ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

INFORMÁTICA

GRADO INGENIERÍA DE COMPUTADORES

SEGURIDAD EN UNA RED UNIVERSITARIA
SECURITY IN A UNIVERSITY NETWORK

Realizado por

JUAN ANTONIO BERNAL ESPAÑA

Tutorizado por

JUAN JOSÉ ORTEGA DAZA

Departamento
LENGUAJE Y CIENCIAS DE LA COMPUTACIÓN
UNIVERSIDAD DE MÁLAGA

MÁLAGA, (Diciembre 2014)

Fecha de Lectura:

El Secretario del Tribunal

“Porque donde están dos o tres reunidos en mi nombre,

allí estoy yo, en medio de ellos”

(Mt 18,20)

Resumen:

Las redes de comunicaciones son muy importantes para las empresas. Se solicita una red de altas prestaciones que pueda llevar muchos sistemas sobre ella (cámaras de seguridad, video, voz, datos, SCADA, wifi). Ahora también necesitamos que la red sea segura. Cuando hablamos de seguridad no solo nos referimos a evitar ataques o virus, también hablamos de cómo puede afectarnos el incendio de un centro de proceso de datos. Basándonos en la ISO 27001:2013 daremos las principales pautas para que la gestión de esta red sea segura. En este trabajo hemos securizado una red universitaria que usa tecnología MPLS.

Palabras clave:

Red, seguridad, iso 27001, MPLS, comunicaciones

Abstract:

Communications networks are very important for businesses. A network of high performance that can carry on many systems it is requested (security cameras, video, voice, data, SCADA, wifi). Now we also need that the network is secure. When we talk about security we mean not only prevent attacks or viruses, we also talk about how it can affect the burning of a data processing center. Based on the ISO 27001: 2013 we give the main guidelines for the management of this network is secure. In this work we have Secured a university network using MPLS technology.

Keywords:

Networks, security, ISO 27001, MPLS, communications.

Índice

1 INTRODUCCIÓN

Cada vez más redes se están viendo afectadas por amenazas de seguridad, ataques y fraudes informáticos, problemas de sabotajes, virus y otro tipo de contingencias, imprevistos y catástrofes mayores, con el posible riesgo de eliminación y pérdida de información.

La relación entre tecnologías de la información, la seguridad de las instalaciones, el personal, la protección y los procesos de negocio es cada vez más estrecha. La clave, no sólo está en la inversión de herramientas que mejoren la seguridad, sino en desarrollar e implementar enfoques y esquemas para el control y gestión de las amenazas presentes y futuras.

Este proyecto surge como continuación de otro: DISEÑO DE UNA RED MPLS en el cual se planteaba una posible solución a las necesidades de comunicación de la Universidad de Málaga usando tecnología MPLS. En posibles mejoras del mismo se incluía la parte de Seguridad y es ese precisamente el motivo del presente Trabajo Fin de Grado, dotar de seguridad el diseño de red planteado, para ello nos basaremos en el estándar ISO/IEC 27001

En este trabajo fin de grado no vamos a decir lo importante que es la seguridad en cualquier organización, pero sí intentaremos eliminar la imagen de que la seguridad es un gasto y no un beneficio.

En el presente TFG se distinguirán 3 partes bien diferenciadas:

- ✓ Introducción a la ISO 27001.
- ✓ Realización del sistema de gestión de seguridad (SGSI) de la red universitaria.
- ✓ Mejoras y conclusiones.

En el segundo capítulo se realizará una introducción muy breve a la ISO 27001:2013. Se hará un desarrollo histórico hasta llegar a la normativa actual y posteriormente se enumerarán las partes que la componen.

En el tercer capítulo aplicaremos la norma UNE-ISO/IEC/27000 al diseño de red. Es obvio que esta norma cubre muchos aspectos así que intentaremos centrarnos en la parte de comunicaciones.

Para conseguir seguridad vamos a realizar un análisis de riegos que proporcionará información sobre los activos expuestos así como el nivel de exposición y el impacto en el caso que lleguen a ocurrir.

Si bien es cierto que nos basamos en la ISO 27001 para securizar nuestra red, el presente TFG no es una guía para conseguir la certificación ISO y sólo pretendemos establecer unos cimientos fuertes para una vez establecidos poder avanzar hacia la certificación.

En cuarto capítulo daremos se recogen las conclusiones finales así como nuevas mejoras al presente TFG.

1.1 Beneficios de la Seguridad

¿Se puede permitir una Universidad no proteger la información que maneja? La respuesta es obvia y es que la seguridad está directamente relacionada con la supervivencia de los servicios que se ofrecen. Hay que tener claro que cuando hablamos de seguridad no sólo nos estamos refiriendo a que determinadas personas tengan acceso a determinada información. Cuando hablamos de seguridad nos estamos refiriendo a muchas más cosas:

- Fallo en las comunicaciones
- Fallo humanos
- Incumplimiento de una ley o reglamento
- Accesos no autorizados
- Virus, troyanos que inundan la red.
- Fallos de sistemas
- Intrusos
- Problemas eléctricos en las instalaciones
- etc.

Para proteger la información de manera coherente y eficaz es necesario definir un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema se basa en el análisis de riesgos del negocio que permite garantizar:

- Confidencialidad: Asegurar que sólo accederá a la información quién esté autorizado
- Integridad: Asegurar que la información es correcta
- Disponibilidad: Asegurar que los datos estarán accesibles cuando los usuarios requieran de ella.

Podemos pensar, y es lógico, que todo lo anteriormente comentado sólo genera gasto. Esto no es así, la seguridad también aporta beneficios:

- Reducción de costes: Cuánto podría costar la solución de un incidente de seguridad. Con la implantación de seguridad no sólo reducimos este riesgo sino que optimizamos los servicios ya que tenemos una visión general de todos los elementos que conforman el servicio que se ofrece.
- Cumplimiento legal: Cada vez existen más leyes de aplicación a la seguridad de la información.
- Garantía de continuidad de negocio
- Mejora la imagen con respecto a otras Universidades

Es obvio que la seguridad total es inalcanzable, sin embargo, debemos reducir los riesgos. Esta reducción de riesgos se consigue mediante un proceso de mejora continua.

Este proceso de mejora deberá ir documentado. La norma ISO/IEC 27000 es un conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización. Está basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Todo esto nos permitirá conocer mejor nuestra organización, cómo funciona y que podemos hacer para mejorarla.

1.2 Esquema General del Diseño de Red MPLS

Como se ha comentado anteriormente, este Trabajo Fin de Grado es continuación de otro: DISEÑO DE RED MPLS que daba solución para las comunicaciones de la Universidad de Málaga usando la tecnología MPLS. MPLS son las siglas de Multiprotocol Label Switching. MPLS es una tecnología de túnel que lo que hace es coger una trama, la encapsula y la envía. Algunas de las ventajas que ofrece:

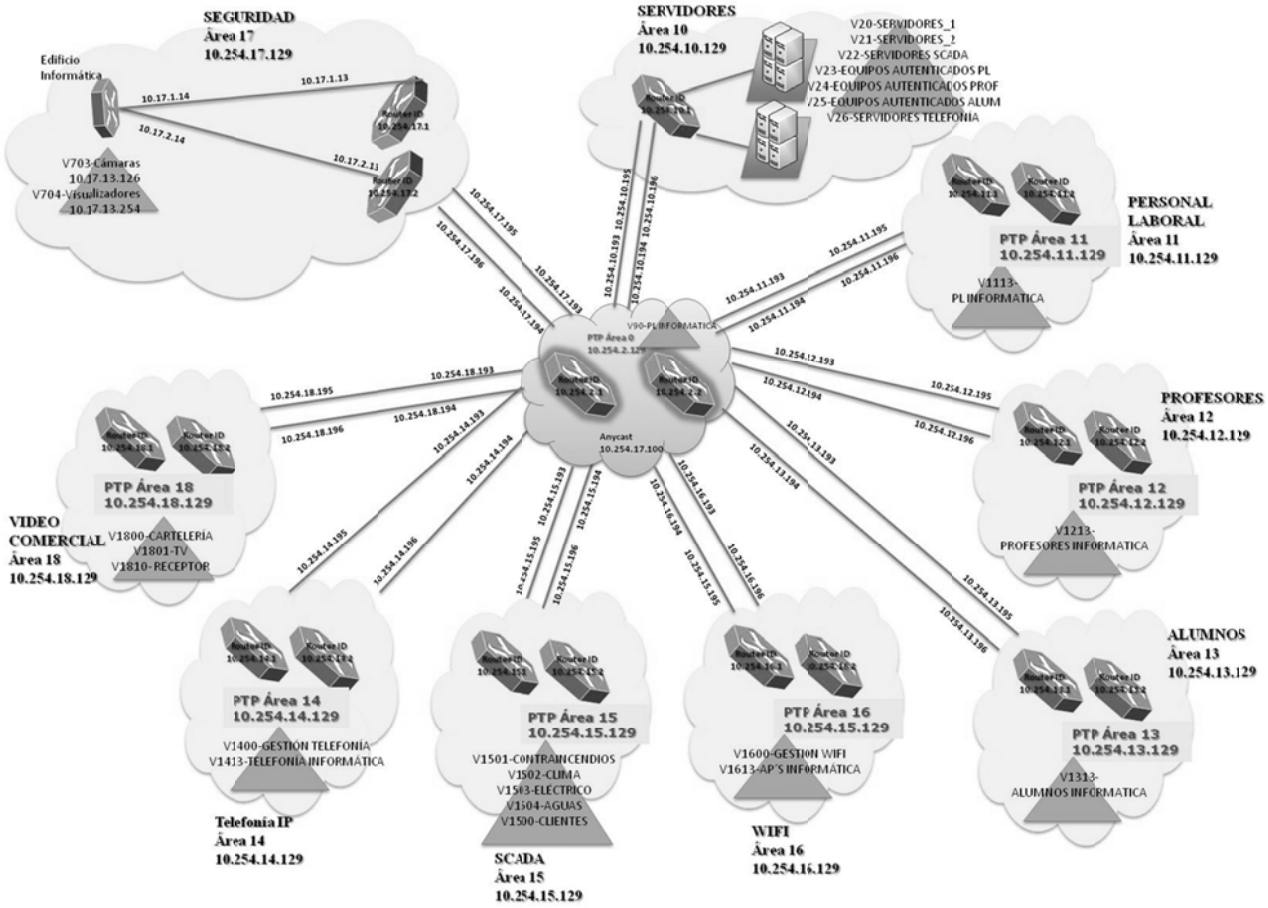
- ✓ Redundancia
- ✓ Flexibilidad
- ✓ Crecimiento
- ✓ Multiprotocolo

Con esta tecnología se pretendía cubrir las necesidades de comunicación de los siguientes servicios:

- Telefonía
  - Permite la comunicación telefónica mediante teléfonos IP.
- Wifi
  - Permite el acceso a los datos a través de equipos inalámbricos
- Datos
  - Permite el acceso a los datos de cualquier gremio (profesores, alumnos y personal laboral)
- SCADA
  - Permite el control de los sistemas de mantenimiento de una forma centralizada
- Cámaras de seguridad
  - Visualización de cámaras IP desde cualquier ubicación de la Universidad.
- TV

- Permite visualizar televisión desde cualquier ubicación de la Universidad

El esquema general de red que se planteó en su momento fue el siguiente:



Cada nube del esquema representa un router virtual. En cada router virtual es donde se encuentran las distintas vlanes del servicio. Hay dos routers a tener en cuenta:

- Router central: es el que permite que desde cualquier punto de la red se pueda acceder a cualquier otro punto de la red
- Router servidores: detrás de él se encontraría la mayor parte de servidores (DHCP, DNS, etc.).

2 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. ISO 27001

Una vez que se tiene claro que hay que implementar medidas de seguridad, el siguiente paso es decidir cómo establecer esta seguridad. Es obvio que tenemos que elegir una normativa ya vigente.

2.1 Un poco de historia

Las ISO/IEC 27000 son un conjunto de estándares desarrollador por el Organismo Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que proporcionan un marco de gestión de seguridad de la información utilizable por cualquier tipo de organización

A primeros de la década de los 90, el departamento de comercio de Industria del Reino Unido inicia el desarrollo de una norma británica (BS) para proteger y regular la gestión de la seguridad en la empresa, y como respuesta a las peticiones de la industria, el gobierno y los comerciantes para crear una estructura común de seguridad de la información. La primera norma fue aprobada oficialmente en 1995 (BS 7799:95) y nace como un código de buenas prácticas para la gestión de seguridad de la información, es decir, no se establecía un esquema de certificación. En 1998 se publica la segunda parte (BS 7799-2), la cual estableció una serie de requisitos para ser certificable por una entidad independiente. Ambas partes son revisadas en 1999.

En aquella época, la organización Internacional de Normalización (ISO) comienza a interesarse por la norma. Así en el año 2000 ISO aprueba la norma ISO 17799 parte 1 que es el código de práctica para los requisitos de seguridad de la información no certificable. Esta norma está formada por un conjunto completo de controles que conforman las buenas prácticas de seguridad de la información y que pueden ser aplicadas por toda organización

con independencia de su tamaño. En 2002 se revisa la parte 2 (la certificable) de la BS 7799-2:2002) con el fin de armonizarla con otros normas de gestión tales como ISO 9001:2000 y la ISO 14001:1996, así como con los principios de la Organización para la cooperación y el desarrollo económicos (OCDE).

Este mismo año (2002) la norma es publicada como norma UNE (UNE-EN ISO /IEC 17799/1.2002) sin apenas modificación y se establece exclusivamente en España otra norma, la UNE 71502.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, este esquema cambia de nombre y se publica por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

La última versión de ISO 27001 es la de octubre de 2013 y es sobre la que trabajaremos.

En España y como ley de obligado cumplimiento para las administraciones públicas tenemos el Esquema Nacional de Seguridad (ENS-Real Decreto 3/2010) que trata la 'protección' de la información y los servicios, contempla y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión.

ISO y ENS difieren en su naturaleza, en su ámbito de aplicación, en su obligatoriedad y en los objetivos que persiguen. Mientras la ISO es una normativa, el ENS es una ley, esto es, una empresa certificada en ISO no puede decir que esté cumpliendo el ENS aunque si es cierto que está muy cerca de cumplirla.

2.2 Esquema General de la ISO 27001

La norma ISO/IEC 27001:2013 tiene los siguientes capítulos:

- Capítulo 0 Introduction: Se indica que la seguridad es un proceso de mejora continua y se obliga a ello. En esta versión no se obliga a que se a PDCA[1]. Sigue siendo necesario un objetivo, una medición y un seguimiento.
- Capítulo 1 Scope: Los controles del anexo A se pueden tomar como referencia pero no son de obligado cumplimiento
- Capítulo 2 Normative references: La ISO/IEC 27001 hace referencia al conjunto de normas 27000
- Capítulo 3 Terms y definitions: Los términos y las definiciones de la ISO/IEC 27000 son de aplicación
- Capítulo 4 Context of the organization: Hay que explicar claramente:
    - a qué se dedica la organización,
    - cómo funciona y las partes que la componen
    - lo que esperamos del SGSI con todo lo que se indica anteriormente

[1] PDCA: Es una estrategia de mejora continua en 4 pasos:
Plan (Planificar): Se buscan las posibles mejoras y se planifica como realizarlas.
Do (Hacer): se realizan las mejoras anteriormente indicadas
Check (Verificar): Una vez implantada la mejora se deja un tiempo de verificación
Act (Actuar): Se estudian los resultados obtenidos y si son buenos se implantan definitivamente, en caso contrario se estudian nuevas mejoras

Es muy importante que la organización haga un esfuerzo en este apartado ya que de él se podrá obtener el funcionamiento real y así como establecer estas dependencias

- Capítulo 5 Leadership: Se requiere una gran implicación por parte de la alta dirección
- Capítulo 6 Planning: Realizar el análisis y la evaluación de riesgo. Puedo elegir cualquier fórmula matemática, sólo se pide que esté documentada
- Capítulo 7 Support: Se refiere sobre todo a los recursos humanos. Hay que proporcionar todos los medios necesarios, establecer competencias, comunicar y concienciar al personal toda la información relevante sobre la gestión de la seguridad de la información. También se describe cómo debe ser la documentación sobre el SGSI.
- Capítulo 8 Operation: Cumplimiento del plannning para mitigar el riesgo.
- Capítulo 9 Performance evaluation: Monitoreo, medición… de las acciones realizadas. Se pide también realizar auditorías internas. Toda esta información debe ser revisada por la alta administración.
- Capítulo 10 Improvement: Acciones correctivas y no conformidades así como las continuas mejoras.

En el presente capítulo se describe como aplica la normativa al diseño de red propuesto en el proyecto anterior.

3 APLICACIÓN SGSI ISO/IEC 27001

3.1 Política de seguridad de la información

Objetivo: El primer documento que debe tener un SGSI es donde se identifica la actividad de la empresa, la importancia de la seguridad, los objetivos a cubrir y sobre todo que cuenta con el respaldo de la alta dirección. Además se debe presentar un listado de roles y responsabilidad

La Universidad de Málaga se dedica a la enseñanza. La enseñanza se realiza tanto presencial como online permitiendo a los alumnos el seguimiento de las clases en casa. Para ello es necesario generar una infraestructura de comunicaciones que permita no sólo que alumno pueda hacer el seguimiento de las clases, sino también todo el sistema de gestión de alumnos, mantenimiento de edificios, comunicaciones telefónicas, etc.

La información, en la comunidad universitaria, es un recurso que debe ser protegido garantizando el acceso al mismo, minimizando los riesgos y contribuyendo a una mejor gestión de la Universidad.

Para que esto suceda es necesaria la implantación de una política de seguridad. Esta política debe contar con el apoyo de todos los colectivos que trabajan para y por la Universidad. El objetivo de esta política de Seguridad debe ser la de proteger los recursos de información de la Universidad frente a amenazas internas o externas, deliberadas o accidentales con el fin de asegurar la confidencialidad, la integridad y la disponibilidad.

Esta política sustenta la implantación de un Sistema de Gestión de Seguridad de la Información apoyada en la ISO/IEC 27001. Esta política está aprobada por la máxima Dirección de la Universidad y se apoya directamente en el responsable de seguridad.

La Dirección aprueba esta política así como los objetivos marcados en la misma.

El alcance de la presente política de seguridad se centrará en las comunicaciones de datos de la Universidad. Los elementos que constituyen las redes de comunicaciones de la Universidad son los siguientes:

- Cableado: Compuesto por el cableado físico tanto en cobre, como en fibra óptica instalados en los racks de los centros de cableado así como en las canalizaciones.
- Dispositivos de comunicaciones: son los dispositivos a los que se conectan los elementos que componen la red (teléfonos, ordenadores, PLC's, etc.).
- Centros de cableado: locales donde se encuentran ubicados los elementos finales de rosetas así como los dispositivos de comunicaciones.

Es obvio que toda documentación relacionada con la seguridad de la información y los datos que tratan tienen un carácter confidencial y sólo está permitido su uso y difusión con carácter interno y por personal autorizado.

La política de seguridad es un proceso continuo de mantenimiento y acciones a realizar. Para ello existirá un comité de seguridad que organizará reuniones periódicas de seguimiento para ver el estado actual y la tendencia de la implantación y mantenimiento de la política de seguridad. Además, se organizarán reuniones semestrales con la Dirección Informática. En estas reuniones se marcarán objetivos, se presentará a la Dirección el estado actual del plan así como nuevas incidencias que hayan podido surgir. Posteriormente se establecerán nuevas metas.

Se realizarán reuniones mensuales entre Seguridad y los diferentes responsables de las distintas áreas.

En la política de seguridad estará involucrado todo el personal. A continuación se fijan los trabajos:

- Dirección:
  - ✓ Aprobar la política y los objetivos.
  - ✓ Conocer y aprobar los riesgos residuales.
  - ✓ Revisión del SGSI.
  - ✓ Apoyar y promover la cultura de seguridad dentro de la organización.
- Responsable de seguridad:
  - ✓ Coordinadas las tareas y esfuerzos en materia de seguridad.
  - ✓ Centralizar todos los aspectos de seguridad de la organización.
  - ✓ Informar a la Dirección sobre avances de implantación así como de nuevas medidas a tomar.
  - ✓ Dar a conocer esta política de seguridad para que cualquier persona conozca y comprenda la política y los procedimientos que apliquen a su trabajo.
- Comité de seguridad:
  - ✓ Tratan los problemas de seguridad y las no conformidades.
  - ✓ Identifican los cambios significativos y cómo deben ser gestionados.
  - ✓ Valorar si los controles implantados son suficientes.
  - ✓ Coordinan la implantación de nuevos controles.
  - ✓ Proponen objetivos a la Dirección revisando la marcha de los mismos.
- Responsables de áreas de informática:
  - ✓ Coordinarse con el responsable de seguridad para llevar a cabo las actividades.
  - ✓ Incluir los requisitos para nuevos desarrollos de los aspectos de seguridad que apliquen.
  - ✓ Asegurarse de los niveles de disponibilidad requeridos así como que solo las personas autorizadas accedan a la información.

- Trabajador en la organización:
  - ✓ Mantenerse informado de los procedimientos y protocolos de seguridad.
  - ✓ No realizar ninguna infracción de seguridad.
  - ✓ Comunicar las incidencias de seguridad de forma inmediata.
- Personal Externo:
  - ✓ Deben conocer y entender la política de seguridad en lo que les afecta con su relación con la organización.
  - ✓ Cumplir las normativas de seguridad.
  - ✓ Comunicar las incidencias de seguridad que detecten.

3.2 Análisis de Riesgos

3.2.1 Activos

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. Un activo de información es aquel elemento que contiene o manipula información.

Los activos se usan para dar un servicio, esto es, el proceso de negocio. Antes de pasar a definir los activos, vamos a especificar el proceso de negocio al que dan soporte las comunicaciones de una Universidad.

PROCESO DE NEGOCIO (SERVICIOS)		
Cod	Nombre	Descripción
S-01	Datos	Incluye los datos que manejan: -PAS (base de datos, correo, almacenamiento de documentos, etc.) -Profesores (toda la documentación que le permite investigación y docencia) -Alumnos (permite a los alumnos acceder a correo y servicios disponibles para su docencia).
S-02	Telefonía	Comunicación telefónica
S-03	SCADA	Gestión de los sistemas de mantenimiento
S-04	Seguridad	Visualización de cámaras de seguridad
S-05	TV	Cartelería, visualización de canales de televisión

Los activos se han clasificado en:

Activo	**Descripción**
Información	Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización. También se englobará en este apartado las configuraciones de los equipos.
Software	Software que se usa para la gestión
Físico	Equipos usados para gestionar las comunicaciones
Instalaciones	Lugares donde se encuentran ubicados los sistemas de información
Servicios	Aire acondicionado, corriente, etc.

Con esto el inventario de activos quedaría de la siguiente manera:

COD	NOMBRE	DESCRIPCIÓN	TIPO	PROPIETAR	LOCALIZAC
IA-01	SR7750	Equipamiento nivel 3	Físico	Responsable Comunicaciones	CC Principales
IA-02	Firewall	Equipamiento de seguridad	Físico	Responsable Comunicaciones	CC Principales
IA-03	ESS7450	Equipamiento nivel 2	Físico	Responsable Comunicaciones	CC Principales
IA-04	Omniswitches USUARIOS	Switches de acceso a usuarios	Físico	Responsable Comunicaciones	Centro de cableado
IA-05	Omniswitches VIDEO	Switches de acceso para cámaras de seguridad	Físico	Responsable Comunicaciones	Centro de cableado
IA-06	Servidor de control	Servidores que permiten la configuración de los sistemas. Por ejemplo: -video: permiten la configuración de canales -centralita permite la configuración de opciones de los teléfonos	Físico	Responsables de Sistemas y Comunicaciones	CPD
IA-07	Servidores de gestión	Equipamiento que permite el control de alarmas de los sistemas	Físico	Responsables de Sistemas y Comunicaciones	CPD
IA-08	Aplicaciones de monitorización	Aplicaciones que permiten la monitorización de los sistemas	Software	Responsable Comunicaciones	CPD
IA-09	Aplicaciones de control	Aplicaciones que permiten la modificación de los sistemas	Software	Responsable Comunicaciones	CPD
IA-10	Software de los equipos de comunicación	Sistema operativo de los switches, routers, etc.	Software	Responsable Comunicaciones	Servidores
IA-11	Centros de cableado	Ubicación de equipamiento de comunicaciones	Instalaciones	Responsable Comunicaciones	Facultades
IA-12	CPD	Ubicación de todos los servidores y de los equipos de comunicac de CPD	Instalaciones	Responsable Comunicaciones	Centro de cálculo

IA-13	Cableado UTP	Llevan la conectividad al usuario	Físico	Responsable Comunicaciones	Todas las instalaciones
IA-14	Cableado FIBRA	Llevan la conectividad a grandes distintas (entre centros de cableado)	Físico	Responsable Comunicaciones	Todas las instalaciones
IA-15	Cuadros eléctricos	Ofrecen la corriente eléctrica a los distintos dispositivos	Servicios	Responsable de Mantenimiento	Centros de cableado
IA-16	Aire Acondicionado	Permite que los equipos no se apaguen por calor	Servicios	Responsable de Mantenimiento	Centros de cableado/CPD
IA-17	Ficheros con configuraciones	Configuraciones de los equipos de comunicaciones	Servicios	Responsable de comunicaciones	Equipamiento

.

Este apartado es una exigencia del SGSI y tal y como indica la norma no debe existir información duplicada. Para aplicar esto a la parte de inventario debemos complementar la información proporcionada por el SGSI con el inventario de material de la organización. El inventario de la organización debe contar con la siguiente información:

Electrónica de datos:

- Part number: Es el código que indica el artículo. Este código identifica al tipo de equipo de manera única.
- Número de serie: Identifica al producto de manera única (entre dos dispositivos del tipo). Es importante de cara a la garantía del fabricante y a la posible reposición del mismo si se tiene con el fabricante un mantenimiento hardware.
- Fecha adquisición del producto: Control de garantías.
- Histórico de donde ha pasado un equipamiento.
- Dentro de un chasis hay componentes gbic, tarjetas, mda, etc. también se debe indicar los números de serie y part-number de estos dispositivos así como la ubicación.
- Regleta de corriente donde está cada fuente de alimentación.

Servidores de gestión y control:

- Sistemas operativos
- Hardware
- Licencias
- Procedimientos de configuración e instalación del software genérico.
- Requisitos mínimos del software

Centros de cableado:

- Plano con ubicación de los centros de cableado.
- Listado de parcheos de cobre (roseta con slot/puerto)
- Listado de parcheos de fibra.
- Ubicación en plano de rosetas
- Ubicación en plano de bandejas de fibra y cobre
- Ubicación en planos de recorridos de fibra y cobre
- Listado de arquetas, banco de tubos, etc.
- Mapas de rack (U en la que va cada dispositivo)

La relación entre cómo afectan los activos al proceso de negocio puede verse en la siguiente tabla:

		PN-01 Datos	PN-02 Telefonía	PN-03 SCADA	PN-04 Seguridad	PN-05 TV
IA-01	SR7750	X	X	X	X	X
IA-02	Firewall	X	X	X	X	X
IA-03	ESS7450	X	X	X	X	X
IA-04	Omniswitches USUARIOS	X	X	X		X
IA-05	Omniswitches VIDEO				X	
IA-06	Servidores de control					
IA-07	Servidores de gestión					
IA-08	Aplicaciones de gestión					
IA-09	Aplicaciones de control					
IA-10	Software de los equipos de comunicaciones	X	X	X	X	X
IA-11	Centros de cableado	X	X	X	X	X
IA-12	CPD	X	X	X	X	X
IA-13	Cableado UTP	X	X	X	X	X
IA-14	Cableado FIBRA	X	X	X	X	X
IA-15	Cuadros eléctricos	X	X	X	X	X
IA-16	Aire Acondicionado	X	X	X	X	X
IA-17	Ficheros con configuraciones	X	X	X	X	X

Si nos fijamos en el esquema no existe un FIREWALL. Ya se planteó en el proyecto anterior la mejora de sustituir el router virtual de servidores por un firewall físico. Si bien es cierto que este cambio puede generar una menor capacidad en el tránsito de paquetes (cada uno de ellos será examinado), sí puede mejorar los registros de quién accede a qué información.

3.2.2 Valoración de los activos

Son las características que hacen valioso a un activo. El valor del activo se puede cuantificar de muchas formas: coste del activo, imagen de la empresa, etc. en nuestro caso, la valoración que recibe un activo es la medida del perjuicio para la organización si el activo se ve dañado, es decir, la disponibilidad del activo. La disponibilidad de un activo responde a la pregunta: ¿qué ocurriría si un activo no estuviera disponible?

Las referencias tomadas son las siguientes:

10	Daño extremadamente grave. Debe estar disponible el 99,9% del tiempo
9	Daño muy grave. Existen equipos redundantes. Fallo de todos los equipos llevaría a caída total del sistema
8	Daño grave. Fallo total de un solo servicio.
7	Daño muy alto. Un grupo de usuarios podrían verse afectados en varios servicios
6	Daño alto. Un grupo de usuarios podría verse afectado en un servicio
5	Daño medio. Un usuario afectado por un servicio
3 y 4	Daño menor
1 y 2	Daño muy bajo
0	Despreciable

La valoración de la disponibilidad en los activos quedaría de la siguiente manera:

CODIGO	NOMBRE	Valor (VA)	Descripción
IA-01	SR7750	9	Existe equipamiento que redunda el fallo de un nodo.
IA-02	Firewall	9	No se tendría acceso a los servidores. La mayoría de los servicios fallarían. Existe equipamiento que redunda el fallo de un nodo.
IA-03	ESS7450	9	Existe equipamiento que redunda el fallo de un nodo
IA-04	Omniswitches USUARIOS	7	Si falla un switch perderían la red todos los usuarios de ese switch.
IA-05	Omniswitches VIDEO	6	Si falla ese switch las imágenes de esas cámaras no podrían ser grabadas ni visualizadas
IA-06	Servidores de control	4	El sistema seguiría funcionando pero no se podría gestionar ni realizar modificaciones en el sistema.
IA-07	Servidores de gestión	2	No se recibirían alarmas y no se podría realizar un mantenimiento preventivo automático pero los sistemas seguirían funcionando.
IA-08	Aplicaciones de gestión	4	No se podría evolucionar ni actuar sobre el sistema, sin embargo, el mismo estaría funcionando.
IA-09	Aplicaciones de control	2	No se recibirían alarmas y no se podría realizar un mantenimiento preventivo automático pero los sistemas seguirían funcionando.
IA-10	Software de los equipos de comunicaciones	9	Un fallo en el software podría provocar reinicios del equipamiento.
IA-11	Centros de cableado	7	La caída de un CC haría que una facultad perdiera el acceso a las aplicaciones
IA-12	CPD	9	La caída de un CPD no debería de producir un fallo total del sistema pero se perdería la redundancia y los balanceos del sistema no podrían funcionar bien.
IA-13	Cableado UTP	7	La rotura de una bandeja de comunicaciones podría hacer que un CC no diera servicio.
IA-14	Cableado FIBRA	7	La rotura de una bandeja de comunicaciones podría hacer que un CC no diera servicio.
IA-15	Cuadros eléctricos	9	La pérdida del suministro eléctrico podría generar problemas en los equipos.
IA-16	Aire Acondicionado	9	Igual que anterior.
IA-17	Ficheros con configuraciones	9	Un fallo en los ficheros de configuraciones podría hacer que ante un reinicio del equipo este no arrancar de forma correcta.

3.2.3 Análisis de los riesgos

Análisis de riesgos es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

La ocurrencia de un riesgo es la siguiente:

Probabilidad	Descripción
5	Muy probable
3	Probable
1	Poco Probable

Las amenazas que se han identificado son las siguientes:

CODIGO	RIESGO	DESCRIPCIÓN	Amenaza (A)
RI-01	Desastres	Fuego, daños por agua, fallos en obras, contaminación electromagnética, etc.	1
RI-02	Robo	Robo de los equipos.	1
RI-03	Contaminación mecánica	Polvo o suciedad.	5
RI-04	Avería de origen físico o lógico	Fallo en el hardware/software.	3
RI-05	Corte del suministro eléctrico	Cese de alimentación.	3
RI-06	Condiciones inadecuadas de temperatura o humedad	Falta de climatización de la sala	3
RI-07	Errores de administradores	Equivocaciones de personas con responsabilidades de instalación y operación.	3
RI-08	Errores en la monitorización	Falta de registros o de la revisión de los mismo.	3
RI-09	Escapes de Información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	3
RI-10	Vulnerabilidades del software	Defectos en el código que dan pie a una operación defectuosa. Posible software con bugs. Entrada de virus a un servidor de monitorización o de gestión.	3
RI-11	Agotamiento de los recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	3
RI-12	Accesos no autorizados	Personal no autorizado accede a datos o equipamiento. Podría escuchar o manipular equipos.	3

3.3 Gestión, tratamiento y valoración de los riesgos. Selección de los controles.

Una vez que conocemos los riesgos y decidido el tratamiento que se le va a dar se deben tomar acciones en consecuencia. Son cuatro tipos de tratamiento:

- Mitigar el riesgo: Reducirlo mediante la implantación de controles.
- Asumir el riesgo: La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable. Los riesgos asumidos han de ser controlados y revisados para que no se conviertan en riesgos mayores.
- Transferir el riesgo a un tercero: Subcontratando el servicio.
- Eliminar el riesgo: Puede ser difícil o costosa.

Según lo exigido por la norma, se deben documentar los controles seleccionados, su aplicación, así como aquellos que no han sido seleccionados y los motivos por los que han sido rechazados.

A continuación vamos a indicar los controles elegidos para mitigar los riesgos.

A.5.5.1 Policies for information security

Responsable: Alta Dirección.
Esta realizado en el apartado 2.1

A.5.5.2 Review of the policies for information security

Responsable: Alta Dirección.
Esta realizado y es el primer documento de este SGSI.

A.8.8.1 Inventory of assets

Responsable: Comunicaciones.
Esta realizado en apartados anteriores.

A.8.8.2 Ownership of assets

Responsable: Comunicaciones
Esta realizado en apartados anteriores.
Nos referimos no solo al material que está en producción sino también al que está en el almacén.

El responsable del inventario o la persona en quien delegue, deberá llevar un control de la entrada y salida del material anotando al menos fecha, dispositivo, part-number y número de serie e indicando el motivo de la entrada. Además de firma y fecha de la persona que entrega o retira material. Las revisiones del material en producción y en almacén se realizarán de forma trimestral. Es muy importante también en este sentido tener la fecha de adquisición de cada elemento así como la duración de la garantía. Cuando hablamos de garantía podemos hablar tanto de la garantía de la adquisición del producto o la garantía hardware que el fabricante nos ofrece mediante la realización de un acuerdo.

A.9.1.1 Access control policy

Responsable: Comunicaciones.
Se debe establecer una política de control de acceso de los usuarios. Profesores, personal laboral, etc. tendrá acceso a los recursos que necesiten pero, no por ejemplo a las cámaras de seguridad. Esta política deberá establecerse para asegurar así que los usuarios sólo acceden a los recursos que necesiten.
Esta política debe venir de la alta Dirección. Tal vez puede ocurrir que un miembro del personal laboral necesite acceder a cámaras de seguridad. Esto puede generar evidentes problemas de seguridad o tal vez un cambio en el diseño de la red.

A.9.1.2 Access to networks and network services

Responsable: Comunicaciones.
Dos controles:
1.-La red debe ser capaz de verificar qué usuarios tienen privilegios para acceder a los segmentos de datos. Además debe controlar que nadie ponga un portátil en una roseta activa y tenga servicio. Para ello, una de las posibles soluciones es integrar 802.1x. la configuración básica podría ser la siguiente
1.- Habilitar los puertos de usuarios como móviles ya que no sabemos qué usuario se conectará y qué vlan necesitará
vlan port mobile <slot/port>
2.- Habilitar 802.1x en los puertos
vlan port 3/1 802.1x enable
3.- Indicar los servidores Radius (se deberán indicar al menos dos).
aaa radius-server <NOMBRE_DEL_RADIUS> host <IP_DEL_SERVIDOR_RADIUS> key <CONTRASEÑA_IGUAL_PARA RADIUS> retransmit 3 timeout 2 auth-port 1812 acct-port 1813
4.-Asociar el Radius con 802.1X
aaa authentication 802.1x <NOMBRE_DEL_RADIUS>

El proceso sería el siguiente: un usuario enciende su ordenador, el puerto de la electrónica lo detecta y el switch solicita al servidor RADIUS si tiene acceso. Si es así la electrónica lo pondrá en la vlan que le indique el RADIUS (es por ello el puerto móvil) y en caso contrario le denegará el acceso o lo dejará en una vlan aislada o simplemente no le dará ninguna conectividad.
2.- Instalación de un firewall.
Ya se comentó que en el diseño pondríamos un firewall sustituyendo el router virtual de servidores. Se puede ver los logs de ip origen y destino. Con los logs que genere el firewall podremos ver realmente si no hay algún agujero de seguridad.

A.9.4.3 Password management system

Responsable: Comunicaciones y personal que gestione el Directorio Activo.
Debe existir una política para las contraseñas. Al menos contendrá:
A todos los usuarios el directorio activo les obligará a cambiar la contraseña cada 3 meses respetando unas reglas (ser al menos de 8 caracteres con algúna en mayúsculas, número, signo de puntación, etc.) Esto implica que los administradores también tendrán que cambiar.
Además las contraseñas de root y admin locales serán cambiadas al menos de forma anual.

A.11.1.1 Physical security perimeter

Responsable: Dirección. Debe permitir locales independientes.
Los centros de cableado y CPD deben estar en un local con llave o tarjetero de seguridad. Así mismo las personas que gestionan los sistemas también deberían estar en una sala aislada de oficinas comunes.

A.11.1.2 Physical entry controls

Responsable: Seguridad
El seguimiento de este control lo realizará Seguridad (quién y cuándo accede, facilitar el acceso, etc.) si bien es cierto que el responsable de comunicaciones podrá solicitar que se habilite o no algún acceso.
Esta seguridad debe contemplar:
1.-Normativa que indique quién tiene privilegios para acceder.
2.-Seguimiento de las personas que acceden.

A.11.2.1 Equipment siting and protection

Responsable: Comunicaciones
El acceso a locales de comunicaciones debe estar protegido mediante control de acceso. Además, todo el equipamiento debe estar en racks cerrados con llave.
Por otro lado y como una nueva barrera de defensa, los equipos no deben permitir que una persona acceda a la gestión de los mismos por el simple hecho de estar físicamente junto al equipo. La forma de conexión (consola) debe estar también securizada mediante una contraseña (RADIUS o en su caso local).
Por otro lado, las personas que tienen acceso a estas instalaciones deben tener en cuenta lo que no se puede realizar en los centros de cableado. Para ello es conveniente definir mediante procedimientos cómo se debe actuar en un centro de cableado. Varios ejemplos:
-En un centro de cableado no se puede comer o fumar..,
-Ante una obra civil los equipos deben de taparse
-Antes trabajos programados de corriente eléctrica los equipos deberán ser apagados de forma ordenada etc.

A.11.2.2 Supporting utilities

Responsable: Comunicaciones

Debe existir una normalización para un centro de cableado. En esta se debe incluir:

- Suelo o techo técnico
- Los equipos presentados en el anterior Proyecto Fin de Carrera disponen de doble fuente de alimentación, así es posible que desde dos líneas de corriente distintas puedan estar alimentados. Esto además se puede reforzar con SAI's en cada entrada. Los equipos deben tener toma a tierra (las condiciones de humedad y temperatura deberían estar resueltas. También debería contar un sistema contra incendios. CENELEC EN 50173-5-ISO/IEC24764).
- Los equipos de capa de usuarios tiene conexión a red a través de dos enlaces (3 equipos en capa de transporte)
- Hay dos equipos que realizan routing y que en caso de fallo de uno de ellos, el otro sería capaz de asumir la carga (implementación del protocolo VRRP).

A.11.2.3 Cabling security

Responsable: Comunicaciones

Se refiere tanto al cableado como a la instalación del mismo. Esto implica entre otros:

- ✓ Máxima torsión de fibra
- ✓ Cableado anti roedores y ignifugo
- ✓ Distribución de cableado en bandejas y en el rack
- ✓ Etc.

El cableado además debería estar etiquetado e identificado

Si bien es cierto que no existe una ley para la instalación del cableado, si existe una serie de normativas de buenas prácticas. Por ejemplo:

A continuación se presentan solo las españolas:

- REALES DECRETOS Y ÓRDENES MINISTERIALES
  - Ncb-cpi96 norma básica de la edificación sobre las condiciones de protección de incendios.
  - Reglamento electrotécnico de baja tensión (REBT)
  - Reglamento de la protección de datos (LOPD)
  - Reglamento de telecomunicaciones (ICT)
  - Compatibilidad electromagnética (EMC)
  - Interferencia electromagnética (EMI)
- NORMATIVA ESPAÑOLA PUBLICADA POR AENOR
  - UNE EN 50173-1:2005. tecnología de información. sistemas de cableado genéricos.
  - UNE EN 50310:2007. aplicación de las redes equipotenciales y de las puestas a tierra en los edificios con equipos de tecnologías de la información.
  - UNE EN 50174-1:2001. tecnología de la información. instalación del cableado. especificación y aseguramiento de la calidad.
  - UNE EN 50174-2:2001. tecnología de la información. instalación del cableado. métodos de planificación de la instalación en el interior de los edificios.
  - UNE EN 50174-3:2005. tecnología de la información. instalación del cableado. métodos de planificación de la instalación en el exterior de los edificios.
  - UNE EN 50346:2004. tecnología de la información. instalación de cableado. ensayo de cableados instalados.
  - BOJA 215:31 octubre 2007. cableado estructurado en edificios de la junta de Andalucía

A.11.2.4 Equipment maintenance

Responsable: Comunicaciones

Se debe hacer un buen mantenimiento de la red. Debe incluir:

- Mantenimiento de los equipos: el fabricante de los equipos debe proporcionar un listado de tareas a realizar en los mismos en cuanto a limpieza física de los mismos.
  También debe realizar al menos una auditoría por año en cuanto a configuración. Estas auditorías deberán incluir ancho de banda, revisión de configuraciones, eliminar configuraciones no necesarias (por ejemplo eliminar vlanes que no se usen), estado de CPU y memoria de los equipos, etc.
- Mantenimiento del cableado: revisión de los parcheos tanto utp como fibra eliminando los que no son necesarios
- Revisión del estado de SAI, aire acondicionado, iluminaria, etc.
- Limpieza del local.

A.12.1.1 Document operating procedures

Responsable: Comunicaciones

Todas las actuaciones, configuraciones, instalaciones, etc. deben estar documentadas. Por ejemplo:

- ✓ Expandir una vpls/vlan y sus parámetros spanning tree.
- ✓ Alta/baja de servicios incluyendo planos y esquemas
- ✓ Backups de los sistemas y recuperación de los mismos.
- ✓ Base de datos con errores y forma de proceder ante los mismos.
- ✓ etc.

A.12.1.2 Change management

Responsable: Comunicaciones

Los cambios en el sistema deben realizarse con una planificación. Por ejemplo, nuevos interfaces en el firewall no deben realizarse sin ser programados. Estos cambios se realizarán en horario de menor afección.

A.12.1.4 Separation of development, testing and operational environments

Responsable: Comunicaciones

Se debe tener un entorno de pruebas. Por ejemplo, al actualizar una versión de toda la electrónica esta debe ser probada en un entorno de pruebas. Al mismo tiempo se debe sacar el procedimiento de actualización.

A.12.2.1 Controls against malware

Responsable: Comunicaciones

Dos posibles controles:

1.-Parámetros de seguridad de la electrónica: la electrónica dispone de configuraciones que protegen a los equipos de posibles ataques. Algunos de ellos:

- Evitar bucles mediante mac-move y protocolos de stp
- Evitar ataques DoS

- Encriptación de protocolos de nivel 3.
- No permitir más de una mac por puerto
- Eliminar tramas bpdu o de ospf de alguna electrónica que no sea propia de la red.
- etc.

2.-La electrónica, mediante dispositivos auxiliares es capaz de poder recoger información sobre qué software hay instalado en cada equipo y si no cumple los requisitos mínimos lo dejaría en un segmento de cuarentena. Esto es, el equipo se conecta a la red, el usuario verifica su usuario y tiene acceso, tras esto, se verifica en el equipo que tiene instalado el antivirus actualizado, parches del sistema operativo y que no tiene ningún otro tipo de software. Si esto no es así, al equipo se le deja en una vlan de cuarentena para que pueda instalar todo el software necesario.

A.12.3.1 Information backup

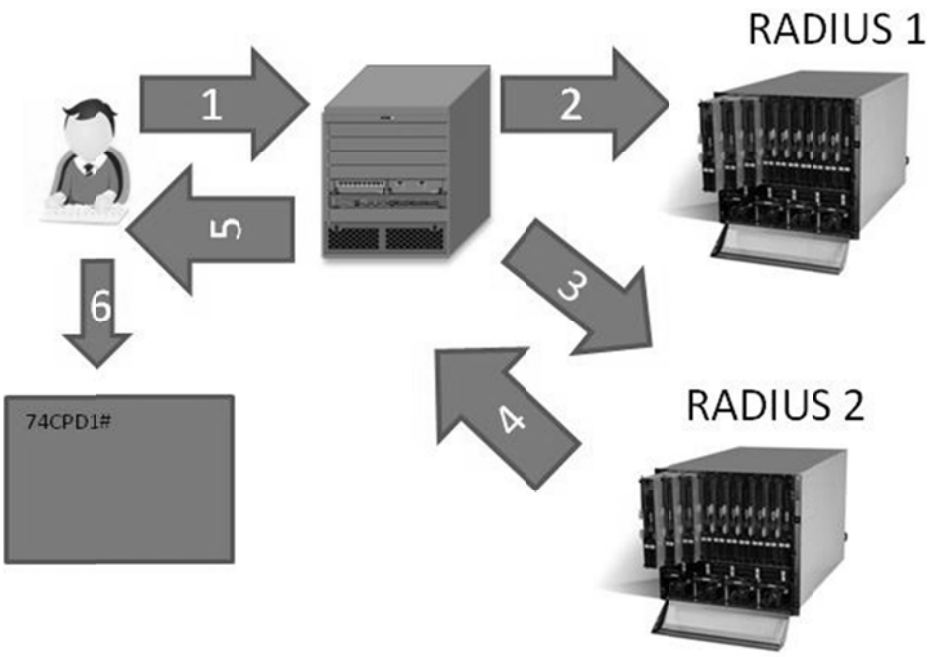
Responsable: Comunicaciones
Las copias de seguridad de la configuración de la electrónica deberían hacerse de forma diaria. También se debería revisar que este procedimiento diario se realiza y comprobar que realmente funciona usando equipos de almacén

A.12.4.3 Administrator and operator logs

Responsable: Comunicaciones

Una parte importante para la seguridad es la forma de control de acceso para gestión de los dispositivos. Esto es lo que se llama AAA (authentication, authorization, and accounting). Básicamente se trata de controlar quién accede a estos equipos para configurarlos y saber qué se hace en cada acceso. Cada equipo posee una base de datos propia en la cual se almacena usuario y contraseña. Se supone que serán varios los usuarios que accederán a la gestión de los equipos de comunicaciones, así que un primer paso sería configurar varios usuarios. Esto no es óptimo, lo mejor sin duda es poder usar el mismo usuario del directorio activo, para lo cual necesitaríamos un servidor RADIUS por ejemplo.

Evidentemente serían varios los RADIUS a configurar. El esquema lógico sería el siguiente:



El usuario que se quiere conectar inicia la sesión ssh a la dirección IP de gestión de la electrónica. La electrónica le solicita el user y el password. El usuario introduce el usuario y contraseña de dominio, así la electrónica consulta en su primer servidor Radius que tiene configurado, si este no le responde irá al segundo servidor Radius el cual será capaz de conectarse al directorio activo y dar o no el OK de acceso. Si la autenticación es correcta el usuario será capaz de poder loguearse y ejecutar los comandos que necesite. Esta electrónica también permite la creación de perfiles. En este caso, cuando hablamos de perfil nos referimos al conjunto de comandos que un usuario puede usar.

A continuación procedemos a describir cómo sería la configuración de este modo de autenticación para los omniswitches:

- En la electrónica hay que dar a conocer el Radius e indicar que los accesos serán a través del mismo.

aaa radius-server <NOMBRE DEL RADIUS> host <IP_DEL_SERVIDOR_RADIUS> key <CONTRASEÑA_IGUAL_PARA RADIUS> retransmit 3 timeout 2 auth-port 1812 acct-port 1813

aaa authentication ssh <NOMBRE DEL RADIUS> "local"

- Servidor RADIUS:

Añadir la dirección IP de la electrónica a controlar usando la misma contraseña que se puso en la línea de comandos anterior.

Indicar el código del fabricante (800 en el caso de Alcatel)

Configurar los distintos perfiles que el servidor Radius tiene que devolver teniendo en cuenta que los comando son solamente una suma

-> show aaa priv hexa
file = 0x00000001 0x00000000,
telnet = 0x00000008 0x00000000,
dshell = 0x00000020 0x00000000,
debug = 0x00000040 0x00000000,
domain-admin = 0x00000069 0x00000000, Es la suma de los anteriores
...

Si la electrónica no tuviera acceso a ningún equipo RADIUS que pudiera validarlo, entonces solo miraría la base de datos que tiene el propio equipo.

A.12.4.4 Clock Synchronisation

Responsable: Comunicaciones

Todos los dispositivos de comunicaciones deben estar con la hora sincronizada. Es vital, por ejemplo, para la revisión de logs.

Es obvio que se hace necesario un servidor que ofrezca este servicio. Los servidores del directorio activo pueden ser una buena solución. El comando en la electrónica a aplicar sería el siguiente:

Ntp server <DIRECCIÓN_IP_SERVIDOR>

3.4 Valoración de los riesgos.

La valoración de riesgos trata de cuantificar el peligro real. Para cuantificar se hace uso de los siguientes parámetros:

- (VA) Es el valor que hemos dado anteriormente al activo.
- (A) La amenaza es la probabilidad que tiene que se produzca la amenaza (calculada anteriormente).
- (VI) La vulnerabilidad es cómo de expuesto está el activo. Para el caso inicial supondremos que no tenemos aplicado ningún objetivo así la vulnerabilidad será máxima.

Valor	Vulnerabilidad
5	Muy vulnerable
3	Vulnerable
1	Poco vulnerable

- (RI) Es el riesgo inicial. Su valor sale de multiplicar:

  VA*A*VI

  Una vez aplicados una serie de controles el peligro real debe bajar, así

- (VC) es la vulnerabilidad a la que queda expuesto el activo tras aplicar una serie de controles. Es VI pero reducido según estimación por aplicación de los controles
- (RS) Es el riesgo residual. Este valor es una estimación de aplicar un control a este activo para disminuir su vulnerabilidad, su amenaza o ambas. Su valor sale de multiplicar:

  VA*A*VC. Hay que establecer el valor umbral del RS. Estimamos aceptamos un valor de RS inferior a 40.

A continuación se presenta una relación de riesgos y controles que intentarán reducir los mismos:

		A.8	A.9	A.11	A.12
RI-01	Desastres	x			
RI-02	Robo	x		x	x
RI-03	Contaminación mecánica	x		x	
RI-04	Avería de origen físico o lógico	x			x
RI-05	Corte del suministro eléctrico	x		x	
RI-06	Condiciones inadecuadas de temperatura o humedad	x		x	
RI-07	Errores de administradores	x	x		x
RI-08	Errores en la monitorización	x			x
RI-09	Escapes de Información	x	x	x	
RI-10	Vulnerabilidades del software	x			x
RI-11	Agotamiento de los recursos	x		x	
RI-12	Accesos no autorizados	x	x	x	

Las siguientes tablas muestran los valores anteriormente comentados aplicados a cada activo y a cada amenaza, esto es, cómo bajo el riesgo inicial aplicando los controles.

IA-01	SR7750	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

IA-02	Firewall	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

IA-03	ESS7450	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

IA-04	Omniswitches USUARIOS	VA	A	VI	VC	RI	RS
RI-01	Desastres	7	1	5	1	35	7
RI-02	Robo	7	1	5	1	35	7
RI-03	Contaminación mecánica	7	5	5	1	175	35
RI-04	Avería de origen físico o lógico	7	3	5	1	105	21
RI-05	Corte del suministro eléctrico	7	3	5	1	105	21
RI-06	Condiciones inadecuadas de temperatura o humedad	7	3	5	1	105	21
RI-07	Errores de administradores	7	3	5	1	105	21
RI-08	Errores en la monitorización	7	3	5	1	105	21
RI-09	Escapes de Información	7	3	5	1	105	21
RI-10	Vulnerabilidades del software	7	3	5	1	105	21
RI-11	Agotamiento de los recursos	7	3	5	1	105	21
RI-12	Accesos no autorizados	7	3	5	1	105	21

IA-05	Omniswitches VIDEO	VA	A	VI	VC	RI	RS
RI-01	Desastres	6	1	5	1	30	6
RI-02	Robo	6	1	5	1	30	6
RI-03	Contaminación mecánica	6	5	5	1	150	30
RI-04	Avería de origen físico o lógico	6	3	5	1	90	18
RI-05	Corte del suministro eléctrico	6	3	5	1	90	18
RI-06	Condiciones inadecuadas de temperatura o humedad	6	3	5	1	90	18
RI-07	Errores de administradores	6	3	5	1	90	18
RI-08	Errores en la monitorización	6	3	5	1	90	18
RI-09	Escapes de Información	6	3	5	1	90	18
RI-10	Vulnerabilidades del software	6	3	5	1	90	18
RI-11	Agotamiento de los recursos	6	3	5	1	90	18
RI-12	Accesos no autorizados	6	3	5	1	90	18

IA-06	Servidores de control	VA	A	VI	VC	RI	RS
RI-01	Desastres	4	1	5	1	20	4
RI-02	Robo	4	1	5	1	20	4
RI-03	Contaminación mecánica	4	5	5	1	100	20
RI-04	Avería de origen físico o lógico	4	3	5	1	60	12
RI-05	Corte del suministro eléctrico	4	3	5	1	60	12
RI-06	Condiciones inadecuadas de temperatura o humedad	4	3	5	1	60	12
RI-07	Errores de administradores	4	3	5	1	60	12
RI-08	Errores en la monitorización	4	3	5	1	60	12
RI-09	Escapes de Información	4	3	5	1	60	12
RI-10	Vulnerabilidades del software	4	3	5	1	60	12
RI-11	Agotamiento de los recursos	4	3	5	1	60	12
RI-12	Accesos no autorizados	4	3	5	1	60	12

IA-07	Servidores de gestión	VA	A	VI	VC	RI	RS
RI-01	Desastres	2	1	5	1	10	2
RI-02	Robo	2	1	5	1	10	2
RI-03	Contaminación mecánica	2	5	5	1	50	10
RI-04	Avería de origen físico o lógico	2	3	5	1	30	6
RI-05	Corte del suministro eléctrico	2	3	5	1	30	6
RI-06	Condiciones inadecuadas de temperatura o humedad	2	3	5	1	30	6
RI-07	Errores de administradores	2	3	5	1	30	6
RI-08	Errores en la monitorización	2	3	5	1	30	6
RI-09	Escapes de Información	2	3	5	1	30	6
RI-10	Vulnerabilidades del software	2	3	5	1	30	6
RI-11	Agotamiento de los recursos	2	3	5	1	30	6
RI-12	Accesos no autorizados	2	3	5	1	30	6

IA-08	Aplicaciones de gestión	VA	A	VI	VC	RI	RS
RI-01	Desastres	4	1	5	1	20	4
RI-02	Robo	4	1	5	1	20	4
RI-03	Contaminación mecánica	4	5	5	1	100	20
RI-04	Avería de origen físico o lógico	4	3	5	1	60	12
RI-05	Corte del suministro eléctrico	4	3	5	1	60	12
RI-06	Condiciones inadecuadas de temperatura o humedad	4	3	5	1	60	12
RI-07	Errores de administradores	4	3	5	1	60	12
RI-08	Errores en la monitorización	4	3	5	1	60	12
RI-09	Escapes de Información	4	3	5	1	60	12
RI-10	Vulnerabilidades del software	4	3	5	1	60	12
RI-11	Agotamiento de los recursos	4	3	5	1	60	12
RI-12	Accesos no autorizados	4	3	5	1	60	12

IA-09	Aplicaciones de control	VA	A	VI	VC	RI	RS
RI-01	Desastres	2	1	5	1	10	2
RI-02	Robo	2	1	5	1	10	2
RI-03	Contaminación mecánica	2	5	5	1	50	10
RI-04	Avería de origen físico o lógico	2	3	5	1	30	6
RI-05	Corte del suministro eléctrico	2	3	5	1	30	6
RI-06	Condiciones inadecuadas de temperatura o humedad	2	3	5	1	30	6
RI-07	Errores de administradores	2	3	5	1	30	6
RI-08	Errores en la monitorización	2	3	5	1	30	6
RI-09	Escapes de Información	2	3	5	1	30	6
RI-10	Vulnerabilidades del software	2	3	5	1	30	6
RI-11	Agotamiento de los recursos	2	3	5	1	30	6
RI-12	Accesos no autorizados	2	3	5	1	30	6

IA-10	Software de los equipos de comunicaciones	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

IA-11	Centros de cableado	VA	A	VI	VC	RI	RS
RI-01	Desastres	7	1	5	1	35	7
RI-02	Robo	7	1	5	1	35	7
RI-03	Contaminación mecánica	7	5	5	1	175	35
RI-04	Avería de origen físico o lógico	7	3	5	1	105	21
RI-05	Corte del suministro eléctrico	7	3	5	1	105	21
RI-06	Condiciones inadecuadas de temperatura o humedad	7	3	5	1	105	21
RI-07	Errores de administradores	7	3	5	1	105	21
RI-08	Errores en la monitorización	7	3	5	1	105	21
RI-09	Escapes de Información	7	3	5	1	105	21
RI-10	Vulnerabilidades del software	7	3	5	1	105	21
RI-11	Agotamiento de los recursos	7	3	5	1	105	21
RI-12	Accesos no autorizados	7	3	5	1	105	21

IA-12	CPD	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

IA-13	Cableado UTP	VA	A	VI	VC	RI	RS
RI-01	Desastres	7	1	5	1	35	7
RI-02	Robo	7	1	5	1	35	7
RI-03	Contaminación mecánica	7	5	5	1	175	35
RI-04	Avería de origen físico o lógico	7	3	5	1	105	21
RI-05	Corte del suministro eléctrico	7	3	5	1	105	21
RI-06	Condiciones inadecuadas de temperatura o humedad	7	3	5	1	105	21
RI-07	Errores de administradores	7	3	5	1	105	21
RI-08	Errores en la monitorización	7	3	5	1	105	21
RI-09	Escapes de Información	7	3	5	1	105	21
RI-10	Vulnerabilidades del software	7	3	5	1	105	21
RI-11	Agotamiento de los recursos	7	3	5	1	105	21
RI-12	Accesos no autorizados	7	3	5	1	105	21

IA-14	Cableado FIBRA	VA	A	VI	VC	RI	RS
RI-01	Desastres	7	1	5	1	35	7
RI-02	Robo	7	1	5	1	35	7
RI-03	Contaminación mecánica	7	5	5	1	175	35
RI-04	Avería de origen físico o lógico	7	3	5	1	105	21
RI-05	Corte del suministro eléctrico	7	3	5	1	105	21
RI-06	Condiciones inadecuadas de temperatura o humedad	7	3	5	1	105	21
RI-07	Errores de administradores	7	3	5	1	105	21
RI-08	Errores en la monitorización	7	3	5	1	105	21
RI-09	Escapes de Información	7	3	5	1	105	21
RI-10	Vulnerabilidades del software	7	3	5	1	105	21
RI-11	Agotamiento de los recursos	7	3	5	1	105	21
RI-12	Accesos no autorizados	7	3	5	1	105	21

IA-15	Cuadros eléctricos	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

IA-16	Aire Acondicionado	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

IA-17	Ficheros con configuraciones	VA	A	VI	VC	RI	RS
RI-01	Desastres	9	1	5	1	45	9
RI-02	Robo	9	1	5	1	45	9
RI-03	Contaminación mecánica	9	5	5	1	225	45
RI-04	Avería de origen físico o lógico	9	3	5	1	135	27
RI-05	Corte del suministro eléctrico	9	3	5	1	135	27
RI-06	Condiciones inadecuadas de temperatura o humedad	9	3	5	1	135	27
RI-07	Errores de administradores	9	3	5	1	135	27
RI-08	Errores en la monitorización	9	3	5	1	135	27
RI-09	Escapes de Información	9	3	5	1	135	27
RI-10	Vulnerabilidades del software	9	3	5	1	135	27
RI-11	Agotamiento de los recursos	9	3	5	1	135	27
RI-12	Accesos no autorizados	9	3	5	1	135	27

4 CONCLUSIONES Y FUTURAS MEJORAS

Como se comentó al principio el alcance de este TFG está solo limitado a las comunicaciones. Para continuar con este trabajo habría que seguir los siguientes pasos:

- Realizar toda la documentación y procedimientos indicados.
- Realizar una planificación en tiempo y coste.
- Establecer responsabilidades
- Iniciar la ejecución de los trabajos.

Posteriormente y una vez implantado habría que ver el estado real de la seguridad en la red y si los valores residuales se ajustan con los calculados.

De forma paralela, es muy importante establecer el plan de continuidad de negocio (PCN), esto es, hay que establecer una serie de pruebas anuales las cuales indiquen que toda la redundancia descrita anteriormente es cierta. Posibles pruebas para este plan:

- Apagar un centro de cableado principal: esto implica la caída de un 7750SR y un 7450ESS de forma simultánea. Todos los servicios deben recuperarse en cuestión de milisegundos.
- Comprobar el estado de las SAI's, estado de las fuentes de alimentación.
- Realizar procedimiento de caso de incendio en uno de los centros de cableado:
    - Saber dónde están ubicadas todas las rosetas (conociendo cuáles son más críticas), esto es, hay que dar servicio primero a las tomas más críticas y posteriormente al resto. Por ejemplo: las rosetas de cámaras son más críticas que las de vídeo comercial.
    - Conocer los caminos de fibra y distancia.
    - Comprobar que las salvaguardas de la configuración de los equipos es correcta.
    - Revisión de inventario.

Todo lo anterior facilita además la contratación de empresas para la realización de los trabajos y materiales.

Existen muchas las formas de ampliar y/o continuar este TFG:

- La principal es la de cómo realizar la conectividad desde fuera de la Universidad para cualquier personal (profesores, alumnos, personal de mantenimiento y seguridad. Suponemos que la conectividad desde fuera debe ser de una única forma (evitar módems, routers por vlan, etc.) y se debe limitar que cada usuario acceda donde realmente necesita. También hay que incluir el formulario de acceso así como quién da la autorización.
- Añadir nuevos elementos al presente TFG: centralita telefónica, cámaras de seguridad, sistemas SCADA, etc.
- Añadir más controles: 113 controles son los que tiene la ISO 27001:2013 y se han realizado la introducción de menos de 20.
- Añadir nuevos riesgos (se pueden ver en la guía MAGERIT).

El presente TFG ha intentado dos cosas:

- Que el diseño de red sea seguro. Para ello se ha bajado a la misma configuración de los equipos.
- Iniciar el proceso de certificación: se establece una serie mínima de controles los cuales podrán ampliarse posteriormente para toda la organización

Al realizar un diseño de red se tiene que definir los servicios a proporcionar. Hablar con los fabricantes de los dispositivos que van a conectar para estudiar sus necesidades (por ejemplo ancho de banda, nivel 3, etc.). Una vez que tenemos los servicios funcionando también hay que estudiar quién tendrá acceso a la gestión y mantenimiento de los sistemas anteriores teniendo en cuenta que

un mismo colectivo puede requerir acceder a varios sistemas… y esto es sólo el principio. Una vez implantada la red van surgiendo nuevas necesidades, nuevos sistemas y nuevos requerimientos.

Durante la lectura del presente trabajo fin de grado se ha ampliado el significado de la palabra seguridad. Ahora no sólo intentamos evitar que alguien pueda romper la seguridad y recoger información o simplemente provocar una caída del sistema, o en el caso de la Universidad que un alumno pueda cambiar las notas de su carrera. Ahora además, tenemos que cumplir con la normativa legal y procurar una continuidad del negocio.

Con el presente trabajo de fin de grado se ha conseguido lo anterior: teniendo un diseño de red ya seguro en cuanto a redundancia en el sistema, se han establecido la seguridad mínima necesaria para este diseño llegue a convertirse en realidad. Durante la implantación es normal que surjan modificaciones, estas no deben ser sustanciales ya que si no estaríamos hablando de una mala política de seguridad.

Hemos conseguido una seguridad física (locales independientes y controles de entrada) y una seguridad lógica (redundancia, encriptación de protocolos, quién accede a la configuración y qué comandos ejecuta, etc.).

La seguridad es un proceso continuo. Una vez implantada, hay que revisarla, ver los puntos fuertes y débiles e ir mejorando este camino.

La política de seguridad son los pilares para una red de comunicaciones segura. Sin el apoyo de la alta Dirección los pilares no serían sólidos y además no tendríamos una ruta.

BIBLIOGRAFÍA

- 7750_SR_OS_Triple_Play_Guide_R6.1-r1-04-01
- 7450_ESS_OS_Routing_Protocols_Guide_R6.1-r1-05-01
- 7450_ESS_OS_Services_Guide_R6.1-r1-05-01
- 7450_ESS_OS_System_Basics_Guide_R6.1-r1-05-01
- 7750_SR_OS_Routing_Protocols_Guide_R6.1-r1-05-01
- 7750_SR_OS_Triple_Play_Guide_R6.1-r1-04-01
- OmniSwitch 6800_6850_9000 CLI Reference Guide
- OmniSwitch 6800_6850_9000 Network Configuration Guide
- OmniSwitch 6800_6850_9000 Switch Management Guide
- http://www.pdcahome.com/5202/ciclo-pdca/
- MAGERIT:

  http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- www.microsoft.com

  http://www.iso27000.es/
- http://www.iso27000.es/iso27000.html
- http://www.iso27000.es/sgsi.html
- Centro criptológico nacional

  https://www.ccn.cni.es/
- Esquema Nacional de Seguridad

  http://administracionelectronica.gob.es/ctt/ens#.VGwaFofMnXQ
- Gómez Fernández, Luis. *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*

  . Madrid : AENOR, 2012. 216 pág. ISBN 9788481437492
- Academia de Networking de CisCo System, Fundamentos de seguridad de redes

  Cisco Press 2004, 832 pag, ISBN 84-205-4540-6

- AENOR (Asociación Española de Normalización y Certificación). *Modelo para el gobierno de las TIC basado en las normas ISO.*

  436 pág. ISBN: 9788481437904

- Alan Calder. *Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide, 2nd Edition*

  Van Haren PublishingVAN. 75 pág. ISBN: 9789087535414