *samba-winbind* y *krb5-client*. El primero, *samba-winbind*, es el paquete con la implementación de Winbind propiamente dicha, por lo que sin él es imposible la integración del cliente en Active Directory. El segundo paquete, *krb5-client*, es el paquete que permite a la máquina Linux funcionar como cliente dentro de un entorno Kerberos V.5. Debido a que Active Directory utiliza Kerberos V.5 como método de autenticación es también indispensable la existencia del paquete en la máquina Linux.

Configuración de red

Los ajustes de red se realizan desde la herramienta YAST, seleccionando dentro de la categoría *Dispositivos de red* la opción *Ajustes de red*.

- Configurar el direccionamiento IP para que esté acorde a la red donde se encuentra el dominio. Lo más adecuado en estos casos es utilizar direccionamiento estático, o en su defecto, utilizar un servidor DHCP bien gestionado donde se puedan asignar las direcciones IP a las direcciones físicas (MAC) de los equipos. La configuración de red se realiza desde las pestañas *Vista Resumen* y *Encaminamiento*.
- Configurar la resolución DNS de Linux. Debe estar configurado como servidor DNS el mismo servidor DNS que utiliza el controlador de dominio de Active Directory. En la mayoría de casos el servidor DNS es un controlador de dominio de Active Directory que además tiene el rol de servidor DNS. Esta configuración se realiza en la pestaña *Nombre de Host/DNS*.
- Configurar el nombre de equipo cualificado en el dominio (e.g. *maquinalinux.miuniversidad.com*), donde *maquinalinux* es el nombre de host y *miuniversidad.com* es el nombre del dominio. Esta configuración se realiza también en la pestaña *Nombre de Host/DNS*.

Configuración de la sincronización de tiempo

El protocolo Kerberos depende de que los sistemas de autenticación estén sincronizados (con un valor relativamente pequeño). Por tanto, es necesario configurar la máquina Linux para que use NTP (*Network Time Protocol*) ofrecido por un controlador de dominio. El Controlador de Dominio con NTP suele ser el principal con el rol FSMO (*Flexible Single Master Operations*).

Para configurar la máquina Linux como cliente NTP hay que acceder a la opción *Configuración de NTP* dentro de la categoría *Servicios de red* en YAST. Es necesario configurar el servicio para que inicie automáticamente al arrancar la máquina, además de añadir la sincronización de tipo *servidor* en la tabla de sincronizaciones.

Configuración de NSS, PAM y Kerberos.

La configuración de los módulos NSS, PAM y Kerberos con Winbind se realiza de forma sencilla a través de la herramienta *Pertenencia a dominio de Windows* dentro de la categoría *Servicios de red* en YAST.

Sólo es necesario introducir el nombre de dominio en el campo correspondiente (por ejemplo miuniversidad.com) y seleccionar la opción *Usar también la información SMB para la autenticación de Linux*, además de las opciones:

- *Crear el directorio home del usuario (home) al iniciar sesión*, lo que generará una carpeta nueva en el directorio *home* de la máquina por cada usuario del dominio que acceda a la máquina.
- *Autenticación sin conexión*, lo que permite que un usuario del domino pueda acceder a la máquina aún sin conexión a Active Directory.

La configuración de pertenencia a dominio de Windows realiza cambios principalmente en los siguientes ficheros de configuración:

- /etc/nsswitch.conf
- /etc/samba/smb.conf
- /etc/krb5.conf
- /etc/pam.d/samba
- /etc/pam.d/common-account
- /etc/pam.d/common-auth
- /etc/pam.d/common-password
- /etc/pam.d/session

Configuración de Active Directory

Para solucionar el problema de incompatibilidad de identificadores y para extender el alcance local de los identificadores de usuario en los entornos Linux, se suele utilizar tanto NIS como un directorio LDAP compartido. Por tanto, es posible utilizar Active Directory (que soporta LDAP) para este propósito, existiendo dos posibles estrategias de implantación:

A. Directory ID mapping

Crear un UID para cada usuario y grupo, y almacenar el identificador con su objeto correspondiente en Active Directory. De esta forma, cuando Winbind autentica un usuario, puede buscar el UID del usuario y suministrarlo a Linux como el identificador interno del usuario. A este tipo de esquema se le llama *Directory ID mapping* o idmap_ad.

No obstante, existe un problema relacionado con esta estrategia ya que es necesario proveer un mecanismo para asegurar que cada usuario y grupo tienen un identificador y que son únicos en un bosque de Active Directory. Por tanto, es necesario realizar modificaciones en Active Directory, concretamente, adaptar el esquema para poder trabajar con los atributos que Winbind utiliza para almacenar la información. Estos cambios se pueden hacer utilizando las herramientas Microsoft Services for UNIX. A partir de Windows Server 2003, y por evolución en Windows Server 2012 este paquete de herramientas vienen integradas en el sistema operativo por lo que sólo es necesario instalar servidor NIS para habilitar la pestaña "Atributos UNIX" en las propiedades de los objetos de Active Directory. El componente que habilita estas propiedades se llama "Identity Management for UNIX", dentro de los servicios de Active Directory. Una vez configurado el esquema, hay que proporcionar identificadores Linux a todos los usuarios (y sus grupos correspondientes) que vayan a logarse en la máquina Linux, lo que se traduce en definir valores para las propiedades uidNumber y gidNumber.

Para configurar esta estrategia de correspondencia en Winbind es necesario editar el fichero */etc/samba/smb.conf* añadiendo la línea "`idmap backend = ad`".

B. RID mapping

La segunda estrategia se sirve de la posibilidad que tiene Windows de identificar unívocamente al usuario dentro de un dominio así como al dominio en sí mismo a través del SID. La parte del SID que identifica unívocamente al usuario dentro del dominio es el identificador relativo (*Relative Identifier* o RID) (ver punto 5.2.7). De esta forma, Winbind puede simplemente extraer el RID del SID cuando un usuario realiza el acceso al sistema, y utilizar el RID como el identificador interno UID. A esta estratega se la denomina como RID mapping o idmap_rid.

El mapeo a través de RID tiene la ventaja de que no requiere tareas administrativas extras, aunque no se puede utilizar en entornos con varios dominios debido a la probabilidad de que los usuarios en diferentes dominios tengan el mismo valor de RID, siendo la opción más adecuada en entornos de dominio único de Active Directory.

Para utilizar esta estrategia de correspondencia, es necesario introducir la línea "`idmap backend = rid`" en el fichero de configuración */etc/samba/smb.conf*.

Por otra parte, aunque se configura PAM para crear el directorio "home" de cada usuario, es necesario que Winbind conozca dicho directorio. Esto se consigue añadiendo la línea "template homedir = /home/%U" en el fichero smb.conf.

C. Intervalos de ID en OpenSuse

Existe una alternativa a las opciones anteriores y es que sea la máquina cliente Linux la que gestione los identificadores de usuarios y grupos. Este es el método por defecto al configurar una máquina OpenSuse con pertenencia a dominio Windows. Se puede acceder a esta configuración en *Configuración Avanzada* dentro de la herramienta de *Pertenencia a dominio de Windows*. Ajustar párrafo a ambos lados

Al utilizar este método se establecen los valores mínimo y máximo de los identificadores que tendrán los usuarios y grupos al acceder a la máquina con un usuario del dominio. Por defecto estos valores son:

- Intervalo de UID: Valor mínimo 10000. Valor máximo 20000.
- Intervalo de GID: Valor mínimo 10000. Valor máximo 20000

Los efectos sobre el fichero de configuración *smb.conf* son que el método de mapeo se establece de la siguiente forma:

```
idmap gid = 10000-20000
idmap uid = 10000-20000
```

En lugar de

```
idmap backend = ad o idmap backend = rid
```

Es importante tener en cuenta que esta estrategia de mapeo de identificadores es gestionada en la máquina local, por lo que si se tiene un número elevado de clientes

Linux la tarea de administración de los identificadores se multiplica, mientras que con las estrategias anteriores la administración de la correspondencia de identificadores está centralizada.

Acceso a recursos compartidos

Existen tres alternativas para compartir recursos entre máquinas dentro de entornos heterogéneos, aunque la más utilizada es la relacionada con Winbind, debido a su uso en la autenticación.

- Utilizando un servidor de directorios personales Linux entre los clientes Linux y el Directorio Activo. Implica que dicho servidor debe ser a su vez cliente de autenticación sobre el Directorio Activo. El protocolo utilizado entre los clientes Linux y el servidor de directorios Linux es NFS.
- Utilizando el protocolo NFS entre el Directorio Activo y los clientes Linux. Para esto es necesario tener instalado Windows Services for Unix en el servidor del Directorio Activo y administrar NFS dentro del mismo.
- Utilizando el protocolo SMB entre el cliente Linux y el Directorio Activo, para lo que es necesario que la máquina cliente esté configurada como cliente Samba. Este método es el utilizado cuando se configura Linux para el uso de Winbind.

Se pueden montar carpetas del directorio de forma permanente desde la *Configuración Avanzada* de la herramienta *Pertenencia a dominio de Windows*, donde se puede gestionar una tabla con directorios montados en la máquina.

Además, un usuario puede compartir sus directorios de la máquina Linux, seleccionando la opción *Permitir a los usuarios compartir sus directorio*s dentro de la herramienta *Pertenencia a dominio de Windows*, permitiendo incluso acceso a invitados que no tengan credenciales concretas en el dominio.

5.4.3. Integración de clientes Windows en servidor Samba

El proceso para ingresar máquinas Windows en un dominio configurado en Samba es el mismo que para añadirlas a un dominio de Active Directory No se debe olvidar que el nombre de máquina debe existir como cuenta en el servidor Samba para poder unirla al dominio.

El proceso para unir una máquina Windows 8.1 es sencillo: dese el botón *Inicio* (botón derecho) – *Sistema*. En la sección "Configuración de n*ombre, dominio y grupo de trabajo del equipo"* pulsar sobre el botón "*Cambiar* configuración" e introducir el nombre del dominio correspondiente (en lugar de utilizar un grupo de trabajo).

5.4.4. Integración de clientes Linux OpenSuse en servidor Samba

Unir una máquina Linux a un dominio definido en Samba es igual que unir el cliente Linux a un dominio Active Directory (ver apartado 5.4.2) utilizando Winbind. Para ello, se realiza la unión fácilmente desde la herramienta *Pertenencia a dominio de Windows* en la categoría *Servicios de red* de *YAST*.

No hay que olvidar que este proceso necesita el paquete de software *samba-winbind*.

Lo más importante es introducir el nombre de dominio, deshabilitar el inicio de sesión automático cuando el asistente lo solicita y seleccionar las opciones:

- Usar también la información SMB para la autenticación de Linux.
- Crear el directorio del usuario (home) al iniciar sesión.
- Autenticación sin conexión.
- Single-Sign-On para SSH.

6 Auditoría en Entornos Mixtos

6.1 Identificación del caso práctico

Como hemos visto en los capítulos anteriores, el número de escenarios posibles en cuanto a entornos mixtos se refiere y posibles sistemas de gestión de la identidad es elevado, dependiendo del tipo de empresa, necesidades asociadas y arquitectura seleccionada para el despliegue de la tecnología.

A continuación se propone un escenario hipotético para el que se definirá la guía de auditoría en los puntos siguientes.

La compañía Data Destiny desarrolla su actividad en el sector de las TIC. Desarrolla productos y servicios para clientes que necesitan procesar gran cantidad de datos para extraer información relevante y conocimiento sobre los mercados en los que operan. La compañía se creó en 2002 en Madrid, y debido a la eclosión que está teniendo el mundo Big Data desde hace unos años su volumen de ventas de productos y servicios se ha incrementado un 10% anual.

En 2010 se inauguraron nuevas sedes de la compañía en Bilbao y Sevilla, y en 2015 tiene previsto abrir otra sucursal en Londres. La empresa cuenta con departamento de: Recursos Humanos, Comercial, Servicios Profesionales, Desarrollo y Soporte. Data Destiny cuenta con 84 empleados:

- 61 en Madrid
- 14 en Bilbao
- 9 en Sevilla

Aunque la mayoría de los empleados utilizan puestos de trabajo con sistema operativo Windows 8.1, en los departamentos de desarrollo y soporte existen equipos que utilizan sistemas Linux (Suse) con el fin de desarrollar con más eficacia productos de calidad acorde a las tecnologías asociadas a Big Data, que en su mayoría se basan en sistemas Linux.

A raíz de la crisis económica, Data Destiny ha planteado una estrategia de reducción de gastos e incremento de la productividad en paralelo. Para ello ha identificado como requisitos:

- Necesidad de flexibilidad y escalabilidad debido a la previsión de una demanda variable de sus productos y servicios.
- Servicios de TI efectivos y de calidad.

- Alto compromiso con la seguridad de la información.
- Cumplimiento con principales estándares metodológicos y buenas prácticas.

Para satisfacer estos requisitos, la empresa plantea un plan global de migración a medio plazo de la infraestructura física a un modelo de computación en la nube (P2V, *Physical to Virtual*), que afecta a diferentes servicios y aplicaciones como: correo electrónico, aplicaciones de oficina, contabilidad y nóminas, gestión de proyectos, gestión de clientes y gestión de identidad.

Para facilitar y suavizar el cambio, y permitir una evaluación y control del mismo, se plantea una migración dividida en varias fases. Con el fin de minimizar los riesgos iniciales asociados al punto de acceso a la red corporativa, la primera fase implicará la migración del sistema de gestión de identidades (Active Directory 2012) a un modelo IaaS de nube privada, ofrecido por el proveedor Isure Inc.

La situación actual es que una vez que la empresa ha finalizado la fase 1 de su plan global de migración, solicita una auditoría del sistema de gestión de identidad para comprobar su grado de rendimiento y eficacia, de tal forma que los resultados ayuden a decidir sobre la continuidad en el desarrollo de las siguientes fases de su plan global de migración.

Para ello, Data Destiny contrata los servicios de RAA Experts, una empresa formada por profesionales de TI con dilatada experiencia, dedicada a proyectos de auditoría y consultoría de las TIC, para que lleve a cabo un proyecto de auditoría sobre su actual entorno mixto cuyo sistema de gestión de identidades es Active Directory. La empresa RAA Experts propone una auditoría basada en la guía expuesta en los puntos 6.2 y 6.3.

6.2 Fase 1. Planificación y alcance de auditoría

La primera fase del proyecto de auditoría implica básicamente realizar la planificación y definición del alcance. Las tareas de esta fase son comunes a cualquier proyecto de auditoría y se plasman en un documento de propuesta de auditoría que puede servir como compromiso comercial entre las partes según la tabla 6-1.

TAREA	DESCRIPCIÓN
PA1	Definir objetivos de la auditoría a alto nivel
PA2	Definir límites de la auditoría
PA3	Identificar y documentar riesgos
PA4	Definir proceso de cambios en la auditoría: • Identificar responsable de la revisión • Establecer proceso de notificación de mejoras e implementación de cambios
PA5	Definir hitos y métricas de éxito de las fases del proceso de auditoría
PA6	Definir recursos necesarios: • Determinar habilidades necesarias para la auditoría • Herramientas de reporting de Active Directory • Permisos de acceso
PA7	Definir entregables
PA8	Comunicación entre las partes

Tabla 6-1. Tareas de planificación y alcance de auditoría

Las tareas PA1 y PA2 determinan las acciones a llevar a cabo en el resto de tareas. Según el caso descrito en el punto 6.1, los límites de la auditoría definidos en la tarea P2 vienen determinados por la arquitectura y el diseño de Active Directory. Para obtener una buena definición de los límites serán necesarias las siguientes sub-tareas expuestas en la tabla 6-2:

SUBTAREA	SUBTAREAS DEFINICIÓN LÍMITES DE AUDITORÍA
PA2.1	Obtener una descripción de los entornos de computación en la nube en uso
PA2.2.	Identificar el tipo de servicio en nube (en este caso IaaS) y determinar los servicios a incluir en la revisión: AD DS, AD LDS, AD FS...

PA2.3	Obtener documentación de diseño de Active Directory
PA2.4	Obtener y revisar la topología de Active Directory
PA2.5	Determinar si se incluye en la auditoría un bosque completo o un subconjunto de dominios
PA2.6	Obtener y revisar las políticas de seguridad e informes de auditoría previos si existen.

Tabla 6-2. Sub-tareas para la definición de límites de auditoría

De forma genérica, y fuera del ámbito del caso práctico propuesto, las actividades que pueden llevarse a cabo en la tarea PA2 dependerán del escenario al que nos enfrentemos (ver punto 5.4), y para ello las consideraciones a tener en cuenta serán:

- Tipo de infraestructura:
  - CPD tradicional: En este caso será muy importante tener en cuenta la seguridad física de los activos de información.
  - Modelo de computación en la nube: será necesario revisar todos los elementos relacionados con la prestación de servicios: gobernanza, gestión de riesgos, gestión con terceras partes, cumplimiento legal y certificaciones del prestador de servicios, informes de auditoría, portabilidad de los servicios, respuesta a incidentes, seguridad de los datos, gestión de accesos y compromiso de controles en la virtualización.
- Arquitectura de Single Sign-On elegida y tecnología subyacente que la soporte: federación de identidades, Active Directory, Samba, OpenLDAP, etc.

6.3 Fase 2. Auditoría del Sistema de Gestión de Identidades

La utilización de técnicas clásicas en la realización de auditorías es muy habitual, ya que complementan muy bien el trabajo del auditor y su criterio. A continuación se plantea un cuestionario que puede servir al desarrollo de los trabajos de auditoría de un Sistema de Gestión de Identidades, en este caso particular Active Directory en las condiciones de despliegue del caso práctico descrito en el punto 6.1.

Podemos dividir la guía en varias secciones para facilitar su utilización:

- Gestión de Active Directory
- Diseño de Active Directoy
- Seguridad en los Controladores de Dominio
- Configuración de políticas de dominio
- Configuración de políticas de controlador de dominio

La seguridad física está fuera del alcance de esta guía ya que el escenario es un modelo IaaS de nube privada albergada en el proveedor de servicios, que será el encargado de la infraestructura. No obstante, será importante establecer controles para revisar el complimiento de los posibles niveles de servicios comprometidos (*SLAs, Service Level Agreement*).

En las siguientes tablas-guías podemos observar que la última columna (VAL) hace referencia a un VALOR. El objetivo es dejar al auditor decidir el tipo de valores que quiere utilizar a la hora de evaluar los diferentes puntos. En general pueden existir dos conjuntos de valores:

- SI / NO
- Valores numéricos en función del nivel de control determinado por el auditor. Esto puede ayudar en el futuro para consolidar los valores de las cuestiones y obtener un valor global que pueda verificarse según una escala de niveles y posibles pesos asociados a las cuestiones. De esta forma se podría buscar un mecanismo de automatización para el proceso de auditoría.

6.3.1 Gestión de Active Directory

CUESTIÓN	DESCRIPCIÓN	VAL
CA1.1	Existe un responsable o grupo responsable que gestiona todo lo relativo a Active Directory, y una adecuada separación de funciones.	
CA1.2	Se han identificado los responsables de: • Establecer la política de Active Directory • Controladores de dominio • Administración del servicio • Administración de los datos • Dominio raíz • Administradores de empresa • Administradores de esquemas • Administradores de dominios • Arquitectura de información • Propietarios de bosques	
CA1.3	El personal de seguridad de la información participa en las actividades y monitorización de Active Directory.	
CA1.4	Existe un plan de gestión de riesgos de Active Directory que forma parte del plan de gestión de riesgos global	
CA1.5	Existe una revisión periódica de cuentas para limpiar cuentas obsoletas o cambios en los derechos de acceso a recursos	

Tabla 6-3. Cuestionario sobre Gestión de Active Directory

6.3.2 Diseño de Active Directory

CUESTIÓN	DESCRIPCIÓN	VAL
CA2.1	El diseño de Active Directory cumple con los objetivos de seguridad y aplica buenas prácticas de diseño	
CA.2.1.1	Existe una política genérica para el dominio, con configuraciones de seguridad del dominio en general que no incluye configuraciones para equipos y usuarios.	
CA2.1.2	Existe una OU con una política asociada con las configuraciones de seguridad base para todos los controladores de dominio.	
CA2.1.3	Existe una OU con una política asociada con las configuraciones de seguridad base para todos los servidores miembros que nos son controladores de dominio.	
CA2.1.4	Existe una política para cada tipo de rol de servidor en la organización (servidor DCHP, servidor de archivos, servidor de impresión, etc). Hay que tener en cuenta que si existen servidores con varios roles, es recomendable crear una OU para la combinación y aplicar los GPO de cada tipo de rol a la OU resultante. La unificación de roles en un mismo servidor requiere una buen planificación y pruebas exhaustivas para comprobar que no interfiere la seguridad de un rol con la seguridad de otro rol.	
CA2.1.5	Existen políticas adicionales para implementar la seguridad de los equipos o puestos de trabajo y para los usuarios.	

CA2.2	El rol de servidor del controlador de dominio es el único habilitado y sólo se incluyen características de Active Directory y DNS.	
CA2.3	Se han establecido relaciones de confianza entre bosques	
CA2.4	Las peticiones de relaciones de confianza entre bosques están controladas y gestionadas a través de procesos administrativos; y asignadas al responsable de la gestión.	
CA2.5	No existen miembros de otros bosques como miembros de grupos con capacidades de administración.	

CA2.6	Los clientes Linux utilizan Samba (Winbind) como mecanismo de autenticación al sistema ("Pertenencia a dominio de Windows"), con las opciones de configuración:
	• Usar información SMB para autenticación de Linux
	  ○ Crear el directorio home al iniciar sesión
	  ○ Autenticación sin conexión
	  ○ Single Sign-On para SSH	

CA2.7	Los clientes Linux utilizan un suministrador de identificadores centralizado, en /etc/samba/smb.conf: • "`idmap backend = ad`" → Están instaladas las utilidades Microsoft Services for Unix en el controlador de dominio, modificado el esquema de directorio y asignado UIDs y GIDs a los usuarios. • "`idmap backend = rid`" → Sólo válido si el dominio es único	
CA2.8	El despliegue del controlador de dominio se ha realizado en modo Server Core.	
CA2.9	Se utilizan controladores RODC si la seguridad del servidor no está garantizada.	
CA2.10	Si se utilizan controladores RODC, se limita la información de seguridad almacenada en ellos.	
CA2.11	Existe un listado de parches de seguridad y se han aplicado a todos los servidores.	

Tabla 6-4. Cuestionario sobre diseño de Active Directory

6.3.3 Seguridad en los Controladores de Dominio

CUESTIÓN	DESCRIPCIÓN	VAL
CA3.1	Existe un SLA con el proveedor de IaaS que describe los incidentes de seguridad, eventos y acciones a realizar en su caso, junto con la definición de las responsabilidades.	
CA3.2	Existe un SLA con el proveedor de servicios que garantiza la seguridad física de la infraestructura.	
CA3.3	El procedimiento de instalación y puesta en marcha de los controladores de dominio está documentado, de manera que sea un proceso repetible con opciones de configuración aprobadas.	
CA3.4	Existe software antivirus instalado y actualizado en todos los controladores de dominio; y se realizan análisis periódicos en busca de malware.	
CA3.5	La política definida para los controladores de dominio sólo permite la ejecución de scripts firmados por parte de administradores.	

CA3.6	La configuración del controlador de dominio cumple los siguientes requisitos: • Todas las unidades formateadas con tipo NTFS • Sólo se permiten los protocolos de nivel de transporte TCP/IP. • Protocolo SMTP deshabilitado Servicios deshabilitados: • Distributed Link Tracking Client • Fax • Internet Information Services • Indexing Service • Portable Media Serial Number Service • Shell Hardware Detection • SMTP • Special Administrator Console Helper • Upload Manager • Utility Manager • Windows Audio Servicios habilitados (además de los correspondientes al rol de controlador de dominio): • IPSec • Netlogon • NTLM Security Support Provider • Plug and Play • Remote Procedure Call • Security Account Manager • Server • Windows Installer • Windows Management Instrument • Windows Time • Cryptographic Services • DHCP Client • DNS Client • DNS Server • Event Log	

Tabla 6-5. Cuestionario sobre Seguridad en los Controladores de Dominio

6.3.4 Configuración de políticas de dominio

<table>
<tr><th>CUESTIÓN</th><th>DESCRIPCIÓN</th><th>VAL</th></tr>
<tr><td>CA4.1</td><td>Definición de la política de contraseñas como sigue (o similar):
<table><tr><td>Almacenar contraseñas con cifrado reversible</td><td>Desactivado</td></tr><tr><td>Exigir historial de contraseñas</td><td>24 contraseñas</td></tr><tr><td>La contraseña debe cumplir los requisitos de complejidad</td><td>Activado</td></tr><tr><td>Longitud mínima de la contraseña</td><td>7 caracteres</td></tr><tr><td>Vigencia máxima de la contraseña</td><td>42 días</td></tr><tr><td>Vigencia mínima de la contraseña</td><td>1 día</td></tr></table></td><td></td></tr>
<tr><td>CA4.2</td><td>Definición de la política de bloqueo de cuenta como sigue:
<table><tr><td>Duración del bloqueo de cuenta</td><td>No definido</td></tr><tr><td>Restablecer el bloqueo de cuenta después de</td><td>No definido</td></tr><tr><td>Umbral de bloqueo de cuenta</td><td>0</td></tr></table></td><td></td></tr>
<tr><td>CA4.3</td><td>Definición de la política de Kerberos como sigue:
<table><tr><td>Aplicar restricciones de inicio de sesión de usuario</td><td>Activado</td></tr><tr><td>Tolerancia máxima para la sincronización de los relojes de los equipos</td><td>5 minutos</td></tr><tr><td>Vigencia máxima de renovación de vales de usuario</td><td>7 días</td></tr><tr><td>Vigencia máxima del vale de servicio</td><td>600 minutos</td></tr><tr><td>Vigencia máxima del vale de usuario</td><td>10 horas</td></tr></table></td><td></td></tr>
</table>

Tabla 6-6. Cuestionario sobre configuración de políticas de dominio

** Valores tomados como referencia de [60]

6.3.5 Configuración de políticas de controlador de dominio

<table>
<tr><th>CUESTIÓN</th><th>DESCRIPCIÓN</th><th>VAL</th></tr>
<tr><td colspan="3">Políticas de contraseñas</td></tr>
<tr><td>CA5.1</td><td>Definición de la política de los derechos de usuario como sigue:

<table><tr><td>Agregar estaciones de trabajo al dominio</td><td>Administradores</td></tr><tr><td>Permitir el inicio de sesión local</td><td>Administradores</td></tr><tr><td>Permitir inicio de sesión a través de Terminal Services</td><td>Administradores</td></tr><tr><td>Cambiar la hora del sistema</td><td>Administradores</td></tr><tr><td>Cargar y descargar controladores de dispositivo</td><td>Administradores; Operadores</td></tr><tr><td>Restaurar archivos y directorios</td><td>Administradores; Operadores</td></tr><tr><td>Apagar el sistema</td><td>Administradores</td></tr><tr><td>Depurar los programas</td><td>Revocar todos</td></tr><tr><td>Denegar el acceso a este equipo desde la red</td><td>Denegar a todos excepto administradores y usuarios autenticados</td></tr></table></td><td></td></tr>
<tr><td>CA5.2</td><td>Definición de la política para las opciones de seguridad como sigue:
<table><tr><td>Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña</td><td>Activado</td></tr><tr><td>Dispositivos: permitir dar formato y expulsar los medios extraíbles</td><td>Administradores</td></tr><tr><td>Dispositivos: evitar que los usuarios instalen los controladores de la impresora</td><td>Activado</td></tr><tr><td>Dispositivos: comportamiento de la instalación del controlador no firmado</td><td>Advertir, pero permitir instalación</td></tr><tr><td>Miembro de dominio: cifrar digitalmente los datos de canal seguro (cuando sea posible)</td><td>Activado</td></tr><tr><td>Miembro de dominio: desactivar cambios de contraseña de la cuenta de la máquina</td><td>Desactivado</td></tr><tr><td>Miembro de dominio: tiempo máximo de la contraseña en la</td><td>30 días</td></tr></table></td><td></td></tr>
</table>

cuenta de la máquina	
Miembro de dominio: requerir una clave de sesión sólida	Activado
Inicio de sesión interactiva: no mostrar el nombre del último usuario	Activado
Inicio de sesión interactiva: no requerir CTRL+ALT+SUPR	Desactivado
Inicio de sesión interactiva: indicar al usuario cambiar la contraseña antes de su vencimiento	14 días antes
Inicio de sesión interactiva: se requiere de la autenticación del DC para desbloquear la estación de trabajo	Activado
Inicio de sesión interactiva: comportamiento de eliminación de la tarjeta inteligente	Bloquear estación de trabajo
Cliente de red Microsoft: firmar digitalmente las comunicaciones	Activado
Cliente de red Microsoft: enviar una contraseña no cifrada a servidores SMB de terceros	Desactivado
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Activado
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente está de acuerdo)	Activado
Servidor de red Microsoft: desconectar clientes cuando venza el tiempo de inicio de sesión	Activado
Acceso a la red: no permitir la enumeración anónima de las cuentas SAM	Activado
Acceso a la red: no permitir la enumeración anónima de las cuentas y usos compartidos SAM	Activado
Acceso a la red: no permitir el almacenamiento de credenciales o .NET Passports para la autenticación de la red	Activado
Acceso a la red: permitir que los permisos de todos se	Desactivado

	apliquen a los usuarios anónimos	
	Acceso a la red: tuberías nombradas a las que se puede acceder de manera anónima	Ninguno
	Acceso a la red: restringir el acceso anónimo a las tuberías y usos compartidos nombrados	Activado
	Acceso a la red: usos compartidos a los que se puede acceder de manera anónima	Ninguno
	Acceso a la red: modelo de uso compartido y de seguridad para las cuentas locales	Los usuarios locales se autentican como ellos mismos
	Seguridad de la red: no almacenar el valor hash del Administrador LAN en el siguiente cambio de contraseña	Activado
	Seguridad de la red: nivel de autenticación del administrador LAN	Envía sólo la respuesta NTLMv2 / Rechazar LM
	Seguridad de la red: requisitos para firmar el cliente LDAP	Negociar firma
	Seguridad de la red: seguridad mínima de la sesión para los clientes en SSP de NTLM (incluyendo RPC seguros)	Todas las configuraciones están activadas
	Seguridad de la red: seguridad mínima de la sesión para los servidores en SSP de NTLM (incluyendo RPC seguros)	Todas las configuraciones están activadas
	Apagado: permitir al sistema apagarse sin tener que iniciar una sesión	Desactivado
	Apagado: eliminar el archivo de página de la memoria virtual	Desactivado
	Criptografía del sistema: obligar una protección de clave sólida para las claves del usuario almacenadas en el PC	Se indica al usuario cuando se utiliza la clave por primera vez
	Criptografía del sistema: utilizar los algoritmos que cumplen con FIPS para cifrado, operaciones hash y firma	Desactivado
CA5.3	Definición de la política de **registro de sucesos** como sigue:	

Tamaño máximo del registro de las aplicaciones	No definido
Tamaño máximo del registro de seguridad	131.072 KB
Tamaño máximo del registro del sistema	No definido
Evitar que el grupo de invitado local acceda al registro de las aplicaciones	Activado
Evitar que el grupo de invitado local acceda al registro de seguridad	Activado
Evitar que el grupo de invitado local acceda al registro del sistema	Activado
Método de retención para el registro de las aplicaciones	Según se necesite
Método de retención para el registro de seguridad	Según se necesite
Método de retención para el registro del sistema	Según se necesite

Tabla 6-7. Cuestionario sobre configuración de políticas de controlador de dominio

** Valores tomados como referencia de [60]

6.3.6 Configuración de la política de auditoría

En un entorno de red con un controlador de dominio y donde existen muchos usuarios con acceso a los sistemas los tipos de sucesos o eventos más comunes para auditar son:

- Acceso a objetos (archivos, carpetas).
- Administración de cuentas de usuario y grupos.
- Inicio y finalización de sesiones de usuario.

En el proceso de definición de la auditoría es necesario especificar las categorías de eventos a auditar, así como definir el tamaño y comportamiento del registro de auditoría. En Active Directory existen nueve categorías cuya configuración se establece utilizando la administración de directivas de grupo en: Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Directiva de auditoría:

- Auditar el acceso a objetos
- Auditar el acceso del servicio de directorio

- Auditar el cambio de directivas
- Auditar el seguimiento de procesos
- Auditar el uso de privilegios
- Auditar eventos de inicio de sesión
- Auditar eventos de inicio de sesión de cuenta
- Auditar eventos del sistema
- Auditar la administración de cuentas

No obstante, se puede hacer una administración más precisa de las directivas de auditoría ya que se dividen en 50 subcategorías. En Windows Server 2012 (y 2008) la administración de las subcategorías no se puede hacer utilizando la herramienta de administración de directivas de grupo sino que es necesario el uso de la herramienta Auditpol. Independientemente de la forma de administrar las subcategorías, los valores recomendados por Microsoft (en términos de su evento tiene éxito, fallo o ambos) en un servidor que realiza las funciones de controlador de dominio son los siguientes.

<table>
<tr><th>CUESTIÓN</th><th>DESCRIPCIÓN</th><th>VAL</th></tr>
<tr><td>CA6.1</td><td>Categoría: Sistema
<table>
<tr><td>Extensión del sistema de seguridad</td><td>Éxito / Fallo</td></tr>
<tr><td>Integridad del sistema</td><td>Éxito / Fallo</td></tr>
<tr><td>Controlador IPSec</td><td>Éxito / Fallo</td></tr>
<tr><td>Otros eventos del sistema</td><td>No auditar</td></tr>
<tr><td>Cambio de estado de seguridad</td><td>Éxito / Fallo</td></tr>
</table></td><td></td></tr>
<tr><td>CA6.2</td><td>Categoría: Inicio / Cierre de sesión
<table>
<tr><td colspan="2">Categoría: Inicio / Cierre de sesión</td></tr>
<tr><td>Inicio de sesión</td><td>Éxito</td></tr>
<tr><td>Cerrar sesión</td><td>Éxito</td></tr>
<tr><td>Bloqueo de cuenta</td><td>No auditar</td></tr>
<tr><td>Modo principal de IPSec</td><td>No auditar</td></tr>
<tr><td>Modo rápido de IPSec</td><td>No auditar</td></tr>
<tr><td>Modo extendido de IPSec</td><td>No auditar</td></tr>
</table></td><td></td></tr>
</table>

	Inicio de sesión especial	Éxito
	Otros eventos de inicio y cierre de sesión	No auditar
	Servidor de directivas de redes	No auditar
CA6.3	Categoría: **Acceso a objetos**	
	Sistema de archivos	No auditar
	Registro	No auditar
	Objeto del núcleo	No auditar
	SAM	No auditar
	Servicios de certificación	No auditar
	Aplicación generada	No auditar
	Manipulación de identificadores	No auditar
	Recurso compartido de archivos	No auditar
	Colocación de paquetes de Filtering Platform	No auditar
	Conexión de Filtering Platform	No auditar
	Otros eventos de acceso a objetos	No auditar
CA6.4	Categoría: **Uso de privilegios**	
	Uso de privilegio confidencial	No auditar
	Uso de privilegio no confidencial	No auditar
	Otros eventos de uso de privilegio	No auditar
CA6.5	Categoría: **Seguimiento detallado**	
	Finalización del proceso	No auditar
	Actividad DPAPI	No auditar
	Eventos de RPC	No auditar
	Extracción del proceso	Éxito

CA6.6 Categoría: **Cambio de plan de directivas**

Cambio en la directiva de auditoría	Éxito / Fallo
Cambio en la directiva de autenticación	Éxito
Cambio en la directiva de autorización	No auditar
Cambio en la directiva del nivel de reglas de MPSSVC	No auditar
Cambio en la directiva de Filtering Platform	No auditar
Otros eventos de cambio de directivas	No auditar

CA6.7 Categoría: **Administración de cuentas**

Administración de cuentas de usuario	Éxito
Administración de cuentas de equipo	Éxito
Administración de grupos de seguridad	Éxito
Administración de grupos de distribución	No auditar
Administración de grupos de aplicaciones	No auditar
Eventos de administración de cuentas	Éxito

CA6.8 Categoría: **Acceso al servicio de directorio**

Cambios de servicio de directorio	Éxito
Replicación de servicio de directorio	Éxito
Replicación de servicio de directorio detallada	No auditar
Acceso del servicio de directorio	No auditar

<table>
<tr><td></td><td></td><td></td></tr>
<tr><td>CA6.9</td><td>Categoría: Inicio de sesión de cuenta<table>
<tr><td>Operaciones de vales de servicio</td><td>No auditar</td></tr>
<tr><td>Otros eventos de inicio de sesión de cuentas</td><td>No auditar</td></tr>
<tr><td>Servicio de autenticación Kerberos</td><td>No auditar</td></tr>
<tr><td>Validación de credenciales</td><td>Éxito</td></tr>
</table></td><td></td></tr>
</table>

6.4 Obtención de evidencias

La versión 2012 de Active Directory trae consigo una serie de herramientas de administración que pueden resultar útiles para la obtención de evidencias, tanto en la operativa y uso del dominio como en la administración y configuración del mismo. Algunas de estas herramientas son [51]:

- Centro de Administración de Active Directory (ADAC, *Active Directory Administrative Center*)
- Powershell
- Equipos y usuarios de Active Directory (ADUC, *Active Directory Users and Computers*)
- ADSI Edit
- LDP
- Registro de eventos de Windows
- Auditpol
- Microsoft Security Compliance Manager

Además del registro de eventos de Windows, que resulta muy útil para monitorizar todo lo que pueda ocurrir en el sistema, destacamos las dos últimas herramientas de la lista anterior.

Microsoft Security Compliance Manager permite configurar y administrar de forma rápida los equipos tanto en la red como en una nube privada. La herramienta aporta configuraciones de línea base recomendadas que pueden importarse directamente en los equipos para conseguir una gestión más eficaz.

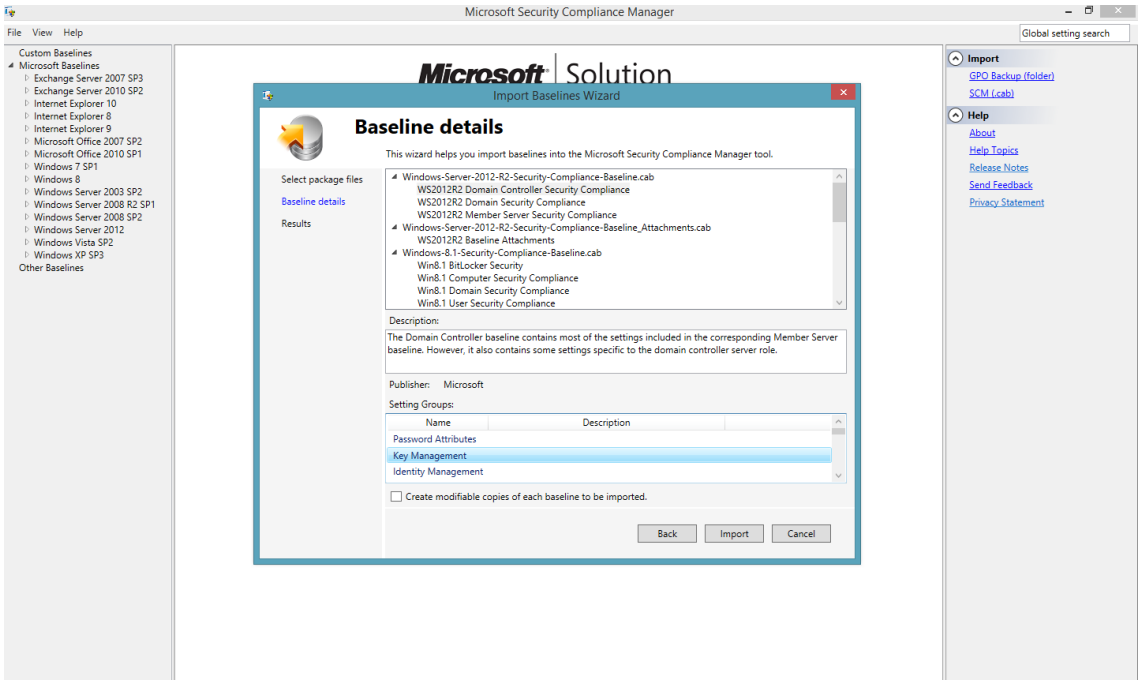


Figura 6-1. Microsoft Security Compliance Manager

Auditpol es una herramienta de línea de comandos (auditpol.exe) incluida en los sistemas Windows para manipular la información de las directivas de auditoría. En líneas generales se pueden realizar las siguientes operaciones con el comando:

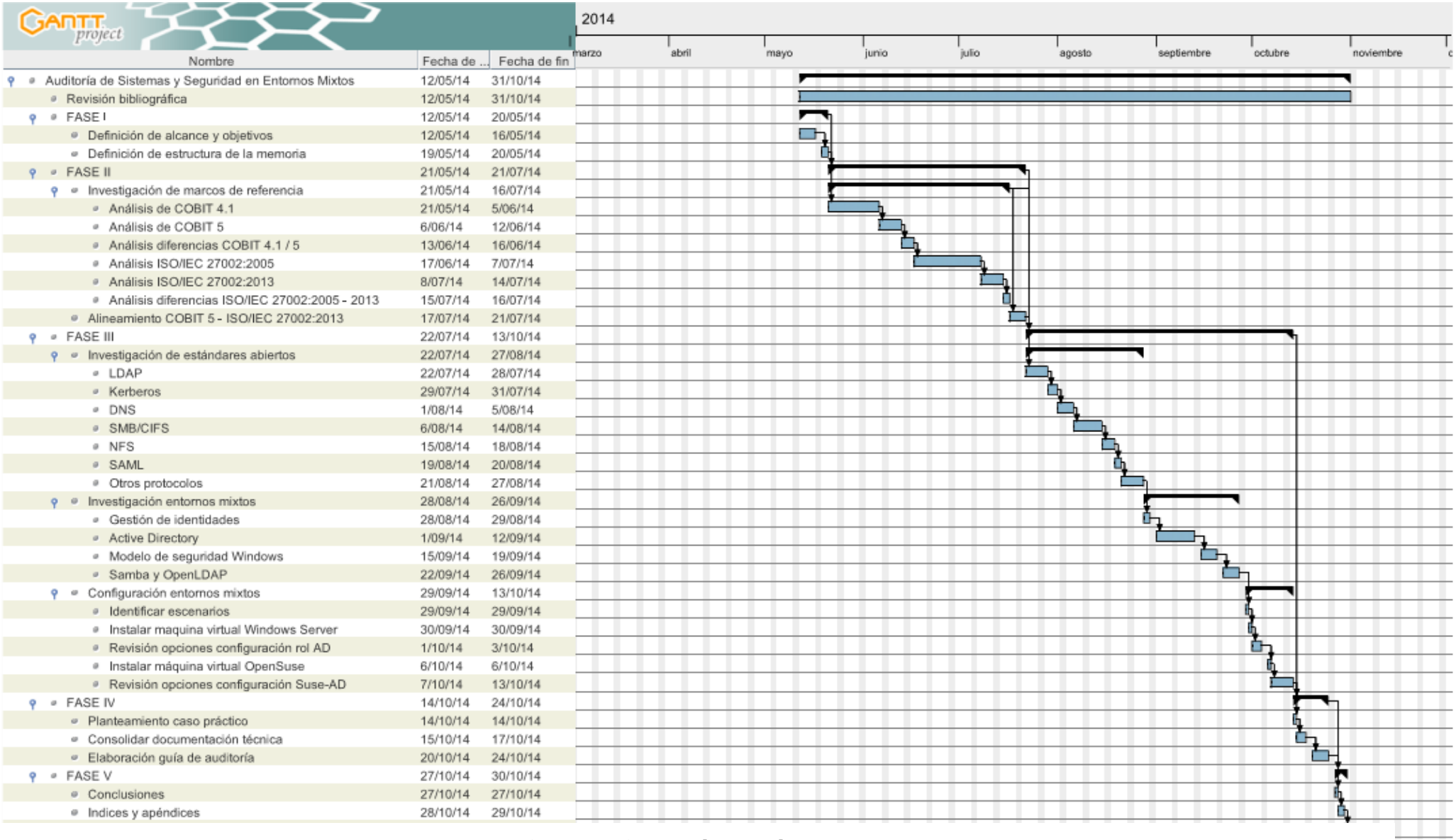
- Establecer y consultar la directiva de auditoría del sistema.
- Establecer y consultar la directiva de auditoría de un usuario determinado.
- Establecer y consultar opciones de auditoría.
- Establecer y consultar los descriptores de seguridad utilizados para delegar el acceso a una directiva de auditoría.
- Guardar la directiva de auditoría en un fichero de texto (CSV).
- Cargar la directiva de auditoría desde un fichero de texto.
- Configurar las SACLs de recursos globales.

La sintaxis general de auditpol en línea de comandos es la siguiente (ver más información en anexo IV):

Auditpol comando [<sub-comando><opciones>]

7 Presupuesto

7.1 Diagrama de Gantt



Nombre	Fecha de ...	Fecha de fin
Auditoría de Sistemas y Seguridad en Entornos Mixtos	12/05/14	31/10/14
Revisión bibliográfica	12/05/14	31/10/14
FASE I	12/05/14	20/05/14
Definición de alcance y objetivos	12/05/14	16/05/14
Definición de estructura de la memoria	19/05/14	20/05/14
FASE II	21/05/14	21/07/14
Investigación de marcos de referencia	21/05/14	16/07/14
Análisis de COBIT 4.1	21/05/14	5/06/14
Análisis de COBIT 5	6/06/14	12/06/14
Análisis diferencias COBIT 4.1 / 5	13/06/14	16/06/14
Análisis ISO/IEC 27002:2005	17/06/14	7/07/14
Análisis ISO/IEC 27002:2013	8/07/14	14/07/14
Análisis diferencias ISO/IEC 27002:2005 - 2013	15/07/14	16/07/14
Alineamiento COBIT 5 - ISO/IEC 27002:2013	17/07/14	21/07/14
FASE III	22/07/14	13/10/14
Investigación de estándares abiertos	22/07/14	27/08/14
LDAP	22/07/14	28/07/14
Kerberos	29/07/14	31/07/14
DNS	1/08/14	5/08/14
SMB/CIFS	6/08/14	14/08/14
NFS	15/08/14	18/08/14
SAML	19/08/14	20/08/14
Otros protocolos	21/08/14	27/08/14
Investigación entornos mixtos	28/08/14	26/09/14
Gestión de identidades	28/08/14	29/08/14
Active Directory	1/09/14	12/09/14
Modelo de seguridad Windows	15/09/14	19/09/14
Samba y OpenLDAP	22/09/14	26/09/14
Configuración entornos mixtos	29/09/14	13/10/14
Identificar escenarios	29/09/14	29/09/14
Instalar maquina virtual Windows Server	30/09/14	30/09/14
Revisión opciones configuración rol AD	1/10/14	3/10/14
Instalar máquina virtual OpenSuse	6/10/14	6/10/14
Revisión opciones configuración Suse-AD	7/10/14	13/10/14
FASE IV	14/10/14	24/10/14
Planteamiento caso práctico	14/10/14	14/10/14
Consolidar documentación técnica	15/10/14	17/10/14
Elaboración guía de auditoría	20/10/14	24/10/14
FASE V	27/10/14	30/10/14
Conclusiones	27/10/14	27/10/14
Indices y apéndices	28/10/14	29/10/14

Figura 7-1. Diagrama de Gantt de proyecto

7.2 Presupuesto

	**UNIVERSIDAD CARLOS III DE MADRID** **Escuela Politécnica Superior**

PRESUPUESTO DE PROYECTO

1. Autor:

Roberto Garrido Pelaz

2. Departamento:

Informática

3. Descripción del Proyecto

Consideraciones y puntos a tener en cuenta para las revisiones en este tipo de entornos, compuestos por servidores WINDOWS y servidores LINUX.

4. Presupuesto total del Proyecto (valores expresados en Euros) 28542,69

Total Jornadas: 125	

5. Desglose de costes (directos)

5.1 Personal

Nombre y apellidos	**Categoría**	**Dedicción** (hombre /jornada)	**Coste*** (hombre/jornada)	**Coste total**
Roberto Garrido Pelaz	Consultor Senior	1	187	**23375**

*El coste por jornada se obtiene con el coste por mes dividido por 20. Incluye salario bruto y cotización a la seguridad social por parte de la empresa.

5.2. Material

Material de oficina	
Paquete de papel	4
Equipo informático *Parte proporcional respecto a una vida útil calculada de 4 años (sobre 600€)	75
Impresora *Parte proporcional respecto a una vida útil calculada de 5 años (sobre 140€)	7
Toner de impresora	40
Copias de CD	8
Total	**134**

5.3. Software	
Paquete ofimática	80
Hipervisor máquinas virtuales	0
Licencias sistemas operativos	0*
Herramienta gestión de proyectos	0
Total	**80**
*Las licencias del sistema operativo para servidores Windows no han incurrido en gasto al utilizar el programa Microsoft Dreamspark for Academic Solutions de la Universidad Carlos III de Madrid	
5.4. Formación	
N/A	**0**

6. Resumen de costes	
Personal	23375
Material	134
Software	80
Formación	0
TOTAL (SIN IVA)	**23589**
IVA	**21%**
TOTAL	**28542,69**

El presupuesto total del proyecto asciende a la cantidad de 28.542,69 €

Leganés, a 12 de noviembre de 2014

Roberto Garrido Pelaz

8 Conclusiones

Consideramos cumplidos los objetivos del proyecto planteados al inicio. Se ha planteado una guía de auditoría que ayudará al lector en el proceso de evaluación de un entorno heterogéneo con elementos técnicos basados en uno de los escenarios propuestos. Estas listas de comprobación podrán extrapolarse a otros entornos similares y también con ciertas diferencias técnicas, siguiendo la misma filosofía de base y referencias del capítulo 5.

A través del alineamiento de COBIT 5 e ISO/IEC 27002:2013 (punto 3.3) hemos conseguido plantear de forma resumida y clara cuales son los puntos de control básicos que cualquier organización, independiente de su tamaño, debería tener en cuenta a la hora de definir e implantar sus sistemas de información, ofreciendo al lector la posibilidad de profundizar en los controles a través de la referencia directa de los conceptos en los estándares.

El proceso de análisis de los diferentes protocolos nos ha permitido aclarar qué tecnologías destacar, y cómo funcionan, cuando nos enfrentamos a la problemática de diseñar y decidir nuestra arquitectura tecnológica, de forma que satisfaga de la mejor forma posible las necesidades de la empresa, y teniendo en cuenta la necesidad de una gestión de identidades y control de accesos adecuados. Hemos concluido como es de importante en el sector el despliegue de sistemas de gestión de identidades, y como destaca entre ellos Microsoft Active Directory.

Además, la revisión de conceptos en cuanto al control de accesos nos ha reafirmado en la importancia de este concepto en lo relativo a seguridad de la información. Hemos visto las situaciones pasada, presente y futura en cuanto a control de accesos. Un futuro donde cada vez existirán más relaciones entre diferentes tecnologías (interoperabilidad) y proveedores de identidades para lograr que los usuarios puedan utilizar diferentes servicios, y en diferentes ámbitos y localizaciones, manteniendo los compromisos de seguridad. En este sentido, cada vez es más importante el concepto de federación de identidades, provisión de servicios de gestión de identidades en la nube y control de acceso único.

En cuanto a valoraciones personales del proyecto, aunque el planteamiento del mismo se hizo hace tiempo, se actualizaron puntos y conceptos en su desarrollo final para adaptarlo a la situación actual. Los principales problemas encontrados están relacionados con el volumen de información a analizar, y el reto de enfocar y resumir eficazmente dado el número de conceptos que se manejan.

Al revisar e introducirse en las referencias bibliográficas, es habitual encontrar nuevos conceptos desconocidos hasta ese momento que amplían el campo de búsqueda de conocimiento. En este sentido, aunque pueda verse algo extenso este documento, realmente supone un resumen de los temas tratados ya que en cada uno de ellos se puede profundizar con el fin de especializarse más. Esto da un grado de percepción de que los dominios de conocimiento de la auditoría y la seguridad de la información son muy amplios.

Por otra parte, abordar un estándar de buenas prácticas no es tarea fácil ya que normalmente suelen ser extensos dado el amplio espectro de casos que deben cubrir. El buen manejo de los mismos es algo fundamental para que un buen auditor, consultor, arquitecto, etc… logre sus objetivos con eficiencia.

9 Líneas Futuras

La guía de auditoría planteada en el capítulo 6 es una guía centrada en un posible escenario de entorno mixto: integración de clientes empresariales, Windows y Linux en Active Directory, desplegado en un modelo IaaS; y por tanto, existen muchas posibilidades de ampliación, continuación y mejora:

- Auditoría de seguridad detallada en un entorno mixto donde el sistema de gestión de identidades sea Samba, Samba con OpenLDAP como backend. Estos entornos podrían a su vez implementarse utilizando un modelo tradicional de infraestructura, o modelos de computación en la nube.
- Auditoría de seguridad detallada donde se ofrezcan servicios de federación de identidades, principalmente Active Directory Federation Services.
- Análisis y puntos a considerar para una auditoría de otros sistemas de gestión de identidades como: NetIQ eDirectory, IBM Tivoli Identity Manager y Oracle Identity Management.
- Análisis de gestión de identidades y acceso en modelos PaaS como: Microsoft Azure Active Directory, Microsof Azure Multifactor Authentication.
- Ampliar la guía de auditoría con los puntos necesarios para poder certificar en base a ISO/IEC 27001.
- A través de las herramientas de obtención de evidencias y otros sistemas de monitorización, definir un modelo de métricas de seguridad basado en ISO/IEC 27004.
- Plantear nuevos protocolos o mejoras de alguno de los analizados en el punto 4.3 que faciliten la integración de sistemas en entornos mixtos.
- A partir de un modelo de métricas de seguridad definir una herramienta de soporte a la auditoría (interna) que además ayude en el proceso de evaluación de controles. Definición de cuadros de mando con información resumida de las métricas de seguridad.
- Proyecto de integración de datos ofrecidos por diferentes sistemas habituales en control de sistemas y seguridad como: Nessus, OpenVas, Nagios, SolarWinds, ACL.

10 Glosario de Términos y Acrónimos

ABAC: Control de Acceso Basado en Atributo.

AC: Servicio de Autenticación. Elemento que participa en el protocolo Kerberos.

ACE: Entrada de Control de Acceso.

ACL: Lista de Control de Acceso.

ADAC: Centro de Administración de Active Directory. Herramienta administrativa para la gestión de dominios.

ADUC: Equipos y Usuarios de Active Directory. Herramienta administrativa para la gestión de usuarios y equipos de un dominio.

AES: Estándar para el Cifrado Avanzado. Protocolo de cifrado simétrico de datos más avanzado que DES.

API: Interfaz de Programación de Aplicaciones.

BDC: Controlador de Dominio de Respaldo.

BIOS: Sistema Básico de Entrada/Salida.

BS: Estándar Británico (Reino Unido).

BSI: Institución de Estándares Británicos (Reino Unido).

BYOD: "Trae tu propio dispositivo". Política empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo.

CCTA: Agencia Central de Computación y Telecomunicaciones (Reino Unido)

CEO: Director Ejecutivo.

CIFS: Sistema de Ficheros Común de Internet. Protocolo de red evolución de SMB.

CISA: Auditor Certificado de Sistemas de Información.

CLUSIF: Club Francés de la Seguridad de la Información (Francia).

CN: Nombre Común. Atributo de una entrada de directorio LDAP.

COSO: Comité de Organizaciones Patrocinadoras de la Comisión Treadway.

CPD: Centro de Proceso de Datos.

CRM: Gestión de las Relaciones con el Cliente.

CSV: Formato de fichero con valores separados por comas.

DAC: Control de Acceso Discrecional.

DAP: Protocolo de Acceso a Datos. Protocolo genérico para el acceso a directorios.

DC: Controlador de Dominio.

DCHP: Protocolo de Configuración de Equipo Dinámico.

DES: Estándar para el Cifrado de Datos. Protocolo de cifrado simétrico de datos

DIT: Árbol de Información de Directorio.

DN: Nombre Distintivo. Identificador descriptivo único de un objeto en un directorio LDAP.

DNS: Sistema de Nombres de Dominio.

DOS: Sistema Operativo de Disco.

DRM: Gestión de Derechos Digitales.

ERP: Sistema de Planificación de Recursos Empresariales.

FAT: Tabla de Asignación de Archivos. Tipo de formato del sistema de ficheros en Windows.

FSF: Fundación para el Software Libre.

FSMO: Rol de Maestro de Operaciones de un servidor Windows.

GID: Identificador de Grupo en un sistema Linux

GNU: GNU No es UNIX. Movimiento/Proyecto raíz para la promoción del software libre.

GPL: Licencia Pública General.

GPO: Objeto de Política de Grupo. Objeto que se utiliza para la definición de directivas de funcionamiento en un dominio Active Directory.

GUI: Interfaz Gráfica de Usuario.

GUID: Identificador Único Global. Implementación de Microsoft del estándar UUID.

IaaS: Infraestructura como Servicio. Tipo de uso de computación en la nube.

IAG: Gobernanza de la Identificación y el Acceso.

IAM: Gestión de Identidad y Acceso.

IdM: Administración de Identificación.

IEC: Comisión Electrotécnica Internacional.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

IETF: Grupo de Trabajo de Ingeniería de Internet.

IoT: Internet de las Cosas.

IP: Protocolo de Internet.

IPPF: Marco Internacional de Prácticas Profesionales.

IPSec: Protocolo de Internet Seguro

ISA: Soluciones de Interoperabilidad para las Administraciones Públicas Europeas.

ISACA: Asociación para la Auditoría y Control de los Sistemas de Información.

ISACF: Fundación para la Auditoría y Control de los Sistemas de Información. Antigua denominación de ISACA.

ISF: Foro para la Seguridad de la Información.

ISO: Organización Internacional para la Estandarización.

ITAF: Conjunto de prácticas profesionales para la auditoría de sistemas de información. Propuesto por ISACA.

ITGI: Instituto para la Gobernanza de las Tecnologías de la Información.

ITIL: Librería de Infraestructura de Tecnologías de la Información.

KDC: Centro de Distribución de Claves. Elemento que participa en el protocolo Kerberos.

LDAP: Protocolo de Acceso Ligero a Directorio.

LDIF: Formato de Intercambio de Datos LDAP.

LOPD: Ley Orgánica de Protección de Datos.

LSA: Autoridad de Seguridad Local. Servicio que interviene en el proceso de autenticación en un sistema Windows.

LSSICE: Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.

MAC: Control de Acceso Mandatorio.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.

MEHARI: Método para el Análisis de Riesgos Armonizado (Francia).

MIT: Instituto Tecnológico de Massachusetts.

NFS: Sistema de Ficheros en Red. Protocolo para la implementación de sistemas de ficheros distribuidos por una red.

NIS: Sistema de Información de Red. Mecanismo para la centralización de cuentas de usuario y grupos en sistemas UNIX.

NIST: Instituto Nacional de Estándares y Tecnología (Estados Unidos).

NSS: Conmutador de Servicio de Nombre: Mecanismo de seguridad Linux para la configuración del método de resolución de nombres de usuario.

NTFS: Sistema de Ficheros de Nueva Tecnología. Tipo de formato del sistema de ficheros en Windows con opciones de seguridad.

NTLM: Gestor de LAN NT. Conjunto de protocolos de seguridad para las versiones antiguas de Windows (NT, 2000).

NTP: Protocolo de hora en red. Protocolo de servicio para la sincronización de los relojes de las máquinas de una red.

OASIS: Organización para el Avance de los Estándares de Información Estructurada.

OAuth: Protocolo de Autorización Abierta.

ORCON: Diseminación y Extracción de la Información Controlada por el Originador.

OU: Unidad Organizativa.

PaaS: Plataforma como Servicio. Tipo de uso de computación en la nube.

PAM: Módulos de Autenticación Conectables. Mecanismo de seguridad de Linux para la configuración del método de autenticación.

PCGA: Principios de Contabilidad Generalmente Aceptados.

PDC: Controlador de Dominio Primario.

PDCA: Modelo Planificar-Ejecutar-Verificar-Actuar.

PDF: Formato de Documento Portable.

PKI: Infraestructura de Clave Pública.

POSIX: Interfaz de Sistema Operativo Portable. Estándar para la especificación de funciones de un sistema operativo portable.

RBAC: Control de Acceso Basado en Roles.

RFC: Petición de Comentarios. Serie de protocolos relacionados con Internet que son propuestos al IETF.

RID: Identificador Relativo. Suministrado de forma aleatoria por una autoridad de gestión de identidades tipo Windows.

RODC: Controlador de Dominio de Sólo Lectura.

RPC: Llamada a Procedimiento Remoto.

RSA: Protocolo de cifrado propuesto por Rivest, Shamir y Adleman.

SaaS: Software como Servicio. Tipo de uso de computación en la nube.

SAM: Gestor Simple de Cuentas. Tecnología utilizada en el proceso de autenticación local de un sistema Windows.

SAML: Lenguaje de Marcado para Confirmaciones de Seguridad.

SANS: Instituto para la Auditoría de Sistemas, Redes y Seguridad.

SecaaS: Seguridad como Servicio. Tipo de uso de computación en la nube.

SFU: Servicios de Windows para UNIX

SGSI: Sistema de Gestión de la Seguridad de la de Información.

SHA-1: Algoritmo de "Hash" Seguro.

SID: Identificador de Seguridad en un sistema Windows.

SLA: Acuerdo de Nivel de Servicio (Service Level Agreement).

SMB: Bloque de Mensaje de Servidor. Protocolo de red para compartir archivos e impresoras.

SQL: Lenguaje de Consulta Estructurado.

SSAE16: Declaración de normas para contratos de atestación (Estados Unidos).

SSL: Capa de Conexión Segura. Protocolo para utilizar conexiones seguras (cifradas) en una red.

SSO: Sistema Centralizado de Autenticación y Autorización.

TCP: Protocolo de Control de Transporte.

TDB: Base de Datos Trivial. Tecnología utilizada por suite de servicios Samba.

TGS: Servicio de Concesión de Tickets. Elemento que participa en el protocolo Kerberos.

TI: Tecnologías de la Información.

TIC: Tecnologías de la Información y las Comunicaciones.

TLS: Capa de Transporte Segura. Protocolo para el establecimiento de conexiones seguras en una red. Evolución de SSL.

TOGAF: Esquema de Arquitectura de Open Group. Metodología estándar para la definición de arquitecturas empresariales.

UDP: Protocolo de Datagrama de Usuario

UID: Identificador de Usuario en un sistema Linux

UNE: Una Norma Española.

UUID: Identificador Universalmente Único (estándar).

VPN: Red Privada Virtual (Virtual Private Network).

W3C: Consorcio para la "World Wide Web".

WAM: Administración de Acceso a la Web.

XACML: Lenguaje de Marcado extensible para el Control de Acceso.

XML: Lenguaje de Marcado Extendido.

11 Bibliografía

[1]. **Fernández Sánchez, Carlos Manuel y Piattini Velthuis, Mario (Coords).** *Modelo para el gobierno de las TIC basado en las normas ISO.* Madrid : AENOR [Asociación Española de Normalización y Certificación], 2012. ISBN 978-84-8143-764-5.

[2]. **ISO [International Organization for Standardization].** ISO Catalog. [En línea] [Citado el: 18 de Agosto de 2014.] Disponible en: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

[3]. **ISACA [Information Systems Audit and Control Association].** *COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Rolling Meadows : ISACA, 2012. ISBN 978-1-60420-282-3.

[4]. **COSO [Committee of Sponsoring Organizations of the Treadway Commission].** COSO. [En línea] [Citado el: 10 de Septiembre de 2014.] Disponible en: http://www.coso.org/default.htm.

[5]. **AXELOS.** ITIL. [En línea] [Citado el: 2 de Septiembre de 2014.] Disponible en: http://www.itil-officialsite.com/.

[6]. **ISO27000.ES.** iso27000. [En línea] [Citado el: 05 de Septiembre de 2014.] Disponible en: http://www.iso27000.es/.

[7]. **NIST [National Institute of Standards and Technology].** NIST Computer Security Division. [En línea] [Citado el: 6 de Octubre de 2014.] Disponible en: http://csrc.nist.gov/publications/PubsSPs.html.

[8]. **CLUSIF [Club de la Sécurité de l'Information Français].** Mehari: Information risk analysis and management methodology. [En línea] [Citado el: 13 de Octubre de 2014.] Disponible en: https://www.clusif.asso.fr/en/production/mehari/.

[9]. **Foro para la Seguridad de la Información.** Estándar de Buenas Prácticas para la Seguridad de la Información. [En línea] 2014. [Citado el: 14 de Septiembre de 2014] Disponible en: https://www.securityforum.org/tools/sogp/.

[10]. **SANS Institute.** SANS Institute. [En línea] [Citado el: 9 de Octubre de 2014.] Disponible en: http://www.sans.org/.

[11]. —. Controles de Seguridad Críticos. [En línea] [Citado el: 9 de Octubre de 2014.] Disponible en: http://www.sans.org/critical-security-controls.

[12]. **Microsoft Corporation; Suse.** MOREINTEROP. [En línea] [Citado el: 5 de Octubre de 2014.] Disponible en: http://www.moreinterop.com.

[13]. **ISACA [Information Systems Audit and Control Association].** *Principios rectores para la adopción y el uso de la computación en la nube.* Rolling Meadows : ISACA, 2012.

[14]. **Tipton, Harold F. y Krause Nozaki, Micki.** *Information Security Management Handbook.* 6th Ed. Boca Raton : CRC Press, 2012. Vol. Vol. 5. ISBN 978-1-4398-5346-7.

[15]. **Symantec.** Security Response Publications. [En línea] 2014. [Citado el: 25 de Octubre de 2014.] Disponible en: http://www.symantec.com/security_response/publications/threatreport.jsp.

[16]. —. *Internet Security Threat Report 2014.* s.l. : Symantec, 2014. Disponible en: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[17]. **Piattini Velthuis, Mario G. (Coord).** *Auditoría informática : un enfoque práctico.* 1a Ed. s.l. : RA-MA, 1997. ISBN 8478972935.

[18]. **Ramos, Miguel Ángel.** Apuntes de asignatura 'Auditoría Informática'. Titulación 'I.T. Informática de Gestión'. Universidad Carlos III de Madrid. Madrid : s.n., 2005.

[19]. **Calder, Alan.** *ISO/IEC 38500: The IT Governance Standard.* Ely : IT Governance Publishing, 2008. ISBN 978-1-905-35657-7.

[20]. **ISACA [Information Systems Audit and Control Association].** *COBIT 5 Procesos Catalizadores.* Rolling Meadows : ISACA, 2012. ISBN 978-1-60420-285-4.

[21]. **ISO / IEC.** ISO/IEC 27002:2013. Tecnología de la Información - Técnicas de Seguridad - Código de Prácticas para Controles en Seguridad de la Información. 2nd Ed. Ginebra : ISO, 2013.

[22]. **ISACA.** *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit.* 2008.

[23]. **IEEE [The Institute of Electrical and Electronics Engineers].** *IEEE Standard Glossary of Software Engineering Terminology.* New York, New York : IEEE, 1990. ISBN 1-55937-067-X.

[24]. **IETF [The Internet Engineering Task Force].** *RFC 1777.* s.l. : The Internet Society, 1995. Disponible en: https://datatracker.ietf.org/doc/rfc1777/?include_text=1.

[25]. —. *RFC 2251.* s.l. : The Internet Society, 1997. Disponible en: https://datatracker.ietf.org/doc/rfc2251/?include_text=1.

[26]. **OpenLDAP Foundation.** www.openldap.org. [En línea] [Citado el: 8 de Agosto de 2014.] Disponible en: http://www.openldap.org.

[27]. **IETF [The Internet Engineering Task Force].** *RFC 1210.* s.l. : The Internet Society, 1990. Disponible en: https://datatracker.ietf.org/doc/rfc1210/?include_text=1.

[28]. —. *RFC 4120.* s.l. : The Internet Society, 2005. Disponible en: https://datatracker.ietf.org/doc/rfc4120/?include_text=1.

[29]. **MIT [Massachusetts Institute of Technology].** MIT. Kerberos. [En línea] [Citado el: 11 de Agosto de 2014.] Disponible en: http://web.mit.edu/Kerberos/.

[30]. **IETF [The Internet Engineering Task Force].** *RFC 1034.* s.l. : The Internet Society, 1987. Disponible en: https://datatracker.ietf.org/doc/rfc1034/?include_text=1.

[31]. —. *RFC 1035.* s.l. : The Internet Society, 1987. Disponible en: https://datatracker.ietf.org/doc/rfc1035/?include_text=1.

[32]. **Carter, Gerald y Eckstein, Robert.** *Using Samba.* 3rd Ed. Sebastopol : O'Reilly, 2007. ISBN 978-0-596-00769-0.

[33]. **Microsoft Corporation.** [MS-CIFS]: Common Internet File System (CIFS) Protocol. [En línea] [Citado el: 28 de Agosto de 2014.] Disponible en: http://msdn.microsoft.com/en-us/library/ee442092.aspx.

[34]. —. Microsoft SMB Protocol and CIFS Protocol Overview. *MDSN Library.* [En línea] [Citado el: 2014 de Agosto de 26.] Disponible en: http://msdn.microsoft.com/en-us/library/windows/desktop/aa365233(v=vs.85).aspx.

[35]. **IETF [The Internet Engineering Task Force].** *RFC 3530.* s.l. : The Internet Society, 2003. Disponible en: https://datatracker.ietf.org/doc/rfc3530/?include_text=1.

[36]. **Callaghan, Brent.** *NFS Illustrated.* Reading : Addison Wesley, 1999. ISBN 0-201-32570-5.

[37]. **OASIS.** SAML XML. [En línea] [Citado el: 13 de Septiembre de 2014.] Disponible en: http://saml.xml.org/.

[38]. **IETF [The Internet Engineering Task Force].** *RFC 4301.* s.l. : The Internet Society, 2005. Disponible en: https://datatracker.ietf.org/doc/rfc4301/?include_text=1.

[39]. —. *RFC 4302.* s.l. : The Internet Society, 2005. Disponible en: https://datatracker.ietf.org/doc/rfc4302/?include_text=1.

[40]. —. *RFC 4305.* s.l. : The Internet Society, 2005. Disponible en: https://datatracker.ietf.org/doc/rfc4305/?include_text=1.

[41]. —. *RFC 5246.* s.l. : The Internet Society, 2008. Disponible en: https://datatracker.ietf.org/doc/rfc5246/?include_text=1.

[42]. **OpenId Foundation.** OpenID. [En línea] [Citado el: 15 de Septiembre de 2014.] Disponible en: www.openid.net.

[43]. *OpenID Single Sign-On.* **Weiskotten, Jeremy.** 10, San Mateo : s.n., 2008, Journal, Dr. Dobb's, Vol. 33, págs. 40-45. ISSN 1044789X.

[44]. **IETF [The Internet Engineering Task Force].** *RFC 6749.* s.l. : The Internet Society, 2012. Disponible en: https://datatracker.ietf.org/doc/rfc6749/?include_text=1.

[45]. —. *RFC 6750.* s.l. : The Internet Society, 2012. Disponible en: https://datatracker.ietf.org/doc/rfc6750/?include_text=1.

[46]. —. *RFC 6819.* s.l. : The Internet Society, 2013. Disponible en: https://datatracker.ietf.org/doc/rfc6819/?include_text=1.

[47]. **OAuth.** Open Authentication. [En línea] [Citado el: 14 de Septiembre de 2014.] Disponible en: http://oauth.net/.

[48]. *Gestión de identidades y control de acceso desde una perspectiva organizacional.* **Montoya, José A. y Restrepo, Zuleima.** 1, Medellín : s.n., 2012, Revista Ingenierías USBMed, Vol. 3, págs. 23-34. ISSN-e 2027-5846.

[49]. **Ramos Álvarez, Bejamín y Ribagorda Garnacho, Arturo (Dirs).** *Avances en criptología y seguridad de la información.* Madrid : Ediciones Diaz de Santos, 2004. ISBN 84-7978-650-7.

[50]. **Bosworth, Seymour, Kabay, M.E y Whyne, Eric.** *Information Security Management Handbook.* 5th Ed. Hoboken : John Wiley & Sons, Inc., 2009. Vol. 1. ISBN 978-0-471-71652-5.

[51]. **Desmond, Brian y Richards, Joe et al.** *Active Directory.* 5th Ed. Sebastopol : O'Reilly Media, 2013. ISBN 978-1-4493-2002-7.

[52]. **Reimer, Stan y Kezema, Conan et al.** *Windows Server 2008 Active Directory Resource Kit.* Redmond : Microsoft Press Store, 2008. ISBN 9780735625150.

[53]. **Policelli, John.** *Active Directory Domain Services 2008 How-To.* s.l. : Sams Publishing, 2009. ISBN 978-0-672-33045-2.

[54]. **Microsoft Corporation.** Microsoft Technet Library. Active Directory. [En línea] [Citado el: 9 de Septiembre de 2014.] Disponible en: http://technet.microsoft.com/en-us/library/dn283324.aspx.

[55]. —. Microsoft Technet Library. [En línea] 24 de Julio de 2013. [Citado el: 20 de Septiembre de 2014.] Disponible en: http://technet.microsoft.com/en-us/library/dn268294.aspx.

[56]. **Samba Tema.** SAMBA. [En línea] [Citado el: 26 de Julio de 2014.] Disponible en: http://www.samba.org.

[57]. **SUSE.** SUSE. Using Samba. [En línea] [Citado el: 10 de Octubre de 2014.] Disponible en: https://www.suse.com/documentation/sles-12/book_sle_admin/data/cha_samba.html.

[58]. —. Open Suse Reference Guide. [En línea] [Citado el: 26 de Septiembre de 2014.] Disponible en: http://activedoc.opensuse.org/book/opensuse-reference.

[59]. **SUSUE.** OpenSuse Security Guide. [En línea] [Citado el: 29 de Septiembre de 2014.] Disponible en: http://activedoc.opensuse.org/book/opensuse-security-guide.

[60]. **Microsoft.** *Windows 2008 Security Guide.* 2009.

[61]. **Wikipedia.** Wikipedia. [En línea] Disponible en: http://www.wikipedia.org.

[62]. **Chaplin, Mark y Creasey, Jason.** *The 2011 Standard of Good Practice for Information Security.* s.l. : Information Security Forum Limited, ISF [Information Security Forum], 2011. Disponible en: https://www.securityforum.org/tools/sogp/.

[63]. **ISO / IEC.** ISO/IEC 19011:2011. Directrices para auditar sistemas de gestión. 2nd Ed. Ginebra : ISO, 2011.

[64]. **Karsberg, Christoffer, Skouloudi, Christina y Dekker, Dr. Marnix.** *Annual Incident Reports 2013.* s.l. : ENISA [European Union Agency for Network and Information Security], 2103. ISBN: 978-92-9204-095-6, ISSN: 2363-2097, DOI: 10.2824/32965.

[65]. **Microsoft Corporation.** *Windows Server 2008 Security Guide.* s.l. : Microsoft Corporation, 2008. Disponible en: http://www.microsoft.com/en-us/download/details.aspx?id=17606.

12 Anexos

ANEXO I. Metas de COBIT

METAS DE NEGOCIO		
Perspectiva	**Num. Meta**	**Descripción Meta Corporativa**
Financiera	1	Valor para las partes interesadas de las inversiones de negocio
	2	Cartera de productos y servicios competitivos
	3	Riesgos de negocio gestionados (salvaguarda de activos)
	4	Cumplimiento de leyes y regulaciones externas
	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio cambiante
	8	Respuestas ágiles a un entorno de negocio cambiante
	9	Toma estratégica de decisiones basada en información
	10	Optimización de costes de entrega del servicio
Interna	11	Optimización de la funcionalidad de los procesos de negocio
	12	Optimización de los costes de los procesos de negocio
	13	Programas gestionados de cambio en el negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje y crecimiento	16	Personas preparadas y motivadas
	17	Cultura de innovación de producto y negocio

METAS DE TI		
Perspectiva	**Num. Meta**	**Descripción Meta Corporativa**
Financiera	1	Alineamiento de TI y estrategia de negocio.
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.
	4	Riesgos de negocio relacionados con las TI gestionados.
	5	Realización de beneficios del portafolio de inversiones y servicios relacionados con TI.
	6	Transparencia de los costes, beneficios y riesgos de TI.
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio.
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas.
Interna	9	Agilidad de las TI.
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones.
	11	Optimización de activos, recursos y capacidades de las TI.
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio.
	13	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones.
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y crecimiento	16	Personal del negocio y de las TI competente y motivado.
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio.

ANEXO II. Modelo de referencia de procesos COBIT 5

DOMINIO	**ID**	**PROCESO**
Evaluar, Orientar y Supervisar	EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno
	EDM02	Asegurar la entrega de beneficios
	EDM03	Asegurar la optimización del riesgo
	EDM04	Asegurar la optimización de recursos
	EDM05	Asegurar la transparencia hacia las partes interesadas
Alinear, planificar y organizar	APO01	Gestionar el marco de gestión de TI
	APO02	Gestionar la estrategia
	APO03	Administrar la arquitectura empresarial
	APO04	Gestionar la innovación
	APO05	Gestionar la cartera
	APO06	Gestionar el presupuesto y los costes
	APO07	Gestionar los recursos humanos
	APO08	Gestionar las relaciones
	APO09	Gestionar los acuerdos de servicio
	APO10	Gestionar los proveedores
	APO11	Gestionar la calidad
	APO12	Gestionar el riesgo
	APO13	Gestionar la seguridad
Construir, adquirir e implementar	BAI01	Gestionar los programas y proyectos
	BAI02	Gestionar la definición de requisitos
	BAI03	Gestionar la identificación y la construcción de soluciones
	BAI04	Gestionar la disponibilidad y la capacidad
	BAI05	Gestionar la habilitación del cambio organizativo
	BAI06	Gestionar los cambios
	BAI07	Gestionar la aceptación del cambio y de la transición
	BAI08	Gestionar el conocimiento
	BAI09	Gestionar los activos

	BAI010	Gestionar la configuración
Entregar, dar servicio y soporte	DSS01	Gestionar las operaciones
	DSS02	Gestionar las peticiones y los incidentes de servicio
	DSS03	Gestionar los problemas
	DSS04	Gestionar la continuidad
	DSS05	Gestionar los servicios de seguridad
	DSS06	Gestionar los controles de los procesos de la empresa
Supervisar, evaluar y valorar	MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad
	MEA02	Supervisar, evaluar y valorar el sistema de control interno
	MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos

ANEXO III. Relación de dominios y objetivos de control ISO/IEC 27002:2013

Dominio	**Objetivo de control**
Políticas de Seguridad de la Información	Directrices de la Dirección en Seguridad de la información.
Aspectos organizativos de la seguridad de la información	Organización interna.
	Dispositivos para movilidad y teletrabajo.
Seguridad en los recursos humanos	Antes de la contratación.
	Durante la contratación.
	Cese o cambio de puesto de trabajo.
Gestión de activos	Responsabilidad sobre los activos.
	Clasificación de la información.
	Manejo de los soportes de almacenamiento.
Control de accesos	Requisitos de negocio para el control de accesos.
	Gestión de acceso de usuario.
	Responsabilidades del usuario.
	Control de acceso a sistemas y aplicaciones.
Cifrado	Controles criptográficos.
Seguridad física y ambiental	Áreas seguras.
	Seguridad de los equipos.
Seguridad en las operaciones	Responsabilidades y procedimientos de operación.
	Protección contra código malicioso.
	Copias de seguridad.
	Registro de actividad y supervisión.
	Control del software en explotación.
	Gestión de la vulnerabilidad técnica.
	Consideraciones de las auditorías de los sistemas de información.

(Cont.)

Dominio	**Objetivo de control**
Seguridad en las telecomunicaciones	Gestión de la seguridad en las redes.
	Intercambio de información con partes externas.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Requisitos de seguridad de los sistemas de información.
	Seguridad en los procesos de desarrollo y soporte.
	Datos de prueba.
Relaciones con proveedores	Seguridad de la información en las relaciones con proveedores.
	Gestión de la prestación de servicios por proveedores.
Gestión de incidentes en la seguridad de la información	Gestión de incidentes de seguridad de la información y mejoras.
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Continuidad de la seguridad de la información.
	Redundancias.
Cumplimiento	Cumplimiento de los requisitos legales y contractuales.
	Revisiones de la seguridad de la información.

ANEXO IV. Opciones de Auditpol

- /get: muestra la directiva de auditoría. La sintaxis del comando es la siguiente:

```
Auditpol /get
[/user[:<username>|<{sid}>]]
[/category:*|<name>|<{guid}>[,:<name|<{guid}>…]]
[/subcategory:*|<name>|<{guid}>[,:<name|<{guid}>…]]
[/option:<option name>]
[/sd]
[/r]
```

- /set: establece la directiva de auditoría. La sintaxis del comando es la siguiente:

```
Auditpol /set
[/user[:<username>|<{sid}>][/include][/exclude]]
[/category:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}>…]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/option:<option name> /value: <enable>|<disable>]
```

Por ejemplo, para establecer los valores para la subcategoría “Inicio de sesión”:

c:/>auditpol /set /subcategory:”Inicio de sesión” /success:enable /failure:enable

- /list: muestra los elementos seleccionables de la directiva. La sintaxis del comando es la siguiente:

```
auditpol /list
[/user|/category|subcategory[:<categoryname>|<{guid}>|*]]
[/v] [/r]
```

Por ejemplo, para mostrar todas las subcategorías:

c:/>auditpol /list /subcategory*

- /backup: guarda la directiva de auditoría a un fichero
- /restore: restaura la directiva de auditoría desde un fichero creado con el subcomando /backup.
- /clear: limpia la directiva de auditoría

- /remove: permite eliminar toda la configuración de la directiva de auditoría tanto para un usuario concreto como para todo el sistema. La sintaxis para eliminar directivas es la siguiente:

```
Auditpol /remove [/user[:<username>|<{SID}>]]
[/allusers]
```

- /resourcesSACL: configura la lista de control de acceso de sistema (SACLs) de recursos globales. La sintaxis del comando es la siguiente:

```
auditpol /resourceSACL
[/set /type:<resource> [/success] [/failure] /user:<user> [/access:<access
flags>]]
[/remove /type:<resource> /user:<user> [/type:<resource>]]
[/clear [/type:<resource>]]
[/view [/user:<user>] [/type:<resource>]]
```

/?: muestra la ayuda de auditpol