UNIVERSIDAD DE CANTABRIA

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

MÁSTER OFICIAL EN EMPRESA Y TECNOLOGÍAS DE LA INFORMACIÓN

CURSO ACADÉMICO 2012-2013

TRABAJO FIN DE MÁSTER

ESTUDIO DE SISTEMAS DE SEGURIDAD BASADO EN LA DETECCIÓN DE INTRUSIÓN FÍSICA Y TECNOLÓGICA

Autor

D. RICARDO ARANDA LUENGO

Director

D. ALBERTO ELOY GARCÍA GUTIÉRREZ

Santander, Octubre 2013

UNIVERSIDAD DE CANTABRIA

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

OFFICIAL MASTER IN BUSINESS AND TECHNOLOGIES INFORMATION

CURSO ACADÉMICO 2012-2013

TRABAJO FIN DE MÁSTER

STUDY OF SECURITY SISTEMS BASED INTRUSION DETECTION PHYSICAL AND TECHNOLOGICAL

Autor

D. RICARDO ARANDA LUENGO

Director

D. ALBERTO ELOY GARCÍA GUTIÉRREZ

Santander, Octubre 2013

A mis padres,

por apoyarme en todo

y ayudarme tanto.

A mi novia Marina,

por ser tan importante para mí

y estar siempre a mi lado.

Por último a Alberto,

por haberme ofrecido un proyecto como éste.

ESTUDIO DE SISTEMAS DE SEGURIDAD BASADO EN LA DETECCIÓN DE INTRUSIÓN FÍSICA Y TECNOLÓGICA

Resumen:

Toda persona u organización requiere de seguridad tanto física como tecnológica. A lo largo de estos últimos años han aumentado las tecnologías y los sistemas de seguridad empleados son cada vez más eficaces.

El objetivo de este proyecto es el análisis y estudio de todos los sistemas de seguridad cuya finalidad es la misma: prevenir y actuar ante cualquier intrusión física y lógica.

Desde hace unos meses formo parte del equipo de Ingeniería de Seguridad de la empresa ITM Sistemas: empresa con una dilatada experiencia en la seguridad integral de todo tipo de instalaciones. Este estudio es una motivación personal como ampliación a mis conocimientos de la seguridad física y aplicaciones actuales de la seguridad privada. Esta motivación deriva del interés y adquisición de conocimientos de seguridad informática dada su relación con la seguridad física pero en su aplicación lógica.

Un claro ejemplo de aplicación de los dos tipos de seguridad es la integración de las grabaciones de las cámaras de tecnología IP a través de la nube.

Con el avance de las tecnologías de la información y, con ello, la integridad, confidencialidad y disponibilidad de las mismas en redes internas y externas, es necesaria la implantación de medidas cada vez más complejas que garanticen la seguridad tanto física como lógica de toda información de vital importancia.

Como objeto de este proyecto se analizará y estudiará la propuesta de un *Sistema de Seguridad Integral* como un único sistema, fruto de la unificación de los sistemas de seguridad física y los sistemas de seguridad informática. Este sistema puede tenerse en cuenta frente al desarrollo del Plan de Seguridad a implantar en una instalación cualesquiera.

STUDY OF SECURITY SISTEMS BASED INTRUSION DETECTION PHYSICAL AND TECHNOLOGICAL

Abstract:

Any person or organization requires both physical and technological security. Over the last few years have increased the technologies and safety systems used are increasingly effective.

The objective of this project is the analysis and studies of all security systems whose purpose is the same: to prevent and respond to any logical and physical intrusion. For a few months I am part of the team of Safety Engineering Systems ITM Company: Company with extensive experience in comprehensive security all facilities. This study is a personal motivation as an extension to my knowledge of physical security and current applications of private security. This motivation comes from the interest and knowledge acquisition computer security as it relates to the physical safety but with their application logic.

A clear example of application of the two types of security is the integration of camera recordings IP technology through the cloud.

With the advancement of information technology and thus the integrity, confidentiality and availability of the same internal and external networks, it is necessary to implement increasingly complex measures to ensure the physical and logical security of all vital information importance.

As the object of this project will analyze and study the proposal of a Comprehensive Security System as a single system, the result of the unification of physical security systems and security systems. This system can be considered ahead of any safety plan to be implemented in any installation.

Índice de figuras:

Índice de tablas:

Palabras Clave: IDS (Sistema de Detección de Intrusos), IP (Protocolo de Internet), CCTV (Circuito Cerrado de Televisión), SGSI (Sistema de Gestión de Seguridad de la Información)…

Key-words: IDS (Intrusion Detection System), IP (Internet Protocol), CCTV (Closed Circuit Television), SGSI (Information security Management System)…

Índice:

MOTIVACIÓN Y OBJETIVOS

El objetivo de este proyecto es desarrollar un estudio completo del estado actual de la seguridad tanto en el mundo real con la aplicación cada vez más de las nuevas tecnologías, así como del mundo virtual, definiendo éste como todo lo que se transmite a través de la red con nuestros dispositivos tecnológicos.

La razón del desarrollo de este proyecto viene dada por el interés acerca de la seguridad informática y de los mecanismos actuales de protección a través de la red. De mis conocimientos de seguridad física y las aplicaciones que se están desarrollando e instalando, así como desde la aparición de las comunicaciones IP y su amplio recorrido y alcance en numerosas aplicaciones tecnológicas, nace mi interés por los sistemas que protegen toda la información que circula por la red y la posibilidad de agrupar todos los mecanismos en una única plataforma, buscando reducir la complejidad de los sistemas y aumentar la eficiencia y eficacia de la seguridad.

ORGANIZACIÓN DE LA MEMORIA

En el primer capítulo se realiza una introducción de las áreas que abarca la seguridad y términos que mencionaremos a lo largo del proyecto.

En el segundo capítulo se hace mención al estado actual de la seguridad física y tecnológica.

El tercer capítulo se centra en una introducción teórica del nuevo modelo de negocio en la nube o “Cloud Computing”.

En el cuarto capítulo se desarrolla una breve descripción de los Sistemas de Detección de Intrusos, haciendo hincapié en los sistemas de detección de intrusos en la red.

En el quinto capítulo se muestran las políticas de seguridad y normativas aplicables tanto a la seguridad física como a la seguridad informática.

En el sexto capítulo se muestra una visión holística de la seguridad, objetivo de análisis y estudio de este proyecto.

En el séptimo capítulo se describen los sistemas de seguridad y sus funciones con el objetivo de su integración y análisis desde una única plataforma.

En el octavo y último capítulo se hará un recopilatorio de las conclusiones obtenidas del proyecto y propuesta de líneas de futuros trabajos.

1. INTRODUCCIÓN

El estado del arte de los sistemas de seguridad actual engloba todo tipo de intrusión, sabotaje y uso no autorizado de una instalación o información pública o privada. Hoy en día las empresas funcionan gracias a la información que manejan en el mercado.

En el estudio actual se analizan todos los ámbitos de la seguridad física, tecnológica e informática. Todo elemento físico o lógico está expuesto a un riesgo de robo o sabotaje. Es por ello por lo que se debe disponer de todas las medidas de protección posibles que garanticen el mayor grado de seguridad. Ese grado de protección no solo contempla la seguridad física, a través de Internet se puede robar o sabotear información de gran importancia, de la misma forma que ocurre a través del medio físico.

A continuación se detallan los posibles riesgos que nos podemos encontrar, así como el tipo de protección y elementos de seguridad aplicables en base al tipo de amenaza.

1.1. Seguridad y Riesgos

La expresión seguridad, se define en su primera acepción, en el Diccionario de la Real Académica Española como: "cualidad de seguro, lo que nos remite al adjetivo seguro para completar la comprensión del concepto, siendo seguro un adjetivo que califica al sustantivo, como libre y exento de todo peligro, daño o riesgo" [1].

Esto nos lleva a profundizar más en el concepto de seguridad y llegar a la conclusión de su definición en base a su aplicación a diferentes situaciones, objetos y actividades.

En el estudio actual haremos referencia al concepto seguridad como "protección del riesgo".

Aparecen los conceptos de sujeto agente y sujeto paciente de la seguridad. Es por ello que, según el grado de seguridad, un sujeto paciente, o lo que es lo mismo, el objeto de protección, está protegido frente al riesgo al que nos enfrentamos, que será el objeto agente de la seguridad.

Una vez definido el sujeto paciente de una protección (objeto a proteger) se analizarán y estudiarán los riesgos (sujeto agente) que le afectan.

El objeto de toda seguridad, es decir, el sujeto paciente, es el elemento a proteger. Cada uno de ellos tiene unos requerimientos específicos y diferenciados, lo cual nos llevará a un análisis y estudio específico frente a los riesgos que amenazan a cada uno de ellos, es decir, prevenir que todo riesgo se convierta en daño. Según su naturaleza, podemos distinguir:

- Seguridad aplicada a las personas.
- Seguridad aplicada a las cosas materiales, incluso medio ambiente.
- Seguridad aplicada a las cosas inmateriales (información, paisaje).

1.2. Protección física, electrónica e informática

En el ámbito de la seguridad, tanto la protección física, electrónica como la protección informática están relacionadas entre sí optimizando la máxima seguridad tanto física como tecnológica. La complementación de todas ellas será objeto de nuestro estudio y análisis.

1.2.1. Protección física

La protección física es un método de aplicación de la seguridad, que por su naturaleza y función, no ofrece información de su actividad, que además es estática y, por tanto, sólo reacciona ante una agresión, oponiendo resistencia.

Aunque todos, de manera intuitiva, seamos capaces de reconocer un elemento o un sistema de protección física no lo somos para definirlo y diferenciarlo de manera concreta.

La seguridad física empezó a avanzar por cuestiones de robo, vandalismo..., hoy en día grandes y pequeñas empresas disponen de sistemas de seguridad física más o menos complejos:

- Vigilantes de seguridad
- Control de accesos físicos
- Sistemas de intrusión física

- Sistemas de CCTV

El único inconveniente que presentan los sistemas de protección física radica en la imposibilidad de generar información, por lo que deben ser complementados con otros sistemas.

No se concibe un entorno seguro frente a cualquier riesgo, que no esté protegido por elementos físicos. No es imaginable proteger contra una intrusión un entorno abierto, a no ser en condiciones muy especiales y con la posibilidad de una respuesta inmediata.

Para la demostración y justificación de cualquier objeto de riesgo protegido mediante sistemas de protección física es necesaria la complementación con elementos de protección electrónica, cuya función sirva de apoyo físico demostrable en cualquier momento posterior al riesgo.

1.2.2. Protección electrónica

En contraposición con la protección física, la protección electrónica se caracteriza por ser capaz de generar información. Es decir, es el proceso de aplicación de métodos y elementos de seguridad, que generan información.

La protección electrónica se distingue y diferencia fácilmente, al observar que los elementos destinados a su aplicación, están constituidos por componentes electrónicos de la más diversa naturaleza, según sean las características de su aplicación.

Es un método de seguridad, por tanto, protege a un bien de los riesgos para los que ha sido diseñado el sistema, aunque hay que aclarar que esta protección en la mayor parte de los casos la ejerce soportada en elementos de protección física.

En su funcionamiento generan información, que nosotros la podremos asimilar a diferentes situaciones: reposo, alarma, aviso, etc. Se basan en dispositivos electrónicos y, por tanto, son capaces de transmitir esa información a distancia y así, hacerla útil. Esta información, por sí sola, no tiene trascendencia y, por ello, precisa de elementos de transmisión para hacerla útil para el propósito diseñado.

Permiten una gran variedad de aplicaciones, entre ellas, las que precisan contar con facilidades informáticas.

Este tipo de protección es denominada en muchos textos como protección activa.

Las características más sobresalientes de los sistemas de protección electrónica, son los siguientes:

- Generan información.
- Son elementos necesarios para la protección en cooperación con los medios físicos.
- Aportan eficiencia a la seguridad.

1.2.3. Protección informática

La protección informática o protección de tecnologías de la información se enfoca en la seguridad de la infraestructura computacional, centrándose tanto en la información contenida como circulante.

Para su aplicación existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes, cuyo fin es minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada [2].

Por lo tanto, la información es el principal activo y objeto de amenaza en un sistema informático y en las aplicaciones de la Seguridad Informática debemos proteger:

- Hardware: conjunto de todos los sistemas físicos del sistema informático.
- Software: todos los elementos lógicos que hacen funcionar el hardware.
- Datos: información lógica que maneja el software y el hardware.

1.3. Terminología

Sistema CCTV: Sistema de Circuito Cerrado de Televisión.

Firewall o cortafuegos: Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se encarga de monitorizar todas las comunicaciones que se realizan desde o hacia el equipo o la red y decide si las permite dependiendo de las reglas establecidas por el administrador del sistema.

IDS (Intrusion Detection Systems): Un IDS es un sistema que intenta detectar y alertar sobre las intrusiones intentadas en un sistema o en una red, considerando intrusión a toda actividad no autorizada o que no debería ocurrir en ese sistema. No sólo, bloquea o permite conexiones sino que analiza dichas conexiones para detectar si alguna de ellas es portadora de contenido peligroso para el equipo o para la red. Además, es capaz de categorizar las distintas amenazas e informar al administrador del sistema siguiendo una lista de reglas y heurísticas.

Sniffer: Programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador. Supone una amenaza grave para la seguridad no sólo de una máquina sino también de toda una red.

Intrusión: Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.

Detección de intrusos: Análisis automático de parámetros que modelan la actividad de un entorno con el propósito de detectar e identificar intrusiones.

Spoofing: En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad, generalmente con usos maliciosos o de investigación.

Spam: Correo electrónico no solicitado enviado masivamente por parte de un tercero.

Hacker: Persona dedicada a la investigación y exploración de las redes y sistemas, capaz de acceder a ordenadores externos de forma remota.

Denegación de Servicio: En seguridad informática, un ataque de denegación de servicios, también llamado ataque DoS (de las siglas en inglés *Denial of Service*), es un ataque a un

sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Malware**:** Abreviatura de **"***Malicious software",* término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

Phishing: Técnica que consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

2. SISTEMAS DE INTRUSIÓN FÍSICA Y TECNOLÓGICA

La seguridad física y tecnológica ha ido avanzando con las nuevas tecnologías. No sólo es vital la seguridad física de las personas o empresas, la evolución de las redes de comunicaciones junto con las Tecnologías de la información hacen que para los ciudadanos y, sobre todo, para las empresas sea imprescindible la implantación de sistemas de seguridad frente a posibles ataques y usos indebidos de información.

2.1. Situación actual

Como referencia de nuestro análisis actual de la seguridad partimos de datos reales extraídos del Instituto Nacional de Estadística en España (INE) [3].

Introduciéndonos en la situación que ocupan las TIC y el uso de Internet tenemos la siguiente información [4]:

- El 71,5% de los hogares españoles con al menos un miembro de 16 a 74 años tiene conexión a Internet.
- El uso de TIC ha aumentado en los últimos años y el perfil del usuario de Internet se ha ampliado, cada vez se han ido incorporando nuevos públicos a la red.
- El 97,29% de los internautas ha recibido una cadena de e-mail, de autoría anónima, con información alarmista sobre un servicio o producto con la petición de ser reenviado.
- Al 84,16 de los internautas les preocupa la seguridad de sus datos privados en Internet.

Algunos de los peligros más comunes a los que se expone el usuario de Internet es la pérdida de control de sus datos personales, la exposición a virus y fraudes económico.

Tal como ocurre en la vida real, en la vida virtual o Internet también se producen estafas, robos, virus y fraudes económicos.

Sin una buena política de seguridad el internauta siempre estará en una situación de desprotección respecto a la seguridad de su información personal. Por ello, es necesario

disponer de medios tecnológicos eficaces con la capacidad de alertar situaciones sospechosas y velar por nuestra seguridad.

La Tabla 1 muestra la situación actual de la seguridad física española de los últimos años, para la cual se obtienen datos estadísticos de criminalidad utilizados por la Oficina Estadística de la Unión Europea (EUROSTAT) [5].

NACIONAL	ANUAL		
TIPOLOGÍA PENAL	2011	2012	Var. % 12/11
1.-DELITOS Y FALTAS (EU)	2.285.525	2.268.665	-0,7
2.-HOMICIDIOS DOLOSOS Y ASESINATOS CONSUMADOS (EU)	385	363	-5,7
3.-DELINCUENCIA VIOLENTA (EU)	109.429	117.139	7,0
3.1.-ROBO CON VIOLENCIA E INTIMIDACIÓN (EU)	87.718	96.855	10,4
4.-ROBOS CON FUERZA	414.961	405.930	-2,2
4.1.-ROBOS CON FUERZA EN DOMICILIOS (EU)	100.780	126.419	25,4
5.-SUSTRACCIÓN VEHÍCULOS A MOTOR (EU)	60.061	55.350	-7,8
6.-TRÁFICO DE DROGAS (EU)	15.220	14.510	-4,7
7.-DAÑOS	254.361	246.391	-3,1
8.-HURTOS	786.704	790.099	0,4

(EU): indicadores estadisticos de criminalidad utilizados por la Oficina Estadística de la Unión Europea (EUROSTAT).

Tabla 1. Estadística de criminalidad últimos dos años

2.2. Sistemas de Seguridad Física

Al hablar de Seguridad Física estamos haciendo referencia a todo aquel sistema desarrollado para la protección física de personas y elementos materiales e inmateriales.

El objetivo de la Seguridad Física es prevenir amenazas como:

- Desastres naturales, incendios, tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Manipulaciones y sabotajes internos y externos.

2.2.1 Tipos de Sistemas de Seguridad Física

Los principales Sistemas de Seguridad Física pueden clasificarse en tres principales tipos, desembocando éstos en varias aplicaciones según su configuración y funcionalidad: Sistema de Intrusión, Sistema de CCTV y Control de Accesos [6].

Sistema Intrusión

Los Sistemas de Intrusión tienen el objetivo de la seguridad contra actos antisociales, con la aplicación de medios y métodos para evitar, reducir o controlar, las acciones delictivas provocadas por actividades antisociales.

El objeto de estos sistemas es proteger al sujeto paciente frente a un riesgo contra:

- La salud.
- La integridad física.
- Sus bienes y patrimonio.
- La intimidad.
- Las comunicaciones.
- La integridad moral.
- El medio ambiente.
- Robo y hurto.
- Atraco.
- Fraude y estafa.
- Vandalismo.
- Amenazas.
- Sabotaje y manipulación.
- Espionaje industrial, comercial o financiero.

Según la situación se estudian y desarrollan sistemas de seguridad frente a los riesgos implicados. Podemos clasificar los sistemas de seguridad en base al método de seguridad requerido como:

- Contención: Disuasión, Detención, Restricción, Canalización.
- Detección: Vigilancia, Alerta, Reconocimiento, Comunicación.
- Reacción: Evaluación, Decisión, Comunicación.
- Intervención: Acción o respuesta.
- Normalización: Restauración, Vuelta a la situación inicial.

Sistema de CCTV

Es el acrónimo inglés de "Closed Circuit Television", es decir: Circuito Cerrado de Televisión, por tanto, es un sistema de transmisión de imágenes (TV) a las que sólo se accede desde una red restringida por las personas autorizadas.

Entre las diversas aplicaciones de seguridad de los Sistemas de CCTV tenemos:

- Control de procesos industriales.
- Control de acceso de vehículos por lectura de placas de matrícula.
- Vigilancia y televigilancia.
- Flujo de personas.
- Detección de intrusión (videosensor).
- Control de tráfico.
- Verificación de alarmas desde CRA.
- Conteo de afluencia.
- Objetos abandonados.
- Seguimiento automático.
- Visión nocturna (cámaras térmicas).

Sus altas prestaciones y la capacidad de integración de este sistema, hace de éste una herramienta tan poderosa que en la actualidad es difícil encontrar una instalación de seguridad que no integre un sistema de CCTV.

Control de Accesos

Resulta obvia la necesidad de mantener entornos cerrados para preservar su contenido, bien se trate de personas, objetos o información. No obstante, la condición de cerrado no puede ser absoluta y se requieren de sistemas sofisticados para su acceso restringido.

La solución para este tipo de seguridad es la implantación de un control de accesos específico para cada actividad deseada. Un control de accesos es tal y como su nombre lo indica, un dispositivo o sistema que controla el acceso a un lugar determinado.

Existen diferentes tipos de control de acceso con varios niveles de seguridad. Los más comunes son los que por medio de una lectora de cualquier tipo, mande la señal a un electroimán, chapa, perno, pluma y de más artículos para brindar o denegar el acceso.

En cuanto a su utilidad y tecnología ofrecen las siguientes ventajas dadas sus funcionalidades:

- Eliminar o evitar al máximo la intervención humana sobre los controles.
- Impedir entradas no autorizadas.
- Posibilidad de gestión de: horarios, rutas...
- Seguridad de obtener una alarma fiable ante cualquier intento de entrada no autorizada, aunque en muchos casos tengamos que apoyarnos en elementos auxiliares.
- Asegurar la identificación, en el caso de acceso de personas, de manera tan fiable como se precise según la valoración de riesgos.
- Obtener información en tiempo real sobre todos los eventos.
- Permitir el control de otros subsistemas.
- Apoyo a la evacuación mediante accesos libres, conteo de personas y conocimiento de cuantas se encuentran en el interior.
- Puntos de conteo de personas para evacuación.
- Gestiones auxiliares de control.
- Control de presencia.

- Control de horarios.
- Control de visitas.
- Control de acreditaciones.
- Gestión de rondas.
- Integración de otros sistemas, Intrusión, CCTV, climatización, detección y extinción automática de incendios...

2.3. Sistemas de intrusión informática

Los sistemas de información y los datos contenidos también son objeto de riesgo de intrusión. Éstos son protegidos mediante el desarrollo y aplicación de mecanismos de seguridad informática denominados Sistemas de Detección de intrusos (IDS).

Al hablar de Sistemas de Detección de Intrusos en el ámbito de la seguridad informática estamos hablando de seguridad de la información donde el objeto a proteger y principal activo por su valor es la información. Éste activo presenta:

- Vulnerabilidades que comprometen su seguridad.
- Amenazas que comprometen la seguridad del activo.
- Riesgo de probabilidad de que se produzca un evento asociado a la vulnerabilidad y amenaza.
- Impacto definido como la medida del daño causado.

Para proteger un sistema se deben aplicar medidas que eliminen la vulnerabilidad o la amenaza y disminuyan el riesgo o impacto causados.

2.3.1. Tipos Sistemas de Detección de intrusos

Existen dos tipos de Sistemas de Detección de Intrusos [7]:

- HIDS (*Host IDS*): el principio de funcionamiento de un HIDS depende del éxito de los intrusos, tal como se indica en la Fig. 1, realizan su función protegiendo un único sistema; de una forma similar a como actúa un escudo antivirus residente en

el sistema operativo, el IDS es un proceso que trabaja en background (o que despierta periódicamente) buscando patrones que puedan denotar un intento de intrusión o mala utilización y alertando o tomando las medidas oportunas en caso de que uno de estos intentos sea detectado.

Fig. 1. Sistema de detección de intrusos de PC.

- NIDS (*Network IDS*): un IDS basado en red, monitorea los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella, tal como se muestra en la Fig. 2. El IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador). Esté donde esté, monitorizará diversas máquinas y no una sola: esta es la principal diferencia con los sistemas de detección de intrusos basados en host.

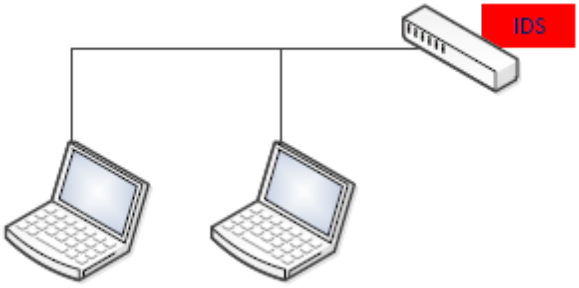

Fig. 2. Sistema de detección de intrusos basado en red.

2.4. Igualdad de objetivos entre Sistemas IDS y Sistemas de Seguridad

Podemos hacer una combinación de un Sistema IDS con Sistemas de Seguridad y CCTV desarrollados en el ámbito de la seguridad física y así obtener una seguridad más completa.

Un sistema de seguridad física está basado en la detección de intrusión mediante sensores de distintos tipos que avisan de un posible ataque o sabotaje. A su vez, los sistemas de seguridad informática y, en concreto, los sistemas de detección de intrusiones, actúan de la misma forma que los sistemas de seguridad física, esto es, detectan y avisan de un posible ataque mediante la captación de anomalías.

Hoy en día y, mayoritariamente en el mundo de las empresas, también nos encontramos con Sistemas de Circuito Cerrado de Televisión basados en cámaras que se configuran para grabar cambios en una situación puntual. Este tipo de elementos de captación de imágenes están configurados por detección de movimiento, es decir, mientras no se produzca un cambio significativo en el escenario no actúan, lo que hace mucho más eficiente su recurso. Estamos ante otro claro ejemplo de mecanismo de actuación por detección de intrusiones.

Los Sistemas de Seguridad y CCTV están aplicados en un ámbito distinto al de los Sistemas de Intrusión en la red pero, a su vez, su configuración es la misma, ambos sistemas actúan al detectar cambios o movimientos por la presencia de anomalías en un entorno; deducimos de ello que el concepto de seguridad es el mismo.

3. CLOUD COMPUTING

En los últimos años ha surgido y se ha ido desarrollando el Cloud Computing o Computación en La Nube, un nuevo modelo informático el cual consiste en el almacenamiento de programas y archivos en servidores de terceros, a los que se puede acceder a través de Internet.

A continuación se describe el modelo de "Cloud Computing" para cualquier organización, analizando la implicación de la seguridad en este nuevo modelo informático.

3.1. Historia de computación de la Nube

En 1961, John McCarthy sugirió que los avances en la informática y las comunicaciones conducirían a que "algún día la computación se organizaría como un servicio público" (*utility*), igual que el modelo de negocio del agua o la electricidad [9].

A finales de los años 90, los técnicos de Amazon se dieron cuenta que tenían una gran infraestructura informática pero que apenas utilizaban el 10-15% de su capacidad. Vieron las posibilidades de ofrecer estos servicios a usuarios y en 2006 presentaron los Servicios Web de Amazon.

Durante los años 2007 y 2008, grandes empresas como Google o IBM se unieron a universidades norteamericanas para iniciar una investigación a gran escala sobre el *Cloud Computing*. Como resultado de esta investigación, en Enero de 2009 apareció Eucalyptus, una plataforma de código abierto que permitía la creación de sistemas en la nube compatibles con los servicios web de Amazon.

3.2. Servicio de Cloud Computing

El servicio que ofrece *Cloud Computing* está dividido en tres niveles [9]:

-Infraestructura como Servicio (IaaS, de sus siglas en inglés *Infrastructure as a Service)*. Se trata del nivel más alto de servicio. Se encarga de entregar una infraestructura de

procesamiento completa al usuario bajo demanda. El usuario puede disponer de una o varias máquinas virtuales en la nube pagando solamente por los recursos que utilice.

-Plataforma como Servicio (PaaS, de sus siglas en inglés *Platform as a Service*). Se trata del nivel intermedio, se encarga de entregar una plataforma de procesamiento completa al usuario, plenamente funcional y sin tener que comprar y mantener el hardware y software.

-Software como Servicio (SaaS, de sus siglas en inglés *Software as a Service*). Este nivel se encarga de entregar el software como un servicio a través de Internet siempre que lo demande el usuario. Se trata del nivel más bajo que permite el acceso a la aplicación utilizando un navegador web, sin necesidad de instalar programas adicionales en el ordenador o cualquier otro dispositivo con acceso a Internet.

La principal característica del *Cloud Computing* es el acceso desde cualquier lugar a los datos. Solo se necesita un navegador web y conexión a Internet para disfrutar de los servicios en la nube, no hace falta tener un sistema operativo determinado o instalar un software específico en cada cliente.

Las tecnologías móviles ocupan un papel importante dentro del modelo de negocio de una empresa. La combinación de dispositivos móviles y fijos crea nuevas oportunidades en el desarrollo de la actividad empresarial permitiendo plena operatividad, lo cual supone una gran ventaja frente a otras tecnologías.

Al igual que con otros sistemas tecnológicos, existen limitaciones: no es posible utilizar las aplicaciones en la nube si no hay conexión a Internet y la calidad y la velocidad de la conexión deben ser altas para poder utilizar el servicio de forma correcta.

Por norma general, las aplicaciones de escritorio tienen un rendimiento mayor que las aplicaciones web debido a que aprovechan mejor todos los recursos del equipo.

3.3. Tipos de Nubes

Una vez entrado en el concepto de La Nube, podemos agrupar los sistemas según su uso [8]:

Nubes públicas: son aquellas en las que todo el control de los recursos, procesos y datos está en manos de terceros. Múltiples usuarios pueden utilizar servicios web que son procesados en el mismo servidor, pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.

Nubes privadas: son aquellas creadas y administradas por una única entidad que decide dónde y cómo se ejecutan los procesos dentro de la nube. Supone una mejora en cuanto a la seguridad y privacidad de los datos y procesos, ya que los datos sensibles permanecen en la infraestructura informática de la entidad, mientras que controla qué usuario accede a cada servicio de la nube. Sin embargo, la entidad sigue siendo la encargada de comprar, mantener y administrar toda la infraestructura hardware y software de la nube.

Nubes híbridas: está basada en una combinación de las dos anteriores. Por ejemplo, una empresa hace uso de una nube pública para mantener su servidor web mientras que mantiene su servidor de bases de datos en su nube privada. De este modo, se establece un canal de comunicación entre la nube pública y privada mediante el cual los datos sensibles permanecen bajo estricto control mientras que el servidor web es administrado por un tercero. Esta solución disminuye la complejidad y coste de la nube privada.

3.4. Ámbito Legal en la Nube

3.4.1. Protección de Datos

El principal funcionamiento de La Nube es la gestión remota de la información. Esto implica la transferencia entre organizaciones de multitud de información, en numerosos casos de gran importancia, todo ello depositado en servidores pertenecientes a terceros.

Esta situación desemboca en numerosas implicaciones jurídicas, más aún en el caso de que los datos se alojen en servidores de otro país, en la medida en que convergen dos o más jurisdicciones y surge la necesidad de determinar aspectos como la Ley aplicable, los tribunales competentes o las condiciones exigibles para que la transferencia de los datos a los sistemas del proveedor pueda ser viable y, en su caso, autorizada por la autoridad nacional de protección de datos.

Al firmar el correspondiente contrato o términos de uso, el cliente o contratante se vincula a aceptar el sometimiento de cualquier conflicto que pueda surgir a una jurisdicción concreta. En el caso europeo, el marco general en cuanto a protección de datos y libre circulación de los mismos lo fija la *Directiva 95/46/CE* [13]. La trasposición nacional operada por cada Estado miembro obliga a tener en cuenta la Ley nacional como criterio rector. Asimismo, existen Decisiones y Comunicaciones de la Comisión Europea y documentos adoptados por los principales actores a nivel europeo en la materia, como es el caso de la Agencia Europea de Seguridad de las Redes y de la Información *(ENISA)* [14] en los que se dispone el carácter fundamental del marco legal aplicable [10].

3.4.2. Regulación de las LSSI

Los prestadores de servicios de la sociedad de la información (servicios de alojamiento de datos en la nube y acceso a Internet), deben cumplir con los requisitos establecidos en la *Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI)* [11].

En concreto, los proveedores de servicios establecidos en España están obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita sobre:

- Los medios técnicos aplicados para aumentar la seguridad de la información (como programas antivirus, antiespías y filtros de correo).
- Las medidas de seguridad que aplican en la provisión de los servicios.
- Las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.
- En el caso de los proveedores de acceso a Internet, además deben comunicar a los usuarios las responsabilidades en que pueden incurrir por el uso ilícito de la Red.

Además de los citados preceptos legales, la *Ley 32/2003 General de Telecomunicaciones* [12] también vela por el cumplimiento de las obligaciones en el secreto de las comunicaciones y protección de datos personales, así como de los derechos y obligaciones

de carácter público vinculados con las redes y servicios de comunicaciones electrónicas, imponiendo a su vez las correspondientes sanciones por su incumplimiento.

3.5. Seguridad en la Nube

3.5.1. Riesgo del Cloud Computing

Como toda tecnología, el *Cloud Computing* no está exento de riesgos. Cuanto más compleja es la infraestructura informática utilizada, más posibles vulnerabilidades aparecen. A continuación se describen los principales riesgos de seguridad al disponer de los recursos en la nube:

El *Cloud Computing* ofrece un gran número de ventajas y oportunidades que también están siendo aprovechadas por los piratas informáticos. Ataques como el robo de contraseñas, envío de Spam o ataques de denegación de servicio distribuido se vuelven mucho más sencillos y baratos.

Los delincuentes informáticos pueden planear sus ataques contratando servicios en la nube para posteriormente ejecutarlos en cuestión de horas. Además, los recursos que utilicen se borrarán una vez concluya el ataque, lo que dificulta mucho su persecución.

Del mismo modo, pueden contratar servicios de almacenamiento en la nube para guardar datos maliciosos o robados, lo cual dificulta que las autoridades puedan acceder a esta información para actuar contra los atacantes.

Las amenazas también pueden venir por el mal uso intencionado o no del servicio de La Nube por parte de los usuarios de la empresa, lo que puede provocar pérdidas de información, con los consiguientes daños en la imagen de la empresa y las posibles consecuencias legales o jurídicas. Para evitar estas situaciones, las organizaciones utilizan medidas como la incorporación de cláusulas de confidencialidad en los contratos laborales o el establecimiento de políticas de seguridad.

Otros riesgos específicos que nos podemos encontrar son los siguientes [8]:

- Ataques en las APIS de la Nube: Las APIS son el único punto de interacción con los programas que se están ejecutando en la nube, siendo éstas un punto crítico de la seguridad y privacidad del sistema. Cada proveedor de servicios en la nube tiene sus propias APIS de conexión que permiten desde arrancar o parar los servicios en la nube hasta aumentar o disminuir los recursos de los mismos. Si no se aplican unas medidas adecuadas de seguridad, las APIS pueden sufrir ataques de malware permitiendo a los atacantes el robo o acceso a la información de la víctima.
- Suplantación de identidad: Dependiendo del uso que se esté haciendo del *Cloud Computing*, la combinación tradicional de usuario y contraseña puede no resultar lo suficientemente segura. Al igual que ocurre con otros sistemas tecnológicos actuales, es necesario investigar otros sistemas mucho más seguros para evitar la suplantación de identidad en la Red. Una solución para incrementar la seguridad es el ejemplo mostrado en la Fig. 3 del actual DNI electrónico como mecanismo de identificación, ya que incluye medidas criptográficas y biométricas como complemento a las tradicionales medidas de seguridad.

Fig. 3. Imagen DNI Electrónico

3.5.2. Seguridad del Cloud Computing

El "Cloud Computing", al tratarse de un modelo tecnológico que está en auge, no es menos seguro que modelos anteriores pero dispone de menos experiencia por parte del personal experto en seguridad y la alta probabilidad de amenazas desconocidas.

Al hacer uso del *Cloud Computing* una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube.

Para entender el modelo de seguridad de la información aplicado en este modelo es necesario conocer los distintos actores que participan en él, reflejados en la Fig. 4:

Proveedor de servicios en la nube

Empresa que dispone de la infraestructura informática necesaria para hospedar los programas siguiendo el modelo de *Cloud Computing*.

Cliente

Persona, organización o empresa que contrata los servicios en la nube. El cliente es quien paga cierta cantidad de dinero para beneficiarse de las prestaciones de la computación en la nube. El usuario final, o la persona o grupo de personas que utiliza el programa, pueden ser distintos al cliente. Por ejemplo, una empresa puede contratar servicios en la nube para hospedar un servidor web al que accederán sus empleados.

Los mecanismos de seguridad que se pueden aplicar para proteger los datos alojados en la nube deben considerarse como un trabajo colaborativo entre las dos partes (proveedor de servicios en la nube y cliente), ya que ambas deben asumir unas responsabilidades. La realización de auditorías de seguridad conjuntas es una buena práctica para revisar que todo el sistema está protegido frente a posibles amenazas [8].

3.5.3. Seguridad por parte del proveedor del servicio de Cloud Computing

El proveedor de servicios en la nube se encarga de garantizar la seguridad física en sus centros de procesos de datos. Deberá impedir que personas no autorizadas entren en dichos edificios para, por ejemplo, robar sus equipos. Del mismo modo, deberá mantener sus equipos actualizados tanto a nivel hardware como software para hacer frente a las amenazas existentes en Internet.

El proveedor utiliza mecanismos como la virtualización y la segmentación de datos para reforzar la seguridad de sus servicios en la nube [8].

- Virtualización: La virtualización puede ser vista como una forma de aumentar la seguridad de los procesos que se ejecutan en la nube. Varias máquinas virtuales pueden ser ejecutadas en un único servidor pero cada máquina virtual ejecuta un sistema operativo de forma aislada. El espacio de memoria y disco están controlados por un *hipervisor* que impide que los procesos ejecutados en distintas máquinas virtuales puedan interactuar entre ellos. El mayor riesgo al que debe enfrentarse el proveedor de servicios en cuanto a este mecanismo es el control y eliminación del software malintencionado que pretenda burlar las protecciones del *hipervisor* para tener acceso a otras máquinas virtuales o incluso al sistema anfitrión.
- Segmentación: La deslocalización de los datos es una característica que también puede ser explotada como un mecanismo de seguridad en sí misma. La segmentación de datos permite que los datos de un cliente residan en diferentes servidores, incluso en diferentes centros de datos. De esta forma, se protegen dichos datos frente a un hipotético robo en las instalaciones del proveedor de servicios. Además, al poder mantener los datos en varias localizaciones de forma simultánea, se dispone de un sistema de copias de seguridad prácticamente en tiempo real. Así, ante fallos de seguridad, se puede recuperar rápidamente la actividad, permitiendo la continuidad del negocio.

3.5.4. Seguridad Cliente de Servicio Cloud Computing

El cliente tiene la responsabilidad de mantener el sistema operativo actualizado e instalar los parches de seguridad que aparezcan. Al igual que ocurre en los servidores que son propiedad de una empresa, es necesario mantener políticas de seguridad tradicionales como el control de usuarios, la eliminación de cuentas de usuario que ya no se utilizan, o la revisión del software para comprobar que no tiene vulnerabilidades, entre otras.

Los mecanismos específicos que puede adoptar el cliente para reforzar la seguridad en la nube engloban el control perimetral, la criptografía y la gestión de *logs* o archivos de registro de eventos [8].

- Control perimetral: Es uno de los pilares de la seguridad informática. Para llevarlo a cabo, es recomendable la instalación y configuración de un firewall o cortafuegos. Para añadir otro nivel de seguridad de red, es igualmente recomendable la instalación y configuración de un IDS.
- Criptografía: Es otro de los mecanismos de seguridad en el uso de los servicios en la nube. La criptografía proporciona un nivel superior de seguridad en tres aspectos principales:
    1. Protección de las conexiones de Red entre los usuarios y las aplicaciones en la nube: El uso de *Secure Sockets Layer* (SSL) y *Transport Layer Security* (TLS) permiten que todos los datos que viajen desde el servidor en la nube hasta el usuario estén cifrados impidiendo su acceso a terceras personas incluso cuando se utiliza una red Wi-Fi no segura.
    2. Protección de las conexiones entre los administradores del sistema y los servicios de la nube: En este caso, el uso de *Secure Shell* (SSH) y *Virtual Private Network* (VPN) permitirá a los administradores del sistema o desarrolladores de las aplicaciones mantener un canal seguro de comunicación con los sistemas en la nube, tal como se muestra en la Fig. 4.

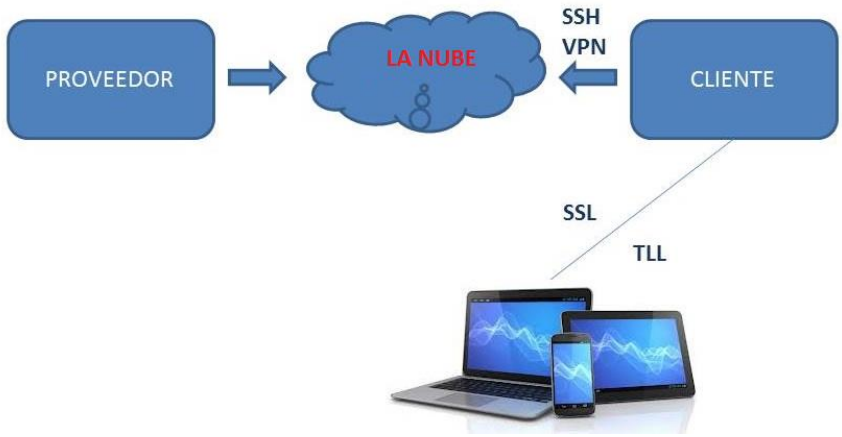

Fig. 4. Seguridad en la Nube mediante VPN

3. Protección de los datos utilizando criptografía: Si se utiliza la nube como un sistema de almacenamiento de datos es muy recomendable utilizar un nivel de cifrado adecuado para aquellos datos sensibles que vayan a ser

depositados allí. De esta forma, si algún usuario no autorizado intercepta los datos o tiene acceso al sistema de ficheros de la nube, no podrá leer el contenido allí depositado sin conocer la clave de cifrado.

- Gestión de *logs*: La única manera de comprobar la actividad informática, detectar incidentes y formular un plan de acción para evitar que vuelvan a suceder en el futuro es gestionar los *logs* del sistema. Aunque es muy posible que no se tenga acceso a toda la información sobre los eventos del sistema, el cliente debe almacenar y revisar todos los *logs* que estén bajo su responsabilidad. Por ejemplo, el registro de usuarios que acceden a la aplicación, manipulan o borran ficheros en la máquina virtual, o el registro de conexiones potencialmente peligrosas detectadas por el IDS y por el cortafuegos. Además, es recomendable realizar copias de seguridad frecuentes de estos *logs* e incluso almacenarlos en una máquina distinta ya que si un atacante se hace con el control del sistema en la nube podría destruir los ficheros de registro borrando así sus huellas.

3.5.5. Integridad

Mantener una correcta integridad de los datos significa que estos permanecen idénticos durante las operaciones de transferencia, almacenamiento o recuperación. En el ámbito del *Cloud Computing*, la integridad de los datos es especialmente crítica: los datos están siendo transferidos constantemente entre los servicios en la nube y los distintos usuarios que acceden a ellos [8].

Debido a las características de la computación en la nube, varios usuarios pueden estar accediendo simultáneamente y modificando determinada información. Por ello, deben implementarse los mecanismos que garanticen la correcta integridad de los datos.

La mayor amenaza para la integridad de los datos en la nube es que los datos se acaben corrompiendo debido a errores en su manipulación. Si no se detecta que ha habido un problema en la transferencia y los datos se almacenan erróneamente, la próxima vez que el usuario quiera acceder a ellos no podrá utilizarlos.

Para evitar que los datos en la nube no puedan utilizarse o que no estén disponibles se utilizan principalmente tres mecanismos: control de integridad, gestión de cambios y copias de seguridad.

3.5.6. Control de accesos

Igual que sucede con las arquitecturas tradicionales, el control de acceso también juega un papel importante en el *Cloud Computing*. Aunque esta tecnología se represente informalmente como una nube a la que se conecta todo el mundo desde sus equipos (tanto fijos como dispositivos móviles), no significa en absoluto que cualquier persona pueda acceder a cualquier dato o proceso en la nube.

Es necesario distinguir claramente entre los servicios que se ofrecen de forma libre y gratuita en la nube y la utilización de recursos en la nube para fines personales o empresariales.

Cuando una empresa o entidad utiliza las capacidades de la computación en la nube, necesita que el administrador del sistema establezca un correcto control de acceso para garantizar que los usuarios sólo utilicen los datos o procesos para los que han sido autorizados [8].

3.5.7. Política de Seguridad

Uno de los mayores riesgos a los que se enfrenta todo sistema informático es la pérdida de datos, ya sea porque un usuario ha borrado información accidentalmente, porque haya un fallo en algún dispositivo hardware o por culpa de un ataque informático. Perder los datos no sólo significa tener que rehacer parte del trabajo realizado, sino que en muchos casos puede significar cuantiosas pérdidas económicas.

La solución a este problema se enfoca desde dos puntos de vista principales [10]:

Por un lado, una correcta *política de seguridad* limita la libertad de los usuarios para borrar elementos del sistema, protege los equipos ante el ataque de software malintencionado y además impide que personas ajenas a la organización accedan o corrompan los datos. El

proveedor de servicios se encarga de solucionar todos los problemas relacionados con los componentes electrónicos. Si detecta un fallo en uno de los equipos dentro de sus instalaciones, automáticamente lo aísla y todos los procesos que se ejecutan en él se migran a otra máquina que no tenga problemas. Este proceso puede durar tan solo unos minutos e incluso realizarse sin cortar el servicio, permitiendo una disponibilidad ininterrumpida de los servicios en la nube.

Por otra parte, una correcta política de copias de seguridad permite recuperar los datos aun cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware. Todos los proveedores de servicios en la nube ofrecen sistemas de copias de seguridad de forma completamente transparente para el usuario. Tan solo es necesario seleccionar los activos que se quieren proteger y la periodicidad con la que se desean estas copias. La recuperación frente a un ataque puede ser tan sencilla como la restauración de un *snapshot* (copia instantánea de volumen) anterior de la máquina virtual.

Las características anteriormente expuestas permiten disponer de un sistema robusto preparado para realizar una correcta recuperación frente a desastres, es decir, asegurando la continuidad del negocio.

Por último, existe otra ventaja relativa a los dispositivos portátiles, cada vez más utilizados en las empresas y desde los que se accede a la información de la organización: ordenadores portátiles, USB's, móviles, etc. Estos dispositivos pueden ser robados u olvidados exponiendo grandes cantidades de datos a personas completamente ajenas a la organización. Si se utilizan sistemas en la nube, aunque se pierda un teléfono móvil o alguien robe un portátil, la información permanecerá inaccesible para terceros.

3.6. Ventajas e inconvenientes de La Nube

Ventajas de la nube [15]

- Acceso desde cualquier lugar y a través de cualquier dispositivo con acceso a internet: Al ubicarse todos los programas y archivos en la nube sólo es necesaria

una conexión a Internet para acceder y hacer uso de forma remota mediante un PC, un laptop, una tablet, un iPad, un Smartphone...

- No requiere la instalación de ningún software: Sólo es necesario disponer del navegador de Internet. El proveedor de los servicios de la nube se encarga de la actualización de los programas usados.
- Ahorro en software y hardware: Los programas son compartidos por los usuarios sin necesidad de hacer ningún tipo de copia y toda la información queda almacenada en la nube.
- Ahorro en mantenimiento técnico: El proveedor de la nube se encarga del mantenimiento técnico de sus propios servidores. El usuario no necesita saber crear redes de computadoras para compartir recursos, porque puede hacerlo a través de la nube.
- Escalabilidad: Un sistema informático es escalable si puede crecer para responder a necesidades más exigentes. Esto es crucial sobre todo para las empresas. Con la nube, la escalabilidad está garantizada sin tener que invertir más de lo necesario en previsión de que las necesidades aumenten. Si un usuario de la nube necesita más o menos capacidad de proceso o de almacenamiento, el proveedor de la nube se lo facilitará casi en tiempo real. Esto optimiza los recursos en todo momento.

Inconvenientes de la nube [15]

- Seguridad y privacidad: Con la computación en la nube los ficheros e información pasan de estar en tu PC a almacenarse en esa nube. Eso implica dejar de tener control sobre ellos. Nunca se puede estar seguro de quién accede a esa información. Es un riesgo para usuarios particulares pero aún más para las empresas. Ellas deben confiar informaciones internas y confidenciales a un tercero, que puede o no ser fiable.

  Además, es más probable que un *hacker* intente acceder a la nube que a un PC privado. El botín es mayor.

- Sin Internet no hay nube: En la computación en la nube todo depende de que la conexión a Internet funcione. Si no es así, el cliente no podrá acceder a los programas ni los datos.
- Problemas de cobertura legal: Los servidores de la nube pueden estar en cualquier parte del mundo. Si hay problemas, no está claro qué ley debe aplicarse o si ésta podrá proteger al cliente.
- Conflictos de propiedad intelectual u otros: La información de los clientes ya no está sólo a su única disposición, con lo que pueden surgir problemas sobre a quién pertenece. Eso puede llevar a situaciones delicadas, por ejemplo si el cliente pretende cambiar su proveedor de computación en la nube o si éste quiebra o comete alguna ilegalidad.

4. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

La expansión en los últimos años y el número de clientes potenciales que ofrece, hace que Internet sea una red muy compleja donde recae una alta responsabilidad para el desarrollo empresarial actual. Es entonces cuando aparece el concepto de "Seguridad de la Información".

Internet es una red tan grande que su control y regulación es casi imposible, por lo que su uso supone una constante exposición a diversos tipos de amenazas y su seguridad recae en todos y cada uno de sus usuarios.

La seguridad de la información es definida por tres conceptos básicos: confidencialidad (sólo quien esté autorizado puede acceder a una determinada información), integridad de toda información y disponibilidad de usuarios autorizados [20].

Si en una empresa es necesaria la implantación de sistemas de seguridad física, en la empresa virtual es necesario sistemas de seguridad informática.

Todo ello implica la necesidad de desarrollar una política de seguridad de las redes de ordenadores en las empresas ante cualquier ataque informático.

Una completa seguridad informática tiene que proteger todo sistema de cualquier vulnerabilidad y ataque a través de la red.

4.1. Introducción

Un sistema de detección de intrusos o IDS (*Intrusion Detection Systems*) [16] es un programa usado para detectar accesos no autorizados a un computador o a una red. Su función principal es monitorear el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Tal y como venimos comentando, toda información tanto local como remota que requiere de protección necesita un sistema de seguridad basado en herramientas de monitoreo: ids, ips…que nos permiten analizar toda topología vulnerable ante la exposición a cualquier amenaza o ataque de intrusión informática.

Según qué se necesite proteger y de qué manera tenemos varios sistemas de detección de intrusos en la red en base a su funcionamiento:

- IDS: intenta detectar y avisar de manipulaciones y ataques, pero no actúa.
- IPS: sistema de prevención de las intrusiones, actúa contra las intrusiones.

Hay varios ámbitos de aplicación en función de su aplicación:

- HIDS: Sistema de Detección de Intrusiones en un host. Monitorizan y sólo llegan hasta la tarjeta de red.
- IPS: no actúa, sólo supervisa, en definitiva, alerta de intrusiones.
- IDS: monitoriza todo lo que pasa por la red, pero no está activo, está observando.

4.2. Antecedentes

La historia [22] sobre los sistemas de detección de intrusos en ordenadores empieza en 1972 cuando James P. Anderson de las fuerzas aéreas norteamericanas (USAF) publica un texto sobre la seguridad en los ordenadores. Este tema empieza a cobrar fuerza paralelamente al desarrollo de la informática, puesto que cada vez hay más procesos "críticos" controlados por ordenadores y los militares temen cualquier situación que no puedan controlar.

Durante los años siguientes se realizan algunos estudios hasta que en 1980 James P. Anderson escribe "Computer Security Threat Monitoring and Surveillance", donde se

inician las bases de la detección de intrusos en sistemas de computadores principalmente mediante la consultas de ficheros de *log*.

Entre 1984 y 1996, Dorothy Denning y Neumann desarrollan el primer modelo de IDS que funcionaba en tiempo real denominado IDES (Intrusion *Detection Expert System*) basado en reglas. A partir de este momento, se han ido proponiendo y creando nuevos sistemas de detección de intrusos hasta obtener una separación clara entre los sistemas que efectúan la detección dentro de los ordenadores (IDS) y aquellos que la efectúan en el tráfico que circula por la red (NIDS).

4.3. Tipos de Amenazas informáticas

Partiendo de la definición de amenaza como toda aquella variación de un entorno por parte de una persona, máquina, suceso o idea que puede comprometer la seguridad de un sistema.

Las amenazas pueden analizarse antes del ataque, durante el ataque o después de haberse producido el ataque. Para su análisis se realizan tres tipos de intervenciones:

- Prevención: mecanismos que aumentan la seguridad de un sistema durante su funcionamiento normal.
- Detección: mecanismos que revelan violaciones a la seguridad.
- Recuperación del sistema: mecanismos que son aplicados cuando se ha producido una violación del sistema. Su función es restaurar el sistema a su funcionamiento normal.

Aunque cada amenaza puede recibir más de una clasificación podemos hacer una clasificación genérica en función de su principal característica [18].

4.3.1. Amenazas por el origen

Una red no está expuesta a riesgo de amenaza o ataque por el simple hecho de estar conectada a un entorno externo, si no está conectada a un medio externo como Internet no nos garantiza la seguridad de la misma. Existen dos tipos de amenazas claramente diferenciadas basadas en el origen del ataque:

Amenazas internas

Este tipo de amenazas pueden ser causadas por el uso malintencionado de usuarios o personal técnico que disponen de algún tipo de acceso a la red por las necesidades de su trabajo. Ahora bien, por otro lado, que el ataque sea interno no necesariamente tiene que ser debido a personas ajenas a la red, puede ser debido también a alguna vulnerabilidad como redes inalámbricas desprotegidas, equipos sin vigilancia... etc.

Los sistemas de prevención de intrusos y firewalls no son mecanismos efectivos para amenazas internas porque por norma general no están orientados al tráfico interno.

Amenazas externas

Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

4.3.2. Amenazas por el efecto

El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en:

- Robo de información.
- Destrucción de información.
- Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.
- Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.
- Robo de dinero, estafas,...

4.3.3. Amenazas por el medio utilizado

Se pueden clasificar por el *modus operandi* del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

- Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que sólo se caracterizan por ser molestos.
- *Phishing*.
- Ingeniería social.
- Denegación de servicio.
- *Spoofing*: de DNS, de IP, de DHCP, etc.

4.4. Funcionamiento

El funcionamiento de las herramientas para la detección de intrusos consiste en el análisis del tráfico de un segmento de red, analizando paquetes y comparándolos con ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc.

Un IDS no sólo analiza qué tipo de tráfico es, sino que también se encarga de revisar el contenido y su comportamiento.

El detector de intrusos es incapaz de detener los ataques por sí solo, por eso normalmente esta herramienta se integra para trabajar conjuntamente con un firewall o cortafuegos, uniendo así la capacidad de detección del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos que permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque.

4.5. Clasificación de IDS

Existen varios tipos de IDS, clasificados según el tipo de detección, reacción ante posibles ataques o ámbito de aplicación [21].

4.5.1. Clasificación según el ámbito de aplicación

Este tipo de clasificación hace referencia a la función que desempeña el software, pueden ser:

- NIDS (Network Intrusion Detection System): Analizan el tráfico de la red.
- HIDS (Host Intrusion Detection System): Analizan el tráfico sobre un servidor o un PC.

Los NIDS analizan todos los paquetes de una red con la función principal de detectar paquetes maliciosos. Una de sus características es la funcionalidad de identificar el programa del servidor web al que se está intentando acceder alertando de cualquier posible intrusión.

Los NIDS están formados por dos componentes [24]:

- Sensor: elemento ubicado en un segmento de red determinado y cuya función es supervisar en busca de tráfico sospechoso.
- Consola: recibe los avisos de alarmas del sensor o sensores y ejecuta una acción determinada en función de la configuración que se le haya establecido. Sus funciones son el análisis basado en datos registrados y procesamiento según el resultado del análisis.

Ventajas de un NIDS:

- Detecta accesos no deseados a la red.
- No necesitan instalar software adicional en los servidores en producción.
- Fácil instalación y actualización.

Desventajas:

- Examinan el tráfico de la red en el segmento en el cual se conecta, pero no puede detectar un ataque en diferentes segmentos de la red. La solución más sencilla es colocar diversos sensores.
- Pueden generar tráfico en la red.
- Ataques con sesiones encriptadas son difíciles de detectar.

Los HIDS están desarrollados para analizar el tráfico sobre un servidor o un PC, se trata de una detección local. Protegen a un host mediante la detección ante un acceso crítico o la modificación sospechosa de un archivo

Ventajas de un HIDS:

- Herramienta potente, registra comandos utilizados, ficheros abiertos,...
- Tiende a tener menor número de falsos-positivos que los NIDS, entendiendo falsos-positivos a los paquetes etiquetados como posibles ataques cuando no lo son.
- Menor riesgo en las respuestas activas que los IDS de red.

Desventajas:

- Requiere instalación en la máquina local que se quiere proteger, lo que supone una carga adicional para el sistema.
- Tienden a confiar en las capacidades de auditoria y logging de la máquina en sí.

4.5.2. Clasificación según el tipo de detección

Los dos tipos de detecciones que pueden realizar los IDS son la Detección del uso indebido y la Detección del uso extraño.

La detección por uso indebido consiste en verificar actuaciones ilegales a través del tráfico de la red. Un ejemplo claro de este tipo de actuación son los intentos de un usuario por ejecutar un programa sin permiso para ello, como es el caso de los sniffers.

Este tipo de detección basada en el uso indebido es desarrollada examinando los puntos más débiles de los sistemas.

La detección por el uso extraño está desarrollada basándose en estadísticas de las cuales se determina cuál es el tráfico normal en la red y cuál no lo es. Como ejemplo claro tenemos la detección de tráfico fuera de horario de oficina o el acceso al sistema desde una máquina remota mediante un rastreo de puertos.

4.5.3. Clasificación según el tipo de reacción

Si nos centramos en el tipo de reacción del propio IDS ante un posible ataque tendremos detectores pasivos o reactivos.

Los IDS pasivos detectan una posible violación de la seguridad, registran la información y generan una alerta.

Los IDS reactivos son desarrollados para responder ante una actuación ilegal, por ejemplo, sacando al usuario del sistema o mediante la reprogramación de los cortafuegos para impedir el tráfico desde una fuente hostil.

4.6. Ataques en la red

Un ataque de red se produce cuando un atacante utiliza vulnerabilidades y fallos en la seguridad para intentar comprometer la seguridad de una red.

El principio de funcionamiento de un atacante está basado en la recopilación de toda la información posible con el fin de lograr su objetivo, esa información puede ser [17]:

-Identificación del sistema operativo.

-Escaneo de protocolos, puertos y servicios:

- Servicios: Son los programas que carga el propio sistema operativo para poder funcionar, servicio de impresión, actualizaciones automáticas,…

- Puertos: Son las vías que utiliza el ordenador para comunicarse, 21 es el del FTP, 995 el del correo seguro…
- Protocolos: Son los diferentes lenguajes establecidos que utiliza el ordenador para comunicarse a través de la red.

Un ataque informático pasa por las siguientes etapas:

- Etapa 1: Reconocimiento → Obtención de información de la víctima.
- Etapa 2: Exploración → Análisis de la información recopilada y estudio de las vulnerabilidades y defectos encontrados.
- Etapa 3: Obtener accesos → Puesta en marcha del ataque según las conclusiones obtenidas en las etapas anteriores.
- Etapa 4: Mantener accesos → Una vez accedido al sistema, el atacante busca herramientas que le permitan volver a acceder en el futuro.
- Etapa 5: Borrar huellas → Una vez se ha obtenido y mantenido el acceso al sistema, se borran todas las huellas del procedimiento de la intrusión para evitar ser detectado. Eliminación de los archivos de registro o alarmas del Sistema de Detección de Intrusos (IDS).

4.6.1. Ataques comunes en la red

Al igual que ocurre con la seguridad física, es imposible lograr una protección total sin ningún tipo de riesgo. Es por ello que el objetivo es tomar el mayor número de medidas preventivas que minimicen ese riesgo.

La falta de monitoreo de redes y la deficiencia de los esquemas de detección de intrusos son considerados como un agujero de seguridad muy común, el cual permite al atacante lograr penetrar en los sistemas sin ser detectado.

La materialización de un ataque puede dar lugar a un acceso no autorizado, manipulación o eliminación de información, la interrupción de alguna aplicación, daños físicos, robo de información, robo de equipos...

Describimos a continuación una relación de los ataques más comunes en la red [20]:

Ingeniería Social → Aplicación de técnicas de engaño de las personas en busca de información de interés para el atacante. La principal diferencia de este ataque con el resto es que no se trata de aprovechar debilidades de un sistema informático sino del engaño de personas.

Phishing → Técnica que consiste en el envío masivo de mensajes electrónicos haciéndose pasar por notificaciones oficiales con el fin de obtener datos personales y bancarios de las víctimas.

Escaneo de Puertos → Detección de servicios activos de los equipos con el objeto de ser utilizado por el atacante.

Código Malicioso / Virus → Todo programa que genera algún tipo de problema en el sistema en cual se ejecuta. Entre los numerosos tipos de códigos maliciosos tenemos:

- Bombas lógicas: se activan ante la ocurrencia de un evento definido.
- Troyanos: se propagan como una parte de los programas de uso común y son activados cuando se ejecutan los programas.
- Gusanos: son virus que tienen el poder de auto duplicarse.
- Cookies: archivos de texto con información acerca de la navegación realizada por los usuarios en internet que puede ser obtenida por atacantes.
- Keyloggers: aplicación que registra todas las teclas tipeadas por un usuario en su computadora.
- Spyware: aplicaciones que recogen y envían información sobre las páginas web que más frecuenta un usuario.

Ataques de Contraseña → Consiste en la prueba continua de contraseñas para lograr el acceso a un sistema que no presente un control de intentos fallidos.

Control Remoto de Equipos → Mecanismo de acceso a un equipo de forma remota y no autorizada mediante programas desarrollados para ello, e instalado por el atacante mediante, por ejemplo, la utilización de troyanos.

Eavesdropping → Procesos por los cuales un atacante capta información que no le iba dirigida mediante técnicas como el Sniffing.

Sniffing → Consiste en capturar paquetes de información que circulan por la red con la utilización de una herramienta para dicho fin, instalada en un equipo conectado a la red.

Trashing → Búsqueda de información dentro de la basura.

Denegación de Servicio → Su objetivo es degradar considerablemente o detener el funcionamiento de un servicio ofrecido por un sistema o dispositivo de red.

4.6.2. Técnicas de Detección de Ataques

Para la detección de posibles ataques en la red, los sistemas de detección de intrusos utilizan una de las dos técnicas que se describen a continuación [21]:

Heurística o Detección de patrones anómalos

El IDS basado en heurística determina la actividad normal de la red tomando como referencia el comportamiento normal del sistema a proteger. Para ello analiza constantemente toda la actividad de manera que cualquier actividad que posee cierta anomalía es considerada por el IDS como sospechosa, alertando entonces a un administrador o usuario.

Como ejemplo de estas anomalías podemos mencionar las siguientes:

- El número de sesiones iniciadas consecutivamente por un usuario es elevado en comparación con el habitual.
- La conexión de un usuario es realizada en horario no habitual.
- Un usuario no asignado para ello, accede a la base de datos de una organización.

- Otras aplicaciones del sistema independientes del usuario.
- Sobrecarga de uso de recursos: tráfico de la red, uso del disco, CPU, base de datos...
- ..etc.

La principal debilidad de esta técnica es que muchos ataques no difieren de los patrones de uso normales, por lo que en ese caso pasarían desapercibidos.

Patrones o Detección por uso incorrecto (firmas)

Se trata de un campo de investigación que en los últimos años está atrayendo la atención sobre distintas arquitecturas y enfoques.

Esta técnica, descrita en la Tabla 2, está basada en el almacenamiento de patrones de uso incorrecto o no autorizado, conocidos como firmas, referenciados por ataques o penetraciones pasadas.

Toda herramienta de ataque deja huella en el servidor, ya sea en el sistema de ficheros, en los registros de actividad o de otra forma, que suele ser característica de cada herramienta o de cada categoría de ataque. El objetivo de éste método es identificar el posible ataque mediante la búsqueda de la presencia de estas firmas en el tráfico de la red, en los registros o en las peticiones enviadas a los hosts. Es decir, un IDS basado en patrones analiza los paquetes en la red y los compara con patrones de ataques conocidos.

El mayor inconveniente de la detección de firmas es que no permite la detección de ataques nuevos y necesita actualizarse constantemente cada vez que es descubierto un nuevo tipo de ataque.

DETECCIÓN POR PATRONES O USO INCORRECTO	
FILTROS	Descartan paquetes de información que cumplen con ciertos criterios como IP fuente, protocolo, puerto, etc.
PATRONES	Comparan la información de los paquetes y los datos mismos para tomar acciones correctivas como desconexión, e-mail, almacenamiento en logs, etc.

Tabla 2. Método de detección por patrones o uso incorrecto

4.6.3. Interoperabilidad y correlación

La interoperabilidad permite que un sistema IDS pueda compartir u obtener información de otros sistemas como Firewalls, Enrutadores y Switches, lo que permite reconfigurar las características de la red de acuerdo a los eventos que se generan. También permite que se utilicen protocolos como SNMP (Simple Network Management Protocol) para enviar notificaciones y alertas a otras máquinas de la red.

La correlación es una nueva característica que añade a los IDS la capacidad de establecer relaciones lógicas entre eventos diferentes e independientes, lo que permite manejar eventos de seguridad complejos que individualmente no son muy significativos, pero que analizados como un todo pueden representar un riesgo alto en la seguridad del sistema.

4.7. Implementación de IDS en la red

Un buen sistema IDS, dado su aplicación de detección para la aplicación a diferentes sistemas de una red debe cumplir los siguientes requisitos:

- Debe estar en continua ejecución y supervisión.
- Se debe recuperar de posibles caídas o problemas con la red.
- Debe poderse analizar él mismo y detectar si ha sido modificado por un atacante.
- Debe utilizar los mínimos recursos posibles.
- Debe estar configurado acorde con la política de seguridad seguida por la empresa.
- Debe de adaptarse a cualquier cambio de los sistemas y usuarios y ser fácilmente actualizable.

Por norma general se ejecutan sólo en uno de los hosts de la red que monitorizan.

Todas las tramas que circulan por una red pueden ser portadoras de un tráfico malicioso en cada uno de sus campos [25]:

- Fragmentación (DF, MF).
- Dirección origen y destino.
- Puerto origen y destino.
- *Flags* TCP.
- Campo de datos.
- . . .

Es difícil detectar ciertos tipos de ataques en el cortafuegos, por eso, es más seguro detectarlos antes de que una intrusión llegue a nuestras máquinas mediante la implementación de un NIDS.

A la hora de implementar un NIDS es importante determinar el número de sensores y su ubicación.

Elementos necesarios para la implementación de un NIDS, identificados en la Fig. 5:

- Hardware: PC+ 2 tarjetas de red+ switch.
- Software: Software de detección de pago o de código abierto.

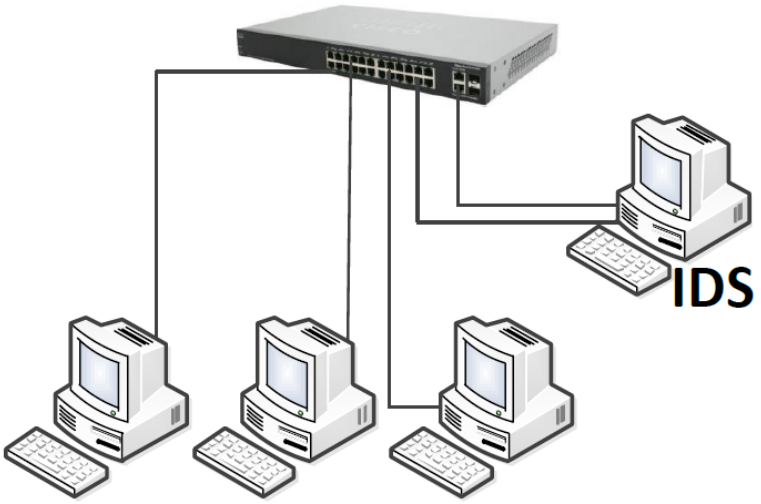

Fig. 5. Elementos que intervienen en un NIDS

Para poner en funcionamiento un sistema de detección de intrusos se debe tener en cuenta que es posible optar por una solución hardware, software o incluso una combinación de estos dos. La posibilidad de introducir un elemento hardware es debido al alto requerimiento del procesador en redes con mucho tráfico. A su vez, los registros de firmas y las bases de datos con los posibles ataques necesitan gran cantidad de memoria, aspecto a tener en cuenta.

En redes es necesario considerar el lugar de colocación del IDS. Si la red está segmentada con *hub* no hay problema en analizar todo el tráfico de la red realizando una conexión a cualquier puerto. En cambio, si se utiliza un switch es necesario conectar el IDS a un puerto SPAN (Switch Port Analiser) para poder analizar todo el tráfico de esta red.

4.7.1. Ubicación del IDS

La ubicación del IDS es la primera decisión que hay que tomar en la instalación de un IDS. De esta decisión dependerán el resto de elementos: el equipo, el software IDS o la base de datos.

La ubicación idónea donde instalar un IDS es en el dispositivo por donde pase todo el tráfico de red que nos interese analizar y proteger [16].

Hay varias posibilidades de colocación del IDS, reflejadas en la Fig. 6:

- Antes del cortafuegos: capturará todo el tráfico de entrada y salida de la red. La posibilidad de falsas alarmas es grande.
- Detrás del cortafuegos: monitorizará todo el tráfico que no sea detectado y parado por el firewall o cortafuegos, por lo que será considerado como malicioso en un alto porcentaje de los casos. La posibilidad de falsas alarmas es muy pequeña.
- Colocación de dos IDS, uno delante y otro detrás del cortafuegos: se obtiene información exacta de los tipos de ataques que recibe la red ya que si el cortafuegos está bien configurado puede parar o filtras muchos ataques. Es la opción más costosa pero ofrece mayor seguridad al obtener lecturas del tráfico total y del tráfico filtrado por el firewall.
- En ambientes domésticos se puede colocar el IDS en la misma máquina que el cortafuegos. De esta manera conseguimos así que actúen a la vez: el firewall detectará los paquetes y el IDS los analizará.

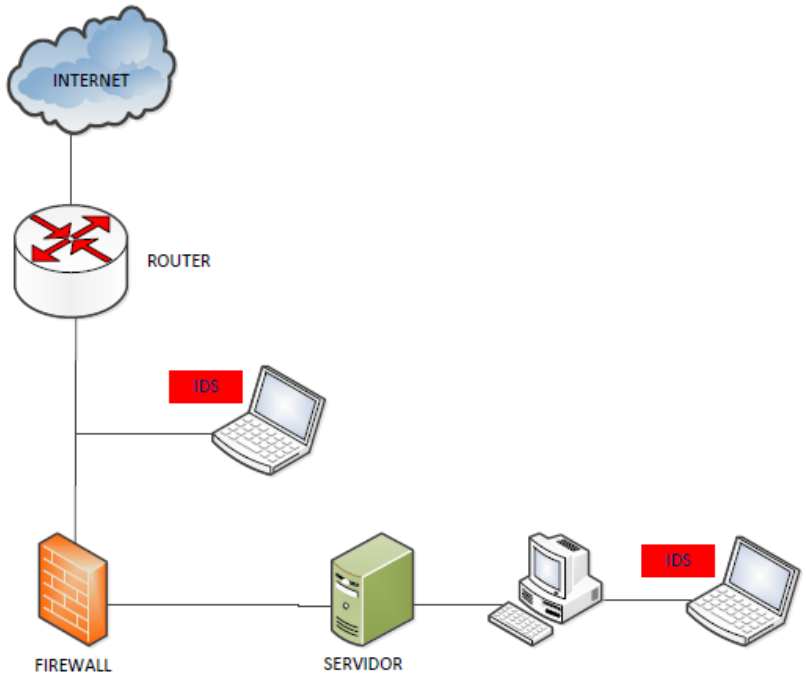

Fig. 6. Ubicación del IDS

4.7.2. Productos comerciales

Entre todos los productos que nos podemos encontrar en el mercado hemos destacado los dos siguientes [23]:

Snort

El Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS).

Es uno de los sistemas más utilizados actualmente, es un sistema de código abierto de detección de intrusiones en la red, capaz de llevar a cabo análisis de tráfico en tiempo real y registros de paquetes en redes IP.

Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos de aprovechar alguna vulnerabilidad, análisis de protocolos, etc.. y puede utilizarse para detectar una gran variedad de ataques y amenazas.

Snort está disponible bajo licencia GPL, es gratuito y funciona bajo plataformas Windows y UNIX/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

Este IDS implementa un lenguaje de creación de reglas flexibles, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, ddos, finger, ftp, ataques web, CGI, escaneos Nmap….

Entre su base de reglas incluye miles de comprobaciones en busca de ataques de denegaciones de servicio. Ofrece la posibilidad de alertar en tiempo real.

SNORT puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los

logs para su posterior análisis, concretamente un análisis offline) o como un IDS normal, en este caso NIDS.

Por lo tanto, tenemos 3 modos:

- Modo Sniffer: motoriza por pantalla en tiempo real la actividad en la red en que se ha configurado el Snort.
- Modo Packet logger (registro de paquetes): almacena en un sistema de log toda la actividad de la red en que se ha configurado Snort para un posterior análisis.
- Modo IDS: motoriza por pantalla o en un sistema basado en *log*, toda la actividad de la red a través de un fichero de configuración en el que se especifican las reglas y patrones a filtrar para estudiar los posibles ataques.

El motor del Snort se divide en los siguientes componentes:

- Decodificador del paquete.
- Preprocesadores.
- Motor de detección (Comparación contra firmas).
- Loggin y sistema de alerta
- Plugins de salida.

El decodificado de paquete toma los paquetes de diferentes tipos de interfaces de red y prepara el paquete para ser preprocesado o enviado al motor de detección.

Además de ser un sistema completo de detección de intrusiones de red, sirve como analizador de paquetes y como herramienta para registrar el tráfico.

Prelude

El Snort es el IDS de red libre más potente, pero en su arquitectura no contempla la posibilidad de usar sensores de máquina, lo cual motivó la aparición del proyecto, también libre, Prelude, que utiliza una arquitectura distribuida con canales autenticados y encriptados y sensores para diversos sistemas operativos.

Prelude no pretende reinventar los IDS's de red y, de hecho, es capaz de nutrirse del Snort e, incluso, incluye él mismo un motor que utiliza los ficheros de reglas de su predecesor.

4.8. Detección de intrusos en la Nube

Las empresas que quieran hacer uso de un entorno de nube para su actividad empresarial deben informarse de la existencia de utilización de tecnologías de seguridad por parte del proveedor en la nube al que contraten sus servicios. Los detectores de intrusos, basados en host y en red, son elementos estándar de muchos programas de seguridad de la información, y muchas empresas necesitan asegurarse de disponer de estas funciones dentro de un entorno en la nube.

En la utilización de sistemas de detección de intrusos (IDS) se deben considerar principalmente los siguientes factores:

- Monitoreo del tráfico de red dentro de la nube.
- Los sensores IDS en la nube tienen un elevado consumo de CPU y memoria.

Algunos proveedores de servicios en la nube incluyen la integración de funciones de detección en sus servicios. Los servicios varían desde los IDS e IPS basados en redes o en host hasta las soluciones de análisis integral de flujos de red, para evaluar análisis de conducta y captar toda la actividad de seguridad en la red.

Las organizaciones que deseen implementar soluciones de detección de intrusiones en la nube también pueden usar soluciones basadas en host. La forma más sencilla es la utilización de productos que pueden desarrollar su actividad dentro del sistema y en las máquinas virtuales del entorno en la nube.

Por ahora existe cierta inmadurez respecto de los IDS en la nube, la mayor parte de protección frente a intrusiones recae sobre los proveedores en la nube [19].

5. POLÍTICA DE SEGURIDAD

Todo sistema de seguridad deberá cumplir toda la legislación aplicable que se le exija, así como las políticas de seguridad y mantenimiento de dispositivos que sean acordados a través de cualquier protocolo y contrato estipulado entre las partes implicadas en una instalación.

El plan de seguridad es determinado por el factor humano, el medio en donde se desempeña, las técnicas y mecanismos con los que se cuenta, las amenazas a las que se está expuesto y las posibles consecuencias de éstas. De una completa evaluación y análisis de todo ello da su fruto un programa de seguridad y todos los protocolos, normas y procedimientos a llevar a cabo.

5.1. Seguridad aplicable en sistemas de intrusión física

Un sistema de seguridad está formado por el conjunto de elementos en instalaciones necesarios para proporcionar a las personas y bienes materiales protección frente agresiones, robos, incendios etc., esté o no conectado a una Central de Alarmas o Centro de Control.

La seguridad aplicada a los sistemas de intrusión física es determinada por el Reglamento de Seguridad Privada [26], donde se contemplan aspectos relacionados con las medidas de seguridad. Se rige por la Norma UNE-EN 50131-1 que establece cuatro grados de seguridad en función del riesgo, quedando en esta orden asignados, además, en virtud de la naturaleza y características del lugar en el que se va a efectuar la instalación y de la obligación o no de estar conectados a una Central de alarmas o Centro de control, del modo siguiente [27]:

- Grado 1: sistemas de alarma dotados de señalización acústica, que no se vayan a conectar a una central de alarmas o a un centro de control.
- Grado 2: viviendas y pequeños establecimientos, comercios e industrias en general, que pretendan conectarse a una Central de alarmas o, en su caso, a un Centro de control.

- Grado 3: establecimientos obligados a disponer de medidas de seguridad, así como otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o, en su caso, a un centro de control.
- Grado 4: infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado, y empresas de seguridad de depósito en efectivo, metales preciosos, materias peligrosas o explosivos, requeridas o no de conexión con Central de alarmas o, en su caso, a Centros de control.

En cuanto a las características del sistema de seguridad:

- Tiene que estar compuesto por al menos 3 elementos de protección que permitan a la central diferenciar las señales producidas por una posible intrusión.
- Contar con la tecnología que permita acceder desde la Central de alarma bidireccionalmente.
- Toda instalación de obligado cumplimiento debe disponer de un proyecto de instalación elaborado de acuerdo con la Norma UNE-CLC/TS 50131-7, y un certificado obligatorio de instalación que deberá garantizar que el proyecto está realizado de conformidad con la Norma UNE antes expresada y cumple con las finalidades previstas.
- Una vez esté operativo el sistema de seguridad se requiere de una revisión anual presencial de todos los parámetros y tres revisiones presenciales o remotas de forma bidireccional si el sistema lo permite. Toda revisión será efectuada por personal cualificado.
- La verificación y confirmación de alarmas deberá ser realizado siguiendo el procedimiento y tiempos estipulados según la normativa establecida.

Actualmente, la mayor parte de los sistemas que se instalan pertenecen a Grado 2, pudiéndose estos conectar o no a CRA.

En la actualidad son más abundantes las instalaciones de sistemas de grado 2, en las cuales es muy aconsejable que cuenten con sistemas de videoverificación, tal y como se dispone

en los sistemas de grado 3, éstos por obligado cumplimiento. La videoverificación es el supuesto más claro que contempla la ley a la hora de validar una alarma y poder realizar el aviso a las fuerzas de seguridad. Por eso es aconsejable, en la mayoría de casos, la instalación combinada de un sistema de alarma con uno de videovigilancia.

5.2. Seguridad aplicable en sistemas de intrusión en la red

Los IDS deben ser tratados como un elemento complementario en las políticas de seguridad de las organizaciones, pero antes de implementar o instalar un sistema de detección de intrusiones se recomienda analizar la política de seguridad y ver cómo adaptar el IDS en ella:

- Se recomienda una política de seguridad bien definida y de alto nivel, que cubra lo que está y lo que no está permitido en nuestro sistema y nuestras redes.
- Procedimientos documentados para que proceda el personal si se detecta un incidente de seguridad.
- Auditorías regulares que confirmen que nuestras políticas están en vigencia y nuestras defensas son adecuadas.
- Personal capacitado o soporte externo cualificado.

Para la aplicación y seguimiento de los protocolos de seguridad a seguir accedemos a las siguientes normativas y leyes relacionadas con la seguridad de la información:

Norma ISO 27001 [29]

Se trata de un estándar para la seguridad de la información que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar).

Un sistema de gestión de seguridad de la información (SGSI) permitirá a las empresas identificar los riesgos de seguridad más significativos de su negocio y reducirlos aplicando los controles adecuados en cada momento. Protegerá así la confidencialidad, integridad y disponibilidad de los datos de su empresa.

Si el SGSI de una empresa cumple y está certificada con el estándar ISO 27001 (ISO/IEC 27001:2005) garantiza la buena aplicación de medidas de seguridad a través de esta normativa internacional.

Puede aportar las siguientes ventajas a la organización:

- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de su organización con la seguridad de la información.
- Reducción del riesgo de robo o corrupción de información.
- Mayor confianza de clientes y socios estratégicos.
- Obtención de un sello que diferencia su organización en el mercado.

Norma ISO 20000 [30]

Estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información) para las empresas que supuso el primer sistema de gestión en servicio de TI certificable bajo norma reconocida a nivel mundial. Está especialmente enfocada a los servicios de TI y a que los proveedores de estos los ofrezcan garantizando determinados requerimientos.

Una manera de demostrar que los servicios de TI están cumpliendo con las necesidades del negocio es implantar un Sistema de Gestión de Servicios de TI (SGSTI) basado en los requisitos de la Norma ISO/IEC 20000.

La ISO 20000 establece que se dispone de procedimientos y controles adecuados *in situ* para proporcionar un servicio de calidad de TI coherente y a un coste efectivo.

Si un proveedor de servicios TI garantiza unos niveles de servicios determinados y está certificado en la ISO 20000, tendremos la garantía de que dicho proveedor ha desplegado el servicio, lo monitoriza y lo gestiona con el objetivo de que dichos niveles de servicio se cumplan. También sabremos que anualmente pasan una auditoría independiente que confirma que esto es cierto.

LOPD [28]

Todas las organizaciones que gestionen datos personales están obligadas a cumplir con La LO 15/1999 de 13 de diciembre de Protección de Datos. Esta legislación afecta a todo tipo de organizaciones, desde autónomos a multinacionales

Según el tipo de datos personales que se gestionen, la organización deberá cumplir con unas medidas de seguridad, disponer de una documentación concreta y realizar unos trámites distintos.

6. VISIÓN HOLÍSTICA DE LA SEGURIDAD

Para obtener un sistema de seguridad completo se requiere la integración de elementos de protección física con elementos de protección informática, logrando así un sistema lo más efectivo posible.

6.1. Protección de la Seguridad Física

Los Sistemas de Seguridad mediante elementos tecnológicos, como son las centrales de intrusión, los sistemas de videovigilancia, control de accesos... requieren su integración con sistemas informáticos que dispongan de medios de protección altamente sofisticados.

La seguridad informática aplicada a la seguridad física está relacionada principalmente con el registro de datos físicos informatizados.

Todos los eventos de infracción detectados por estos sistemas son gestionados y analizados a través de medios y recursos informáticos, pasando a ser objeto de delito en caso de verificación de una infracción. Dada la importancia de cualquier evento, así como su gestión por personal autorizado, también es necesaria la disponibilidad de sistemas de protección de equipos que garanticen la privacidad e integridad de los datos utilizados. Para garantizar todo ello se requieren medidas de protección informática como es el caso de los IDS, analizados a lo largo de este estudio.

Los sistemas de protección informática enfocados hacia la seguridad física, son necesarios ante el riesgo de cualquier tipo de configuración y manipulación de información de vital importancia para el funcionamiento correcto de estos dispositivos.

Algunos ejemplos de aplicación son:

- Puestos de control de datos donde se almacenan los registros de grabaciones testigos de algún tipo de incidencia.
- Acceso a claves de armado y desarmado de Centrales de alarma de hogares y empresas.

- Intento de robo de claves de accesos de usuarios de terminales de control de accesos o sistemas de protección similar.
- Accesos a visualización de cámaras o registros de grabaciones mediante sistemas de grabación IP a través de la red.
- Control de bases de datos de las Centrales Receptoras de Alarmas donde son recibidos los avisos generados por las centrales de intrusión mediante comunicaciones GPRS / GSM y vía Ethernet a través de módulos de transmisión integrados en los sistemas.
- …etc.

6.2. Protección de la Seguridad Lógica o Informática

Cuando hablamos de *Seguridad Física* nos referimos a todos aquellos mecanismos generalmente de prevención y detección destinados a una protección física.

Si aplicamos la Seguridad Física a la Seguridad Informática hablaremos entonces de proteger físicamente cualquier recurso del sistema informático o dispositivo tecnológico, es decir, la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y protección ante amenazas, a los recursos e información confidencial.

Dependiendo del ámbito de aplicación y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

Los sistemas de Seguridad Física deben actuar como complemento de protección de sistemas de información ante las siguientes situaciones:

- Acceso físico: si un sistema informático tiene acceso físico al mismo, toda medida de seguridad implantada se convierte en inútil.
- Desastres naturales: además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los desastres naturales pueden tener consecuencias muy graves, por ello, es imprescindible contemplarlos en la política de seguridad de las empresas. Algunos desastres naturales son: tormentas eléctricas, inundaciones, humedad, incendios…

- Entorno inestable: factores que pueden sufrir variaciones en los sistemas informáticos como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

Como venimos diciendo a lo largo de todo el estudio de la seguridad, la Seguridad Informática tiene la misión principal de velar por la máxima protección e integridad de la información.

Toda información es archivada en uno o varios sistemas informáticos cuyo destino final es un medio de almacenamiento físico, partiendo desde el almacenamiento más simple, como es el caso de un dispositivo de almacenamiento como los discos duros, hasta los servidores ubicados en los Centros de Bases de Datos.

Cualquiera que sea el medio de almacenamiento debe ser protegido de cualquier robo o sabotaje, es ahí donde tienen su función los Sistemas de Seguridad y CCTV, así como el resto de sistemas de seguridad y medidas tanto de protección como de acceso al medio localizado.

6.3. Integración de sistemas de seguridad

Con todo lo expuesto en cuanto a la seguridad de los medios físicos y la seguridad de los medios tecnológicos diremos que se produce una acción recíproca entre ambos medios de seguridad. No existe ninguna plataforma totalmente segura, todo sistema de protección debe seguir una estrategia de seguridad integral.

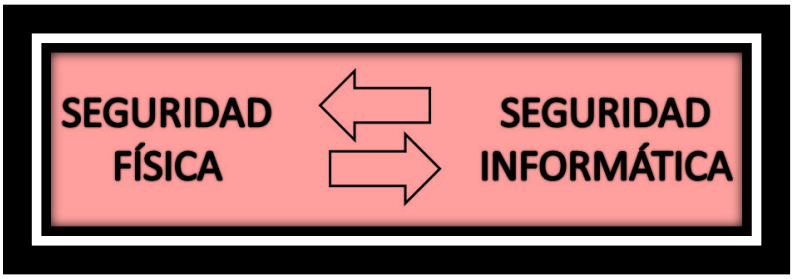

Fig. 7. Seguridad Física - Seguridad Informática.

Tal como se muestra en la Fig. 8, partiendo de la instalación más pequeña propia de una oficina o pequeño domicilio, hasta la instalación más compleja que se implante en una empresa, es necesario disponer tanto de seguridad física como de seguridad informática. Cualquier instalación que carezca de una de las dos no dispondrá de un grado mínimo aceptable de seguridad que garantice su protección. Ambos sistemas de protección requieren uno del otro para poder hacer efectivo el objetivo que se persigue: la seguridad.

7. SISTEMA DE SEGURIDAD INTEGRAL

7.1. Objeto del sistema a implantar

Para obtener un sistema de seguridad completo se debe realizar una integración de todos los componentes cuya finalidad es la misma: la protección absoluta de cualquier medio físico o lógico a proteger. Esto es posible mediante la convergencia entre los dos tipos de seguridad que hemos analizado: seguridad física y seguridad informática.

- Seguridad Física → *Aplicación de mecanismos de control y barreras físicas como medidas de protección de amenazas ocasionadas tanto por el hombre como por la naturaleza del medio.*
- Seguridad Lógica → *Aplicación de técnicas de control para asegurar la confidencialidad, integridad y disponibilidad de la información.*

Estamos analizando dos tipos de seguridad diferentes, pero a la vez están destinadas al mismo fin y con interpretaciones similares. Por ejemplo, en los dos sistemas de seguridad se habla de:

- Análisis de riesgos.
- Control de accesos.
- Detección de intrusiones.
- Protocolos y medidas de seguridad.

Un servicio de seguridad integral tiene el objetivo de contrarrestar todos los posibles ataques a la seguridad mediante mecanismos y sistemas de seguridad.

Las principales funciones de este servicio son las que se detallan en la Tabla 3:

SERVICIO	OBJETIVO
Autentificación	Garantizar la procedencia de los objetos o personas
Control de Acceso	Prevenir el uso no autorizado
Confidencialidad	Proteger toda información importante
Integridad	Garantizar el estado correcto de la persona o elemento físico o lógico.
Disponibilidad	Asegurar que el objeto o información esté disponible al personal autorizado.

Tabla 3. Funciones del Sistema de Seguridad Integral

La seguridad integral de una persona u organización contempla el acceso a las instalaciones o puntos críticos de las mismas, la protección de los elementos físicos y la protección de los sistemas informáticos de accesos internos no autorizados e intrusiones a través de la red.

7.2. Elementos de seguridad

7.2.1. Controles de Seguridad Física

Dentro de los elementos que van a componer un Sistema de Seguridad completo podemos hacer una diferenciación general en varios apartados: Circuito Cerrado de Televisión, Sistema de Seguridad y Control de accesos.

Circuito Cerrado de Televisión

Un sistema de CCTV está compuesto por los siguientes elementos necesarios: servidor de video, cámaras de vigilancia, cables y monitor.

Un correcto diseño del sistema requiere:

- Determinar la finalidad del sistema y la ubicación de las cámaras.
- Elegir el tipo de cámara adecuada según su utilidad.
- Determinar el puesto de control de visualización de las cámaras.

- Determinar el medio de transmisión de la señal de vídeo de la cámara al monitor.
- Elegir el equipo de videograbación.

Describimos los elementos principales con las características mínimas a tener en cuenta de un sistema de CCTV:

Grabador de video

Se trata del elemento principal del Sistema de CCTV. Será el encargado de administrar todas las imágenes recibidas desde las cámaras. Está dotado con un software con el que podemos gestionar según las necesidades del usuario todas las acciones relativas al almacenamiento y visualización de los videos captados, la Fig. 8 muestra un ejemplo.

Fig. 8. Grabador Digital.

Cámaras tipo “minidomo” interior/exterior

Cámara tipo “minidomo” de color, similar a la mostrada en la Fig. 9, con sistema antivandálico y protección IP66, especialmente diseñada para resistir las inclemencias del tiempo y los malos tratos propios de cualquier instalación.

Gracias a su óptica varifocal esta cámara puede controlar todo lo que pase en el exterior cubriendo un amplio rango de visión.

Fig. 9. Cámara tipo “minidomo”.

Cámaras tipo “bullet” exterior

Para la recepción de imágenes en las instalaciones se utilizan cámaras tipo “bullet” de exterior, como la que aparece en la Fig.10, apta para captación de imágenes tanto de día como en condiciones de baja luminosidad.

Poseen funcionalidad día/noche con filtro de conmutación mecánica. Asimismo, utilizan leds infrarrojos para conseguir captar imágenes en total oscuridad. Las podemos encontrar con óptica fija o varifocal para una mejor adaptación a los objetos que se desea enfocar.

Fig. 10. Cámara tipo “bullet”.

Cámara domo motorizada

Elemento de captación de imágenes apto para exterior y con óptica varifocal obteniendo una mayor adaptación del objeto a enfocar. Permite controlar el movimiento horizontal, vertical y el zoom de la cámara, la Fig. 11 muestra un ejemplo.

Está compuesta por un sensor CCD con alta resolución y protocolo de impermeabilidad IP66, lo que permite su utilización tanto para exteriores como interiores, resistiendo tanto a la lluvia como al polvo.

Fig. 11. Cámara tipo "domo".

Cámara IP

Cámara con tecnología IP y alta resolución con visualización día / noche. Contiene un servidor web integrado y permite una transmisión en tiempo real con control remoto de imágenes desde cualquier dispositivo.

Cámara térmica

Cámara para visualización de imágenes por infrarrojos que no requieren de iluminación, lo que permite una amplia visualización de amplias zonas incluso en condiciones meteorológicas desfavorables, cubriendo una visión mayor que una cámara convencional En la Fig. 12 aparece una imagen de este tipo de cámaras.

Fig. 12. Cámara térmica.

Sistema de Seguridad

Hoy en día los sistemas de intrusión son un elemento más en las tiendas y empresas, siendo cada vez más habituales también en los hogares particulares. Protegen sus bienes y activos de posibles robos proporcionando una alta seguridad mediante su alta tecnología. Paralelamente actúan como elemento disuasorio y permiten su automatización con sistemas de encendido de luces, puertas u otros dispositivos.

El principal funcionamiento de los Sistemas de Seguridad está basado en la detección de robo, intrusión e incendio mediante sensores de varias tecnologías conectados a Centrales de alarmas.

Las centrales disponen de elementos de salida con los que avisar del estado del sistema. Cuando uno de los elementos sensores detectan una situación de riesgo estos transmiten inmediatamente el aviso a la central, esta procesa la información recibida y ordena en repuesta la emisión de señales sonoras o luminosas alertando de la situación. Todos estos elementos poseen un control contra sabotaje de manera que si en algún elemento se corta la alimentación o se produce la rotura de algunos de sus componentes se enviará una señal a la central de alarma para que ésta accione los elementos de señalización y aviso correspondientes.

Central de intrusión

Dentro del Sistema Anti-intrusión definimos este elemento como el encargado de gestionar todos los saltos de alarma producidos en cada uno de los detectores instalados. Desde la central podremos realizar todas las acciones de configuración necesaria, armado/rearmado del sistema, programación de eventos, etc. En la Fig. 13 podemos visualizar el modelo de una central de intrusión de uno de los numerosos fabricantes del mercado actual.

Fig. 13. Central y teclado de intrusión.

Detectores volumétricos infrarrojos

Este dispositivo electrónico es capaz de captar la radiación térmica emitida por los elementos de la zona controlada, por lo que, en consecuencia, la radiación que es emitida por un intruso será detectada.

La Fig. 14 muestra un ejemplo de este dispositivo, cualquier movimiento no autorizado dentro de un edificio es detectado por este elemento, el cual producirá el salto de alarma correspondiente.

Fig. 14. Detector volumétrico IR.

Detectores de doble tecnología

De aspecto similar al detector infrarrojos, como su nombre indica, aúna dos tipos de detección diferentes, sirviéndose, en este caso, de tecnología infrarrojos y microondas. De esta manera, se consigue reducir significativamente las falsas alarmas generadas en espacios conflictivos.

Detectores magnéticos

Elemento de alta seguridad para protección contra sabotaje de apertura de puertas y ventanas.

Dispositivo sensor de apertura integrado por dos unidades necesariamente hermanadas en una posición determinada, tal y como muestra el ejemplo de la Fig. 15. La separación de estas dos piezas produce un cambio mecánico en los contactos de una de ellas, lo que provoca una abertura, produciéndose así un salto de alarma.

Fig. 15. Detector magnético o de apertura.

Barrera infrarrojos

Estas barreras están compuestas por un emisor y un receptor. El principio de funcionamiento está basado en la emisión continua de un haz de infrarrojos invisible que va del emisor al receptor.

Este dispositivo es elegido, por su diseño específico, similar al de la Fig. 16, para cubrir accesos tipo puerta o ventana. En este caso, no se necesita cubrir grandes distancias con lo que de esta forma se consigue una solución más económica, a la vez que eficiente y ajustada a cualquier necesidad.

Fig. 16. Barreras IR.

Barrera microondas

Este dispositivo nos permite crear un "muro invisible" para la protección del flanco más proclive a sufrir intentos de intrusión. Son las más apropiadas para detección a larga distancia y su tasa de falsas alarmas es notoriamente baja debido a su sensibilidad y volumen de detección parametrizable.

Estas barreras están formadas por un emisor y un receptor, como los mostrados en la Fig. 17. El emisor está continuamente emitiendo microondas que son recibidas por el receptor**.** Cuando algún cuerpo u objeto se interpone en la transmisión, es decir, cruza la barrera, el receptor recibirá las microondas con menos potencia (ya que parte han sido absorbidas por el obstáculo).

Fig. 17. Barreras Microondas.

Control de accesos

Los sistemas de control de accesos son los sistemas de seguridad que más demanda han obtenido en los últimos años en seguridad. Se dispone de varios tipos de tecnologías en base a la función a desempeñar.

Control de acceso peatonal

Los sistemas de control de acceso peatonal se implementan para tener el control de todo el personal que transita en un espacio público o privado, asegurando el paso de personas que cuentan con un libre tránsito y restringiendo el paso de personas no autorizadas. La Fig. 18 indica un ejemplo de los sistemas de alta tecnología que se están instalando en la actualidad.

Fig. 18. Control de accesos peatonal.

Control de acceso vehicular

La integración de sistemas de control de accesos vehicular mediante lectores de matrículas, propios de parkings y accesos a grandes instalaciones, permite el control de vehículos en un espacio público o privado.

Control de personal

Un sistema de control de asistencia como los que se pueden ver en la Fig. 19, mediante lectores de tarjetas de proximidad o sistemas biométricos como lectores de huella digital permite llevar el control exacto de todas las entradas y salidas a instalaciones.

Fig. 19. Control de accesos personal.

7.2.2 Controles de Seguridad Informática o Lógica

Control visual

En el ámbito de la seguridad es importante conocer el tipo de tráfico que circula por la red y poder detectar tráfico de carácter malicioso.

La forma de vigilar el tráfico se realiza mediante el monitoreo de forma constante con el fin de determinar el tipo de tráfico que circula con el fin de detectar posibles fallos de dispositivos específicos, de diseño de la topología y de la seguridad. La Fig. 20 escenifica desde el mundo real el procedimiento lógico llevado a cabo en las redes.

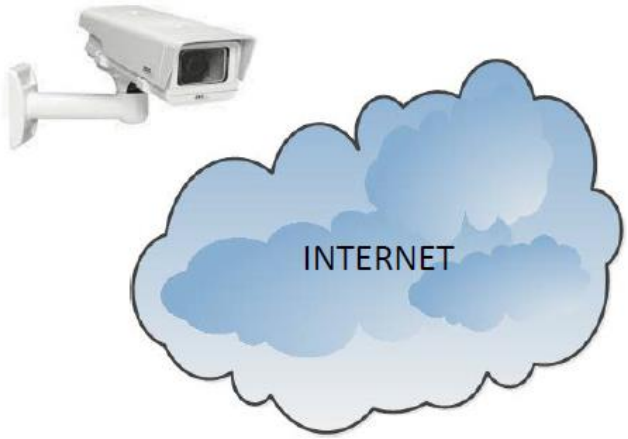

Fig. 20. Vigilancia de la red.

La técnica de visualizar tráfico en la red se llama “SNIFFING”.

Un sniffer es un programa que retiene o captura datos de la red, almacenándolos para su análisis posterior. Esta técnica permite obtener información y claves de acceso de sistemas de una red.

Existen dos formas de hacer sniffing, mediante software que es la más habitual, o mediante hardware, que consiste en conectar un cable de red a un dispositivo que permita capturar el tráfico.

Por lo tanto, un sniffer de software captura todos los paquetes que pasan por delante del PC en la que está instalado, es decir, un usuario que se conecte a Internet vía módem e instale un sniffer en su máquina sólo podrá capturar los paquetes de información que salgan o lleguen a su máquina.

Las tarjetas de red Ethernet están construidas de tal forma que, en su modo normal de operación, sólo capturan los paquetes de datos que van dirigidos hacia ellas, ignorando la información cuyo destino es otra máquina. Para capturar todos los paquetes que pasan por delante del sniffer, la tarjeta de red tiene que configurarse en modo promiscuo.

La forma más inmediata de saber si un determinado adaptador de red está en un modo promiscuo es utilizar un programa que nos permita configurar los adaptadores de red instalados en una determinada máquina y obtener información de su configuración.

Uno de los programas que nos permiten detectar cuándo un adaptador de red se encuentra en modo promiscuo es el conocido como "ifconfig".

En Internet existen varios programas, además de "ifconfig", que permiten detectar sniffers que utilizan el modo promiscuo.

Podemos utilizar estas herramientas para rastrear problemas en la red o para monitorear actividades de la misma.

Sistema de detección de intrusiones

Tal y como hemos analizado a lo largo de este estudio, en base a lo que se necesite proteger y de qué manera tenemos varios sistemas de detección de intrusos:

- IDS: intenta detectar y avisar de manipulaciones y ataques, pero no actúa.
- IPS: sistema de prevención de las intrusiones, actúa contra las intrusiones.

Hay varios ámbitos de aplicación en función de su aplicación:

- HIDS: sistema de detección de intrusiones en un host. Monitorizan y sólo llegan hasta la tarjeta de red.
- IPS: no actúa, sólo supervisa, en definitiva, alerta de intrusiones.
- IDS: monitorizar todo lo que pasa por la red, pero no está activo, está mirando.

Haciendo una clasificación genérica, tenemos dos tipos de sistemas de seguridad como medidas de protección ante cualquier ataque o sabotaje:

- Sistema Proactivo (IPS): Establece políticas de seguridad para proteger un equipo o una red.
- Sistema Reactivo (IDS): Alerta ante la detección de un posible intruso.

Al igual que ocurre con los sistemas de seguridad física, los sistemas de detección de intrusos están formados por un elemento central o consola y por detectores o sensores que avisan de las intrusiones.

Control de accesos lógico

Los controles de accesos están implementados para garantizar el acceso a un recinto o sistema mediante la identificación de un usuario o grupo de usuarios autorizados.

Hay tres métodos de identificación de personas:

- Dispositivos biométricos.
- Identificación usuario / contraseña
- Sistemas criptográficos: tokens o certificado digital

En la actualidad el sistema más utilizado sigue siendo la identificación por usuario y contraseña. En seguridad, con el paso del tiempo se están desarrollando e incorporando cada vez más dispositivos biométricos, su lenta implantación ha sido causada por el precio de los equipos de esta tecnología.

Una seguridad más completa está basada en la combinación de varios de estos sistemas, en especial la identificación mediante contraseñas combinada con cualquier otro sistema.

En los sistemas operativos y las aplicaciones con seguridad a través de identificación por contraseñas, se deben guardar las contraseñas encriptadas en ficheros. El problema recae en que estos ficheros no disponen de permisos, lo cual implica que, en un principio, sean accesibles a cualquier usuario. Para hacer difícil el descifrado de contraseñas se utilizan sistemas de encriptación irreversibles y, además, el descubrimiento de una contraseña no da pistas sobre las otras.

Vulnerabilidad de contraseñas

Las contraseñas son el punto más crítico y vulnerable de la seguridad del sistema de información es la vía directa de ataque a cualquier recurso.

Las técnicas empleadas para descubrir una contraseña de usuario son:

- Acceso al fichero de contraseñas: Si se tiene acceso al fichero de contraseñas se utilizan programas denominados *Crackers* que prueban todas las posibilidades hasta encontrar una que al encriptarse coincide.

  Utilizan dos métodos:

  - Diccionario. Técnica que consiste en probar palabras que puedan aparecer en una enciclopedia: nombres, números, fechas…
  - Prueba y ensayo. Se prueban todas las combinaciones de letras, números y signos posibles. Método mucho más lento que el anterior pero al final siempre da resultado.
- Caballos de Troya: Se sustituyen programas útiles por aplicaciones preparadas por el atacante que tienen el mismo nombre. Los ejecuta el propio usuario pensado que son un programa y realizan funciones de observación, modificación o destrucción de la información. Los caballos de Troya sirven para muchos tipos de ataques, uno concreto es la captura de contraseñas. Se puede hacer sustituyendo uno de los programas que tratan las contraseñas, capturando el teclado o capturando las transmisiones por la red.
- Espías de la red. Método consistente en la instalación de un programa llamado sniffer que captura toda la información que circula por la Ethernet o Token Ring de la máquina. Estos programas descubren las contraseñas mientras circulan por la red. Si no están encriptadas (hay muchos sistemas que no encriptan las contraseñas para enviarlas), el atacante ya ha conseguido su medio de acceso. Pero si están encriptadas también los puede utilizar repitiendo el mensaje como respuesta a una petición de identificación. El atacante únicamente necesita poder instalar en el servidor o en una máquina de la misma red un programa de este tipo.
- Ingeniería social: Método más utilizado por los atacantes que consiste en descubrir las contraseñas directamente de los usuarios, observando el teclado cuando se introduce la contraseña, descubriendo la contraseña escrita en un papel, pedirlo por correo electrónico o teléfono haciéndose pasar por el administrador, etc...

Certificado digital

Un certificado digital es un documento que permite al firmante identificarse en Internet por mediación de un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Este sistema está protegido contra robo y pérdidas mediante el siguiente proceso de acceso por validación:

Un usuario autorizado con este sistema debe tener:

- Clave privada de algún algoritmo asimétrico.
- Certificado digital con la clave pública pareja de la privada y firmado digitalmente por el servidor.

En seguridad de control de accesos de sistemas informáticos si siempre se accede desde la misma máquina se puede grabar en el disco, pero si se requiere el control de accesos a distintas máquinas o lugar la solución es utilizar tokens (en concreto tarjetas chip) donde se almacenan los certificados y se implementa el protocolo.

Tokens

Los tokens son dispositivos electrónicos utilizados para el control de accesos de usuarios, son de un tamaño reducido y se usan para almacenar claves criptográficas como las firmas digitales o datos biométricos.

Existen dos clases claramente diferenciadas:

- Memorias: Guardan una palabra clave, contraseña. La ventaja es poder utilizar contraseñas aleatorias sin necesidad de recordarlas.
- Inteligentes: Son equipos electrónicos que realizan un algoritmo donde se crean contraseñas de un uso (OTP) o se genera un protocolo entre el servidor y el token (certificados).

Pueden estar contenidos en:

- Tarjetas magnéticas. Sólo permiten memoria, se necesita un lector magnético.
- Tarjetas chip. Tienen un procesador interno que permite inteligencia. Se necesitan lectores especiales.
- Memorias EPROM o Flash. Se introducen en llaveros u otros objetos pequeños y permiten almacenar contraseñas sin inteligencia.

El principal problema de este sistema es la pérdida del token, por ello son configurados con la identificación por contraseña o sistema biométrico.

Sistemas biométricos

Estos sistemas utilizan una característica física del usuario como medio de autentificación del usuario. Son sistemas mucho más seguros que los de contraseña sobre todo si se combinan con otros y proporcionan las siguientes características:

- Intransferibles: El atacante no los puede utilizar aunque los conozca, característica suficiente para considerarlos mejor sistema que los de identificación por contraseña.
- No requiere gestión: no es necesaria gestión del usuario, como cambiarlos a menudo, recordar frases, etc...
- Sirven tanto para accesos físicos como lógicos.
- Son muy seguros ante cualquier ataque.

Fig. 21. Sistema biométrico de lectura de huella digital.

La principal desventaja que presentan es su coste, al necesitar dispositivos electrónicos adicionales para realizar las lecturas resultan ser más caros.

Los sistemas biométricos actuales están basados en el reconocimiento por huella digital, como el modelo que aparece en la Fig. 21, rostros, iris, retina, voz...

Con los sistemas de accesos mediante tecnología biométrica se consigue eliminar mecanismos que puedan suponer pérdidas o robos, como las tarjetas de acceso y la identificación por contraseña.

7.3. Implantación del sistema de seguridad

En la actualidad toda la vida personal y empresarial está basada en la información y aunque esta no tiene por qué estar contenida en sistemas informáticos, es difícil imaginar que no lo esté en los tiempos que vivimos. Dada esta situación actual planteamos la integración de los medios de protección física e informática como objetivo de la implantación del plan de seguridad de cualquier instalación.

Al hacer un estudio de todos los activos a tener en cuenta en la propuesta de integración de sistemas de seguridad describimos la relación de estos elementos dentro de una organización:

- Personal: conjunto de personas que interactúan en una organización, en este caso usuarios internos y usuarios externos.
- Datos: son el objeto a proteger, siendo el resto de activos los medios de protección de los datos. Tenemos datos a modo empresarial: económicos, fiscales… y datos a modo personal: intimidad, confidencialidad…
- Software: está formado por los sistemas operativos y aplicaciones que ponen en funcionamiento todo tipo de sistema de información.
- Hardware: se trata de los medios físicos en los que se instalan los sistemas operativos y aplicaciones que permiten el funcionamiento de éstos y almacenamiento de información. Entre los distintos tipos de hardware tenemos: servidores, terminales, periféricos, módem, router…
- Redes: forma la vía de comunicación y transmisión de datos tanto en redes internas de las organizaciones como en Internet.

- Instalaciones: lugar donde se ubican los medios a proteger: edificios, locales, oficinas, vehículos…
- Soportes: ubicaciones donde se registran y almacenan datos de forma permanente, como pueden ser DVD, CD, disco duros, tarjetas de memoria, papel…

Una vez descritos los activos, hay que valorar el tipo de amenaza al que se está expuesto:

- Accidental o de fuerza mayor: incendios, inundaciones, errores humanos…
- Intencionada: siempre producida por la acción humana. Intrusión informática, robos o hurtos.

La protección de una empresa empieza por la seguridad perimetral, es decir, todo sistema que analiza el área de acceso a la misma. Esta protección la forman todos los mecanismos activos de prevención de intrusiones tanto físicamente como a través de la red.

Entre los mecanismos activos de seguridad física nos encontramos:

- Sistemas de CCTV y videoanálisis.
- Barreras perimetrales.
- Sistemas de detección perimetral.
- Control de accesos.

De forma análoga, en sistemas de seguridad lógica nos encontramos:

- Sistemas de detección de intrusos: IDS.
- Vigilancia de las comunicaciones.
- Control de accesos.

A la hora de establecer una política de seguridad se deben analizar todos los riesgos y amenazas con el fin de seleccionar las medidas de protección que garanticen los objetivos de seguridad.

Para ello se deben realizar, entre otras, las siguientes acciones:

- Identificación y valoración de los activos.
- Analizar las vulnerabilidades y amenazas que puedan afectar a la seguridad de los activos.
- Identificar los objetivos de seguridad de la organización y seleccionar las medidas de protección.

Según el mecanismo utilizado como medida de seguridad dentro del plan de seguridad establecido, hablaremos de seguridad física o seguridad lógica. Clasificamos los mecanismos de seguridad como:

- Prevención: actúan antes de que se produzca un ataque y su función es evitarlo.
- Detección: actúan cuando se produce un ataque y antes de que cause daños.
- Corrección: actúan después de producirse un ataque con el objetivo de corregir los daños causados.

Del análisis y estudio de la situación actual de la seguridad frente al riesgo de intrusión en las empresas u hogares y a través de la red, planteamos las siguientes medidas para obtener una protección lo más efectiva posible. Para ello analizamos a continuación, uno a uno, todos los mecanismos de seguridad que pueden intervenir según el tipo de sistemas a implantar en base al riesgo que se debe proteger, tal como se detalla en la Tabla 4.

- Seguridad lógica: *sistemas operativos, aplicaciones, bases de datos y todo tipo de información almacenada electrónicamente.*
- Seguridad física: *personas, instalaciones, hardware…*

SEGURIDAD FÍSICA	SEGURIDAD LÓGICA
INTRUSIÓN	
Sistemas de Seguridad: Transmisión Vía Radio, sistemas cableados, detectores volumétricos, detectores de vibración, contactos magnéticos, videoverificación, detección perimetral…	Sistemas de detección de intrusos: Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software…
CONTROL DE ACCESOS	
Control de Accesos: Lectores de proximidad, biométricos, sistemas de reconocimiento de matrículas...	Control de accesos lógico: Criptografía, Usuario / Contraseña, sistemas biométricos…
VIGILANCIA	
CCTV: Sistemas de Circuito Cerrado de Televisión, Videovigilancia IP, Análisis de video…	Vigilancia del tráfico de red
ANTIHURTO	
Sistemas Electromagnéticos, RF, Acustomagnéticos…	Protección de archivos, permisos de usuario…

Tabla 4. Elementos de seguridad física y lógica.

El plan de seguridad a implantar que garantice la máxima protección posible, bien sea de un pequeño local o de un domicilio, hasta una protección más compleja como puede ser una empresa de grandes dimensiones, comprende la prevención tanto de la intrusión física a las instalaciones como de la intrusión lógica por personal interno o a través de la red.

Centrándonos en la seguridad de sistemas informáticos, además de proteger el hardware, se deben emplear medidas de protección de los datos ya que, en realidad, la mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

La Tabla 5 muestra un esquema donde, en base a la función a desempeñar por cada elemento que compondrá el sistema íntegro de seguridad, podemos clasificar los dispositivos tanto físicos como lógicos en dos tipos:

- Seguridad activa: *Acciones previas a un ataque. Son de este tipo todas las medidas de seguridad lógica.* Como ejemplo tenemos los mecanismos de control de accesos a usuarios no autorizados a lugares o sistemas informáticos, instalación de sistemas de detección de intrusiones…
- Seguridad pasiva: *Acciones correctivas. Minimizan el impacto y los efectos causados por accidentes, es decir, se consideran medidas o acciones posteriores a un ataque o incidente.* Un claro ejemplo son las copias de seguridad.

En todo tipo de seguridad y si concretamos, en seguridad informática, nunca puede obtenerse una seguridad activa del 100%, con lo que se debe combinar la seguridad activa con medidas de seguridad pasiva.

MEDIO	SISTEMA DE SEGURIDAD		ELEMENTOS	
	FÍSICO	LÓGICO	ACTIVO	PASIVO
Acceso a instalaciones	**X**		Control de accesos: Sistemas biométricos, Reconocimiento de matrículas…	Sistema de intrusión y CCTV
Acceso a Información		**X**	Permisos de usuarios, Identificación usuario/contraseña, elementos criptográficos, Control de accesos biométricos, Sistemas IDS…	Sistemas IPS
		X		Sistemas de intrusión y CCTV
Robo de elementos materiales	**X**		Control de accesos	Sistemas de intrusión y CCTV

Tabla 5. Elementos de seguridad según el tipo de acción que desempeñan

Una medida de seguridad pasiva puede convertirse en activa en situaciones concretas. Un ejemplo muy claro de ello son los sistemas de CCTV. En caso de producirse un robo en unas instalaciones y todo quedase registrado por las cámaras de seguridad, si mediante los registros de éstas es posible la identificación del intruso, este sistema, principalmente pasivo, está actuando también de forma activa.

Una vez implantada y puesta en marcha la política de seguridad establecida de una organización, se deben programar auditorías que analicen el estado de los sistemas de seguridad. El objetivo de una auditoría es descubrir, identificar y corregir futuras vulnerabilidades, así como verificar el cumplimiento de la normativa actual de seguridad.

7.4. Convergencia Seguridad física-lógica

En tiempos de seguridad anteriores a la implantación de la tecnología IP, los entornos de seguridad física y seguridad lógica no permitían la integración y presentaban problemas de incompatibilidad.

Para resolver esta problemática, las organizaciones más avanzadas han apostado por integrar la seguridad física con la seguridad lógica a partir de un elemento común: la red IP.

Principales ventajas de la convergencia en seguridad:

- Reducción de riesgos, fallos y vulnerabilidades
- Visión holística de la seguridad empresarial
- Ahorro en costes y tiempo
- Mejor gestión de la seguridad
- Prevención de pérdida de datos
- Control de amenazas
- Comunicaciones seguras
- Control de acceso a infraestructuras y a la red

La integración de la seguridad en la red permite realizar procesos con mayor eficacia mediante el acceso a la información de forma inmediata y la interoperabilidad entre varios sistemas, reaccionando ante cualquier evento con mayor rapidez.

Todas las organizaciones deberían seguir una serie de pasos:

- Analizar el valor de cada activo
- Identificar posibles amenazas
- Aplicar los mecanismos de protección apropiados

El trabajo ya no es el local donde acudimos cada día, sino unas funciones laborales que pueden realizarse en cualquier momento y desde cualquier lugar.

La red IP es sin lugar a duda el único medio para lograr la unificación de los sistemas físicos y lógicos para garantizar una protección holística.

7.4.1. Seguridad de Accesos

La primera solución de la convergencia entre ambas seguridades empieza en la integración de los controles de accesos lógicos a la seguridad física. Los controles de acceso lógico y físico pueden unificarse y obtener la administración y gestión de personas mediante mecanismos de validación por accesos de autorización por credenciales y contraseñas. Se permite con ello combinar los accesos lógicos con accesos físicos, como pueden ser los lectores biométricos, resolviendo con ello el robo de información dentro de las organizaciones, al estar integrados los eventos de seguridad física con los accesos lógicos.

La integración de acceso físico-lógico permite solucionar la posible amenaza por parte de usuarios que acceden a la información a través de dispositivos de otros empleados sin autorización para ello.

Otra ventaja de esta solución es la encriptación de información en función de las credenciales de acceso físico, evitando la pérdida de información en caso de robo.

7.4.2. Seguridad de la información

En seguridad física la transmisión IP permite la configuración de equipos como las centrales de intrusión, configuración de forma remota de zonas, usuarios, contraseñas… Sin un buen sistema de seguridad de intrusión informática como puede ser el caso de los Sistema IDS analizados, los sistemas de Seguridad Física estarán en peligro, es decir, pasan de ser un elemento de seguridad a ser un elemento totalmente inseguro.

Otro ejemplo de la convergencia entre seguridad física y seguridad lógica son los sistemas de videovigilancia IP. Estos sistemas frente a los antiguos equipos de seguridad analógicos permiten la transmisión de información en tiempo real sin importar la ubicación, y la integración con otros sistemas.

Una vez analizado el funcionamiento de los sistemas de seguridad física actual, es evidente la importancia de la protección de la información que transmiten estos sistemas. Es necesaria la implantación de buenas medidas de seguridad informática que garantice el buen funcionamiento de los mecanismos de seguridad física, ocupando la responsabilidad de la buena transmisión de la información y la conservación de la información registrada y almacenada.

7.4.3. La Nube como nuevo modelo de almacenamiento

No hay duda de las ventajas de la tecnología del Cloud Computing, siendo una de las más significativas el ahorro económico gracias a la externalización de la infraestructura informática y del personal técnico.

Desde los departamentos de ingeniería informática de muchas empresas se están desarrollando aplicaciones para los sistemas de CCTV. Entre estos desarrollos se están ofreciendo servicios para el control y la gestión de eventos de los sistemas de CCTV en la nube.

El almacenamiento de videovigilancia es realizado en los últimos años por los servidores de almacenamiento DVR y NVR, junto con las soluciones IP.

La rápida modernización de las aplicaciones tecnológicas da lugar al desarrollo de Centros de Datos con cada vez más soluciones. Por su parte, el aumento de la virtualización, consolidación y optimización de éstos está abriendo camino a la implementación del Cloud Computing como modelo de negocios.

El Cloud Computing o Nube, con su desarrollo en estos últimos años, se está convirtiendo en un medio de almacenamiento y control de sistemas de CCTV cada vez más eficaz y con grandes beneficios para el usuario.

Hay informes que indican que aún existen estrategias poco definidas en cuanto a la gestión y seguridad para este tipo de aplicación de la Nube, pero las previsiones dicen que la evolución es buena y el mercado experimentará un buen crecimiento.

La solución de sistemas de CCTV basado en La Nube aporta los servicios propios del Cloud Computing, la reducción de gastos energéticos, los gastos por la administración y la gestión de los centros de datos pertenecientes a la empresa.

Esta solución permite la grabación de forma remota a través de La Nube y tener en la misma almacenadas grabaciones, obteniendo las siguientes ventajas:

- Almacenamiento Masivo.
- Respaldo remoto.
- Consultas locales y remotas.
- Seguridad de la información por parte del proveedor de servicios.
- Menor costo que los sistemas convencionales
- Respaldo de las grabaciones en la nube

7.4.4. Control de procesos de Sistemas ERP

Dada la importancia de la visualización de imágenes y la ventaja que aportan las cámaras de videovigilancia ofreciendo características cada vez más mejoradas, como la alta resolución que presentan, hay empresas que están planteando e implantando otras variantes de control y seguridad. Una de estas alternativas es vincular las imágenes de las cámaras como medida de verificación de los procesos de logística de las empresas.

Se están empezando a aplicar mecanismos de control de procesos de los Software de Gestión Empresarial ERP (Enterprise Resource Planning) de las empresas más sofisticados. Uno de estos mecanismos se corresponde con el seguimiento visual.

El principal objetivo de este mecanismo es controlar todos los procesos de logística mediante la vinculación de los datos de los productos con las imágenes captadas por cámaras ubicadas para ello.

El procedimiento es el siguiente:

1º Llega un pedido a la instalación.
2º Se escanea el producto y se graba una imagen del evento.

3º El software de integración establece una conexión con el sistema ERP y se vinculan los datos del producto con la imagen.

7.5. Plataforma de integración de la seguridad en la empresa

7.5.1 Objeto de integración

Es habitual que en las organizaciones se disponga de varias áreas de seguridad gestionadas por departamentos distintos, sin embargo, en los últimos años se están planteando modelos de integración y gestión de sistemas de seguridad. Ahora bien, están integrando, por un lado, todos los elementos de sistemas de seguridad física y, por otro lado, sistemas de seguridad lógica o informática.

Las gestiones y comunicaciones empresariales mediante tecnologías móviles y accesos remotos a través de la red con clientes, partners y proveedores han dado lugar a una evolución empresarial más eficaz. Esta evolución necesita implantar medidas que garanticen la fiabilidad de este nuevo modelo de negocio ante cualquier riesgo de la seguridad empresarial. Cabe destacar que tal y como hemos venido comentando, las organizaciones ya no sólo se enfrentan a amenazas internas a la empresa, sino que también están expuestas a riesgos procedentes de otras empresas o personas ajenas a la organización.

Al proteger los activos empresariales suelen clasificar las amenazas como físicas o lógicas, haciendo las amenazas lógicas referencia a todo tipo de amenaza informática, de la información o de las TI (Tecnologías de la Información).

En los sistemas de Seguridad Física actuales se están implantando Sistemas de Integración de Subsistemas, es decir, Sistemas de Intrusión, Sistemas de CCTV, Sistemas de Reconocimiento de Matrículas y Sistemas de Control de Accesos, todo ello integrado en un único software. Esta integración se consigue a través de la comunicación de redes IP, mediante compatibilidad de sistemas y módulos IP de entradas y salidas adaptables a un software de integración desarrollado para ello. Todos los sistemas integrados pueden ser

controlados mediante el software, el cual permite, entre otras funciones, dibujar símbolos y configurar acciones a ejecutar según los eventos producidos.

Se pretende ir más allá de la integración física o lógica, la integración de ambos sistemas, todo ello embebido en un mismo servidor o hardware de integración. Esta situación permite ubicar e integrar todos los sistemas de seguridad en una misma máquina.

El propósito de una seguridad íntegra es la pretensión de unificar todos los desafíos de seguridad para poder así identificar e interactuar desde un único software con todos los sistemas de seguridad. Se consigue, con ello, evitar toda la complejidad de monitorización y gestión de cada sistema, así como poder realizar la cooperación de varios sistemas entre sí ante un evento de alarma.

7.5.2. Desarrollo del sistema

En instalaciones con alto riesgo de robo o sabotaje se están implantando medidas de seguridad importantes, y uno de los elementos en los que más se ha invertido y desarrollado son las plataformas de integración, con las cuales se consigue visualizar y controlar en tiempo real cualquier elemento de protección desde un mismo punto.

Características generales del software de integración:

- Software de video IP.
- Integración de cámaras de múltiples fabricantes.
- Independiente del hardware.
- Multiservicio.
- Integración con software de terceros: control de accesos, intrusión, incendio, reconocimiento de matrículas…

Todo esto se consigue mediante la creación de una red IP interna. Esta red es llevada a cabo por todas las canalizaciones y elementos de transmisión necesarios para conectar todos los dispositivos a la plataforma principal con la que se gestiona toda la seguridad.

El objeto de estos sistemas es la protección de los perímetros, de las instalaciones y seguridad en los edificios.

Ahora bien, como hemos podido analizar, con el avance de la tecnología y sus aplicaciones, hoy en día juega un papel más importante la seguridad informática.

Una simulación de lo que se visualiza y controla mediante los software de integración, que están desarrollando e instalando muchos fabricantes de dispositivos de seguridad física, se muestra en la Fig. 23, donde se detallan los elementos de protección física de una pequeña instalación.

Cada dispositivo está enlazado con la cámara que cubre el escenario donde está ubicado dicho dispositivo, obteniendo de la cámara un medio pasivo ante la actuación del elemento activo de amenaza de intrusión o sabotaje.

Este software de integración permite adjuntar planos y, a su vez, ubicar los distintos elementos de seguridad en los planos mediante símbolos de identificación pudiendo, de esta manera, localizar el dispositivo de forma inmediata ante cualquier posible evento. Conseguimos así, no solo la gestión de todos los dispositivos de seguridad, sino también su localización, lo que nos permite actuar de forma inmediata.

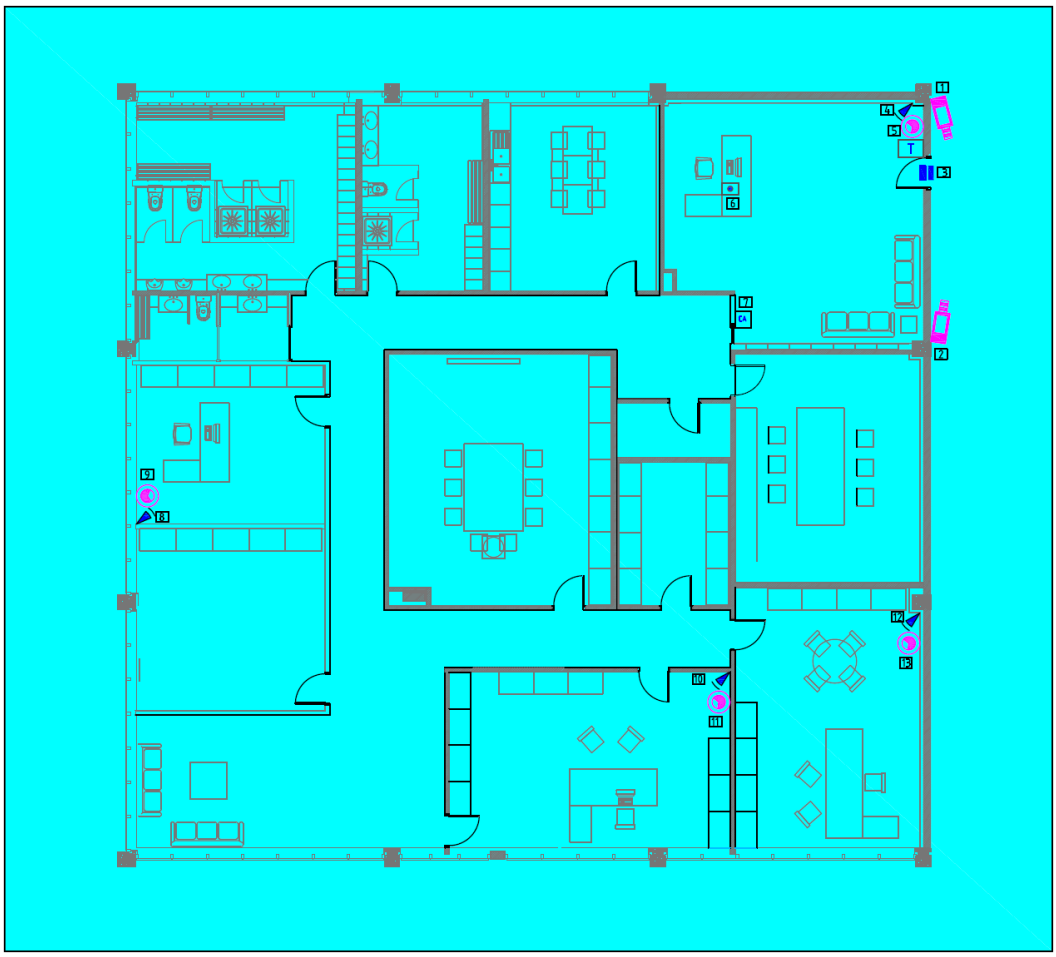

Fig. 22. Software de Integración de Seguridad Física.

Son claras las ventajas que han aportado los sistemas centralizados de la seguridad de instalaciones en un único puesto de control con una supervisión y control de todos los elementos de protección de forma más efectiva y eficaz.

Las cámaras de CCTV son enlazadas con los distintos elementos del Sistema de Seguridad, mediante las cuales se puede comprobar en tiempo real cualquier evento y obtener las grabaciones. Es decir, una amenaza del Sistema de Seguridad es detectada por uno o varios de los elementos de detección: sensores infrarrojos, contactos magnéticos, detectores de rotura, controles de accesos… y, posteriormente, es verificada por las cámaras de videovigilancia vinculadas al elemento de detección.

Actualmente, el acceso perimetral puede ser detectado y analizado directamente por las cámaras de vigilancia mediante sistemas de analítica de video. Éstos sistemas mayoritariamente, dado su elevado coste, son integrados principalmente en situaciones meteorológicas adversas como niebla, viento…, donde los sistemas de seguridad no pueden ser aplicados, haciendo necesaria la implantación de sistemas de analítica de vídeo con cámaras térmicas.

Estos software de integración, gracias a la tecnología IP, permiten su integración entre diferentes dispositivos de seguridad. También son adaptables con otros mecanismos que complementan una mayor seguridad. Entre estos mecanismos podemos encontrar dispositivos de automatismos como luces, puertas automáticas…

Para completar el sistema, se visualiza en la Fig. 24 el propósito de integración analizado, donde se incorporan elementos de seguridad informática al ejemplo de software de integración anterior. Entre los elementos de seguridad informática tenemos, por ejemplo, dispositivos de accesos mediante mecanismos de reconocimiento de tarjetas, contraseñas o sistemas biométricos, así como los sistemas de detección de intrusos del ordenador de cada empleado. Se consigue así la gestión y control tanto de la seguridad física como informática.

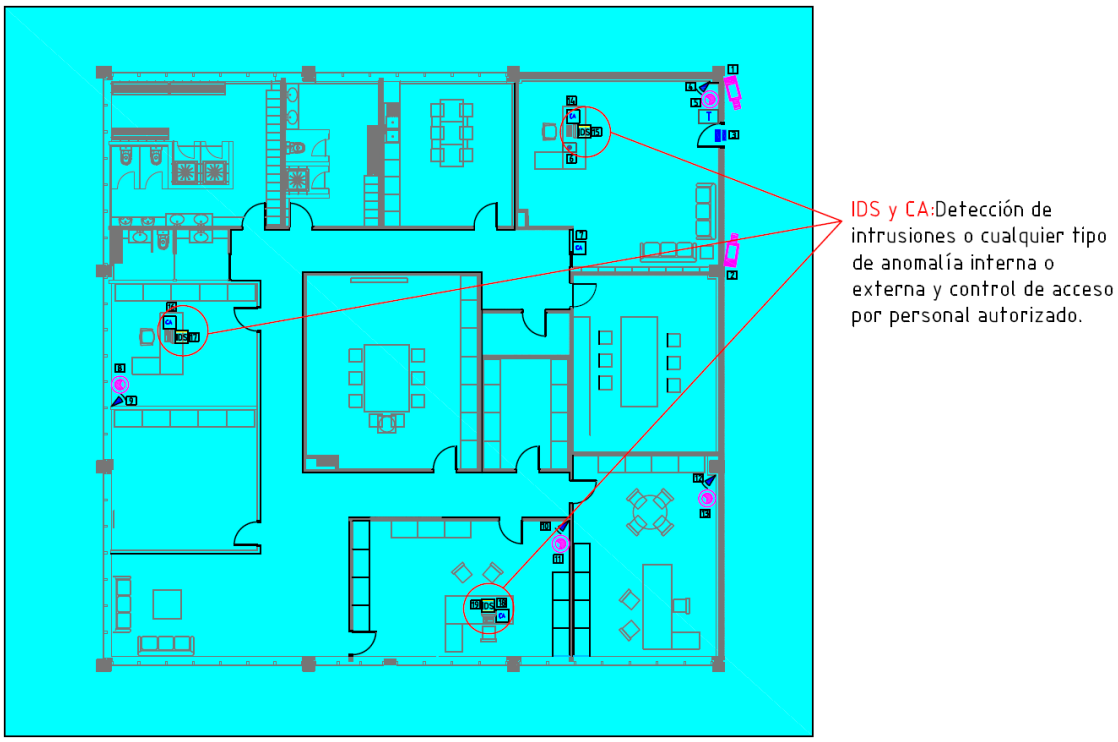

Fig. 23. Software de Integración de Seguridad Física y Lógica.

De forma análoga a la Seguridad Física se pueden obtener logros similares con la integración a la seguridad lógica.

Las cámaras de videovigilancia de los Sistemas de CCTV, al igual que ocurre con los sistemas de seguridad física, son un gran complemento para la seguridad informática.

Un intento de acceso a un equipo informático por personal no autorizado puede ser detectado mediante controles de acceso por lectura de tarjetas, introducción de contraseña o sistemas biométricos. Con el control visual de los equipos informáticos, a través de cámaras de videovigilancia enlazadas al control de accesos de cada equipo, se puede verificar cualquier amenaza mediante la visualización del evento en tiempo real y su grabación.

Otra aplicación más a añadir a la protección informática es la detección de anomalías, uso indebido o intrusiones de los sistemas informáticos. A través del puesto de control central y mediante la plataforma de integración se pueden recibir señales de alarmas de los sensores

de los sistemas de detección de intrusos IDS, permitiendo además poder actuar en tiempo real. Esto es posible con la integración de un software de acceso remoto enlazado al puesto de control central con cada equipo informático.

En definitiva, este tipo de plataforma es ampliable con cualquier elemento de seguridad, mediante la compatibilidad de los distintos sistemas que se quieran enlazar a través de las diversas configuraciones que nos permite la tecnología IP.

8. CONCLUSIONES Y LÍNEAS DE FUTUROS TRABAJOS

8.1. Conclusiones

El objetivo de un Plan de Seguridad es la protección de todo riesgo al que nos enfrentemos con el fin de garantizar la seguridad en su mayor grado respecto del sujeto a proteger, bien sea éste personas o elementos materiales o inmateriales.

Actualmente, en el mundo empresarial es imprescindible la comunicación con clientes y proveedores a través de la red: enviar y recibir correo, buscar información, realizar gestiones, etc.

La creciente evolución de Internet y las nuevas tecnologías desarrolladas en el ámbito de la seguridad, implica que paralelamente se esté produciendo un aumento de las necesidades y exigencias de los clientes con el fin de disponer de la máxima protección.

El avance de los sistemas de seguridad de intrusión física, así como los sistemas de CCTV como medio de verificación de sistemas de seguridad y control visual de instalaciones y recintos de forma remota con la aparición del análisis de video inteligente, capaz de detectar y visualizar intrusiones, implica la necesidad de asociar estos sistemas con sistemas de seguridad informática haciendo uso de redes IP. Esta convergencia permite la virtualización de ambos mecanismos de seguridad con el objetivo de la protección mutua.

Las redes IP necesitan del análisis, estudio y desarrollo continuo de sistemas de prevención y detección de intrusiones. Estos sistemas son el elemento principal y máximo responsable de la seguridad, es por ello que se requiere la integración de todo mecanismo de protección informática con los sistemas de seguridad física ya integrados en un único software.

La seguridad es una convergencia entre elementos físicos y elementos lógicos cuyo objetivo es el mismo: proteger y ser protegido.

Implementar una solución de seguridad integrada con medios de protección informática garantiza comunicaciones seguras, mayor tranquilidad frente a amenazas externas y prevención de pérdidas de información por acciones internas.

Hemos analizado todos los mecanismos de seguridad y comprobado el alcance que nos permite las comunicaciones de éstos mediante el uso de la tecnología IP. El desarrollo de software compatible entre varios productos y la integración de dispositivos mediante módulos IP, confirma y presenta una gran ventaja de cara a la seguridad de las empresas. Todo ello presenta un gran avance en seguridad para las empresas y la necesidad de implantar sistemas de seguridad unificados que abarquen todos los ámbitos de la seguridad, cuyo fin es garantizar una protección total.

8.2. Necesidades, líneas de trabajo

Con el avance de las tecnologías de la información y las comunicaciones a través de Internet, se propone la necesidad de investigar y avanzar un poco más en los sistemas de seguridad.

La utilización de los Sistemas de Seguridad y CCTV de instalaciones y recintos implica un aumento en las necesidades y exigencias de los clientes.

Hasta hoy, dentro de este mercado, el trabajo siempre ha estado orientado a la instalación de cámaras tanto analógicas como IP, cuyo objetivo es siempre el mismo: ser capaces de ofrecer y garantizar una protección y control visual remoto de instalaciones, recintos, viviendas, locales…

Para lograrlo, cumplimos necesariamente con varias premisas que han de cumplirse:

- Disponer de suministro eléctrico para la alimentación de los diversos equipos.
- Contar con comunicaciones ADSL para realizar una transmisión estable de las imágenes captadas.
- Ser capaces de guiar el cableado necesario desde cada cámara al equipo de grabación / transmisión (DVR o NVR) o establecer enlaces inalámbricos dentro de un área determinada (WiFi, Radio, etc…).

Actualmente, hemos de ir un paso más allá y ser capaces de controlar áreas remotas en las que no cumplimos uno o varios de los requisitos que enumerábamos:

- Zonas aisladas sin suministro eléctrico ni acceso a red.
- Visualizar varios puntos aislados y geográficamente alejados entre sí.
- Lograr un control visual de ubicaciones esporádicas y temporales.

Para lograrlo, se están aunando las diferentes tecnologías de las que ya disponemos hoy en día para conseguirlo. En definitiva, la meta consiste en llegar a cualquier ubicación sean cuales sean las condiciones que se presenten.

Ahora bien, como propuesta a ello se deben analizar también el estado actual y desarrollo de sistemas de seguridad informática que garanticen la protección máxima en su aplicación con tecnologías inalámbricas: WiFi, Bluetooth, GPRS…

9. BIBLIOGRAFÍA

[1]Real Academia Española, Diccionario de la Lengua Española. Vigésima Segunda Edición.
http://lema.rae.es/drae/?val=seguro

[2]Seguridad Informática SMR. Wiki del Módulo de Seguridad Informática del segundo curso del ciclo Sistemas Microinformáticos y Redes del profesor Sinuhé Navarro Martín. *IES Medina Azahara*
http://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

[3]III Estudio sobre bulos y fraudes en Internet. Asociación de internautas (AI). Madrid, 13 de septiembre de 2012.
http://www.internautas.org/graficos/PPT_IIIEstudioBulosyFraudes13sept.pdf

[4]INE: Instituto Nacional de Estadística
http://www.ine.es/

[5]Balance de la criminalidad 2012. Secretaría de Estado de Seguridad. Ministerio del Interior
http://www.interior.gob.es/file/59/59648/59648.swf

[6]CURSO OFICIAL DE "SISTEMAS ELECTRÓNICOS DE SEGURIDAD", Colegio Oficial de Ingenieros Técnicos de Telecomunicación. Julio de 2010.

[7]Apuntes de la Asignatura "Redes de computadores". Cuarto Curso de Ingeniería Informática y Doble Titulación. Rogelio Montañana, Profesor asociado del Departamento de Informática de la Universidad de Valencia.
http://www.uv.es/~montanan/redes/index.html

[8]Guía para empresas: seguridad y privacidad del *cloud computing*. Observatorio de la Seguridad de la Información de INTECO: Instituto Nacional de Tecnologías de la Comunicación. Edición: Octubre 2011
http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&ved=0CFMQFjAB&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2F2KMNG7mbyKb6gqdnJquPKw&ei=W1srUrOQGYfEsgadtYAo&usg=AFQjCNG7OaFYulQajLwfGbJMQenqBXS29g&bvm=bv.51773540,d.Yms

[9]Computación en la Nube e innovaciones tecnológicas. El nuevo paradigma de la Sociedad del Conocimiento. Luis Joyanes Aguilar, Catedrático de Lenguajes y Sistemas Informáticos. Universidad Pontificia de Salamanca.
http://gissic.files.wordpress.com/2011/07/computacion_en_nube_revista_paraguay_luis_joyanes.pdf

[10]Guía para clientes que contraten servicios de Cloud Computing. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS - 2013
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

[11]Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

[12]Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones
http://www.boe.es/buscar/doc.php?id=BOE-A-2003-20253

[13]Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp--Directiva-95-46-CE.pdf

[14]ENISA: Empresa Nacional de Innovación S.A.
http://www.enisa.es/

[15]PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 8. REVISTA BIMESTRAL. OCTUBRE 2010
http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/num_08.pdf

[16]Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Ingeniería Informática. Emilio José Mira Alfaro. Universidad de Valencia 2002.
http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

[17]Ataques informáticos. Debilidades de seguridad comúnmente explotadas. Jorge Mieres. Evil Fingers, Enero de 2009
https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

[18]Seguridad en Redes y Telecomunicaciones. Tipos de ataques en la red. Universidad Autónoma de Santo Domingo. 16 de Abril de 2012.
http://www.slideshare.net/alexpolanco1/tipos-de-ataques-en-la-red-alex-anny-dilannia-sixta-y-virtudes

[19]Detección de intrusiones en la nube: Consideraciones sobre los IDS en nubes públicas. Dave Shackleford
http://searchdatacenter.techtarget.com/es/consejo/Deteccion-de-intrusiones-en-la-nube-Consideraciones-sobre-la-IDS-en-nubes-publicas

[20]Seguridad Informática SMR. Wiki del módulo de Seguridad Infomática del segundo curso del ciclo Sistemas Microinformáticos y Redes del profesor Sinuhé Navarro Martín. *IES Medina Azahara*
http://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

[21]Seguridad Perimetral. Lección 5. INTYPEDIA: Information Security Encyclopedia. Alejandro Ramos Fraile. Madrid, febrero 2011.
http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

[22]Sistema de Detección de Intrusiones. Diego González Gómez. Julio 2003
http://derecho-internet.org/docs/ids.pdf

[23]Sistemas de Detección de Intrusos. Revista del Instituto Tecnológico de Informática.
http://www.iti.es/media/about/docs/tic/06/2005-02-intrusos.pdf

[24]Detección de intrusos en redes de telecomunicaciones IP usando modelos ocultos de Markov. Eduard Leandro Robayo Santana, Tesis de Maestría presentada para optar al título de Magíster en Ingeniería de Telecomunicaciones. Universidad Nacional de Colombia 2009.
http://www.bdigital.unal.edu.co/2409/1/299726.2009.pdf

[25]Sistemas de detección de intrusos. Antonio Villalón Huerta. Universidad Politécnica de Valencia. Mayo 2005.

[26]Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.
http://www.boe.es/buscar/doc.php?id=BOE-A-1995-608

[27]Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada.
http://www.boe.es/boe/dias/2011/02/18/pdfs/BOE-A-2011-3170.pdf

[28]LEY ORGÁNICA 15/1999 de 13 de diciembre, de protección de datos de carácter personal.
http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[29]NORMA ISO 27001
http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

[30]NORMA ISO 20000
http://www.aenor.es/documentos/certificacion/folletos/w_207_ISO_20000-1.pdf