Fundamentos de Auditoría Informática Basada en Riesgos

Daisy Elizabeth Imbaquingo Esparza
Marco Remigio Pusdá Chulde
José Guillermo Jácome León

EDITORIAL UTN
IBARRA - ECUADOR

Imprenta Universitaria 2016
Universidad Técnica del Norte

Diagramación & Diseño
Fernando Mafla Ibarra-Ecuador

EDITORIAL UTN
IBARRA - ECUADOR

ISBN: 978-9942-984-18-0
9 789942 984180

FUNDAMENTOS DE AUDITORIA INFORMÁTICA

BASADA EN RIESGOS

UNIVERSIDAD TECNICA DEL NORTE

AUTORES

Daisy Elizabeth Imbaquingo Esparza

Docente Investigadora
Facultad de Ingeniería en Ciencias Aplicadas
Universidad Técnica del Norte
deimbaquingo@utn.edu.ec

Marco Remigio Pusdá Chulde

Docente Investigador
Facultad de Ingeniería en Ciencias Aplicadas
Universidad Técnica del Norte
mrpusda@utn.edu.ec

José Guillermo Jácome León

Docente Investigador
Facultad de Ciencias Administrativas y Económicas
Universidad Técnica del Norte
jgjacome@utn.edu.ec

PARES REVISORES EXTERNOS:

MsC. Albert Espinal Santamaría
Docente Investigador
Facultad de Ingeniería en Ciencias Aplicadas
Escuela Politécnica del Litoral ESPOL

MsC. Margoth Elisa Guaraca Moyota
Directora de la Escuela de Sistemas
Pontificia Universidad Católica del Ecuador- Sede Santo Domingo

MsC. Paulina Ayala

Docente Investigador
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
Carrera de Ingeniería en Electrónica y Comunicaciones
Universidad Técnica de Ambato

ÍNDICE GENERAL

PRESENTACIÓN

El crecimiento exponencial de las tecnologías informáticas y su uso transversal en todo tipo de procesos, productos y servicios en empresas e instituciones, desemboca que en momentos determinados el uso de estas tecnologías se vuelva incontrolable, en ciertos casos llegando a ocasionar diferentes amenazas y vulnerabilidades informáticas intencionales o no intencionales y no identificadas, por lo es necesario tener mecanismos, procedimientos, metodologías, estándares que se enfoquen en la prevención, detección y mitigación de todo tipo de riesgos.

Para ello se ha desarrollado el presente libro con la finalidad de que el lector disponga de una base sustancial que nos permita llevar a cabo una auditoría informática vista desde las distintas aristas tecnológicas que se pueden presentar en las empresas o instituciones.

Se espera que el lector después de aplicar el presente texto en procesos de auditoria informática basada en riesgos obtenga la información necesaria que le permita implementar exámenes de auditoria informática de una manera técnica y documentada, resultados que le permitan efectuar recomendaciones sustanciales con la finalidad de que se implementen planes de mejora continua.

AGRADECIMIENTO

A la Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas y a la Carrera de Ingeniería en Sistemas Computacionales, por permitirnos cumplir un sueño de desarrollar un texto guía para los profesionales de Informática que deseen implementar una Auditoria Basada en Riesgos en cualquier tipo de institución.

1 SEGURIDAD INFORMÁTICA

1.1 Introducción a la Seguridad Informática

Seguridad Informática, es la disciplina que se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.(Cano, 2011)

1.2 Elementos vulnerables de un sistema informático

Una vulnerabilidad o fallo de seguridad, es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente a como funcionaban, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible. Las amenazas pueden ser de diferentes tipos, que son hardware, software, factor humano, y datos.

Vulnerabilidades en el hardware

Se pueden producir de forma intencionada o no. Incendios fortuitos en los sistemas, fallos físicos, rotura física de cables.

Otras vulnerabilidades pueden ser el desgaste el uso constante del hardware dejando el hardware obsoleto hasta dejarlo inutilizable.

El descuido y mal uso es otro de los factores requiriendo un mantenimiento, ya que no seguir estos hábitos supone un mayor desgaste reduciendo el tiempo de vida útil.

El suministro de energía es otro punto ya que los picos de voltaje pueden dañar nuestro sistema porque es recomendable instalar sistemas de suministro de energía.

Clases de vulnerabilidad de hardware:

Mal diseño: Es cuando los componentes de hardware del sistema no son apropiados y no cumplen los requerimientos necesarios, en otras palabras, dicha pieza del módulo no fue diseñada correctamente para trabajar en el sistema.

Errores de fabricación: Es cuando las piezas de hardware son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar usarse. Aunque la calidad de los componentes de hardware es responsabilidad del fabricante, la organización que los adquiere es la más afectada por este tipo de amenaza.

Suministro de energía: Las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos.

Desgaste: El uso constante del hardware produce un desgaste considerado como normal, con el tiempo este desgaste reduce el funcionamiento óptimo del dispositivo hasta dejarlo inutilizable.

Descuido y mal uso: Todos los componentes deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento.

Tipos de vulnerabilidades a la Red: La hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

1.3 Actividades de reconocimiento de sistemas

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

Detección de vulnerabilidades en los sistemas

Este tipo de ataques tratan de detectar y documentación las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como “exploits”).

Robo de información mediante la interceptación de mensajes

Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

Modificación del contenido y secuencia de los mensajes transmitidos

En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como “ataques de repetición” (“replay attacks”).

1.4 Análisis del tráfico

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los “sniffers”. Así, se conoce como

“eavesdropping” a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

Una organización podría protegerse frente a los “sniffers” recurriendo a la utilización de redes conmutadas (“switches” en lugar de “hubs”) y de redes locales virtuales (VLAN). No obstante, en redes locales que utilizan “switches” (es decir, en redes conmutadas), un atacante podría llevar a cabo un ataque conocido como “MAC flooding” para provocar un desbordamiento de las tablas de memoria de un switch (tablas denominadas CAM por los fabricantes, “Content Addresable Memory”) para conseguir que pase a funcionar como un simple “hub” y retransmita todo el tráfico que recibe a través de sus puertos (al no poder “recordar” qué equipos se encuentran conectados a sus distintas bocas o puertos por haber sido borradas sus tablas de memoria). Por otra parte, en las redes VLAN (redes locales virtuales) un atacante podría aprovechar el protocolo DTP (Dynamic Trunk Protocol), utilizado para poder crear una VLAN que atraviese varios switches, para intentar saltar de una VLAN a otra, rompiendo de este modo el aislamiento físico impuesto por la organización para separar sus distintas redes locales.

Políticas de hardware

- ✓ Inventario de Activos
- ✓ Perímetros de Seguridad físicas

- ✓ Controles de Seguridad Física
- ✓ Ubicación y Protección de equipos
- ✓ Suministro de Energía
- ✓ Seguridad De cableado
- ✓ Mantenimiento de los equipos
- ✓ Seguridad dl Equipamiento fuera de la organización
- ✓ Reutilización o Eliminación de equipos
- ✓ Ruta Forzosa
- ✓ Autentificación de Usuarios para Conexiones externas

Vulnerabilidades en el Software

Los ataques al software se pueden centrar contra los programas del sistema operativo, a los programas de utilidad o a los programas de usuario. Necesita de mayores conocimientos técnicos para los ataques hardware.

Una característica del malware, es que tiene la capacidad de acceder de forma remota a un sistema, sin consentimiento o discernimiento del usuario. Deshabilita las medidas de seguridad (como firewall, o antivirus), perjudicando al sistema y a la información, y en algunos casos incluso dañando la parte física del computador. Existe variedad de ataques software:

Bomba lógica: El programa incluye instrucciones que, al cumplirse una condición, provocan una distorsión del funcionamiento normal del

programa, que normalmente, deriva en daños al ordenador que lo ejecuta. Esta técnica es usada por algunos programadores. Introducen en la aplicación un código que se activa en una fecha determinada para que, si no ha cobrado por su trabajo ese día, destruya la información del ordenador en el que ha sido instalado.

Código Malicioso: Es cualquier software que entra en un sistema de cómputo sin ser invitado e intentar romper las reglas, esto incluye troyanos, virus, gusanos, bombas y otras amenazas.

Virus: Conocidos por todos los virus atacan a ficheros de nuestro sistema con el propósito normalmente de dañar nuestro sistema.

Puertas traseras: Son programas que permiten la entrada en el sistema de manera que el usuario habitual del mismo no tenga conocimiento de este ataque.

Troyanos: El objetivo de estos programas no es el mismo para el que aparentemente están diseñados. Se utilizan normalmente para instalar puertas traseras

Ingeniería Social: Consiste en mantener un trato con la persona administradora para indagar en sus costumbres o conocerla para elaborar un ataque más preparado. Esto incluye también suplantación de identidad.

Bonet: El crecimiento acelerado de la informática trae como consecuencia el malware, o software malicioso. Con el desarrollo de la inteligencia artificial, esta se combina con el software dañino o malware, naciendo así las botnets, redes de pequeños robots (o bots) con el fin de atacar y tomar hosts para que formen parte de su red. Realizando este proceso de forma automática y autónoma, y creciendo a un ritmo vertiginoso. Las Botnets, son llamadas también redes zombies, ya que los hosts se encuentran a merced de su BotnetMaster. Estas redes han logrado expandirse a lo largo de Internet afectando a miles y millones de usuarios, valiéndose de ingeniería social para "engañar" a sus víctimas. Un fenómeno que crece y difícilmente pueden atraparse a los culpables, ya que evolucionan constantemente para volverse casi indetectables.

1.5 Bases de la seguridad Informática

El amplio tema de la seguridad informática abarca todos aquellos mecanismos tanto de prevención como de corrección que utilizan las personas y las empresas sean estas grandes, pequeñas y medianas con el fin de proteger uno de sus mayores activos, su información. Siendo este un bien que tiene un valor equivalente a los activos de cualquier organización.

La protección de la información requiere de un conjunto de software específicos, estándares y metodologías existentes que permitan aplicar

las normativas certificables internacionalmente y técnicas apropiadas para llevar un control en la seguridad. Para ello se requiere los controles de seguridad, porque se considera un tanto difícil garantizar la seguridad de la información a un 100%, por cuanto intervienen diferentes amenazas a las que las organizaciones y/o personas se encuentran continuamente expuestas.

Para proteger de manera adecuada la información a gran escala se requiere de tres pilares fundamentales. En la Figura 1 se representa gráficamente los pilares de la seguridad de información.

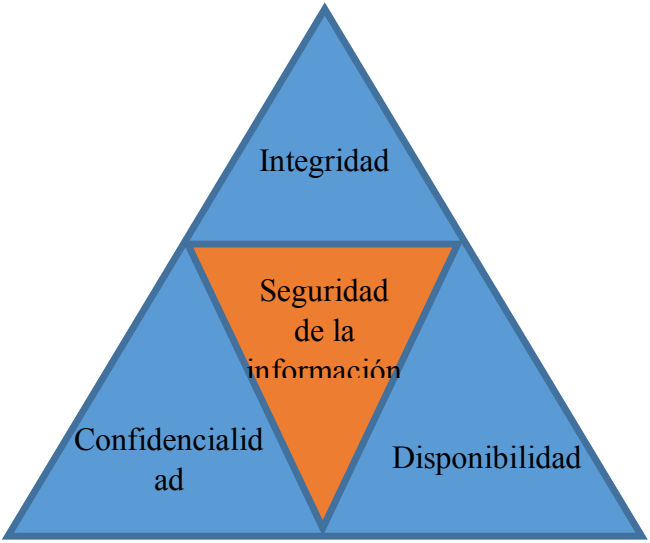


Figura 1. Pilares fundamentales de la seguridad de la información

Confidencialidad: La información sólo puede ser accedida y utilizada por el personal de la empresa que tiene la autorización para hacerlo.

En este sentido se considera que este tipo de información no puede ser revelada a terceros, ni puede ser pública, por lo tanto, debe ser protegida y es la que tiende a ser más amenazada por su característica.

Los profesionales responsables en las empresas de manejar información confidencial conllevan a una serie de connotaciones de carácter ético, pero sobre todo en seguridad informática conlleva a proteger los datos cuando sean transferidos o se encuentren disponibles en recursos compartidos e internet. En este orden se han considerado los mecanismos criptográficos para cifrar la información, en caso de que esta sea interceptada, ya que a pesar de que el atacante tenga la información esta estará cifrada y difícilmente podrá descifrarla. También existen mecanismos de ocultamiento de información, la cual se pueda a través de archivos teniendo presente que no existen sistemas 100% seguros, cuando el que ataca tienen el conocimiento para buscar el mecanismo de descifrar.

Integridad: Se refiere al momento en que la información no ha sido borrada, copiada o modificada, es decir, cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino. Un ataque a la integridad de la información se puede presentar en archivos planos de bases de datos, información documental, registros de datos, etc. Uno de los mecanismos más utilizados para

asegurar la integridad de la información es a través de la firma digital. (Suarez Sierra & Amaya Tarazola, 2013)

Disponibilidad: Se refiere a que la información facilitada en cualquier medio digital o software se encuentre disponible para el procesamiento de la información, para el correcto funcionamiento de una organización, así como de sus clientes o personal requerido sin que estos sean interrumpidos. Un claro tipo de ataque a este pilar, se puede presentar cuando se ha realizado la desconexión de un cable o medio de comunicación en la red de telecomunicaciones de la empresa, lo que ocasiona la denegación del servicio a sitios web o aplicativos, herramientas de seguridad antivirus, entre otros. (Suarez Sierra & Amaya Tarazola, 2013)

Hay que considerar que antes de que exista un indecente de seguridad que afecte cualquiera de sus pilares, debe haber un riesgo de seguridad que en su momento no fue detectado, esto quiere decir; que el significado de un riesgo es cuando existe una amenaza a la seguridad que no ha llegado a afectar a la organización. Un incidente, es cuando se materializa el riesgo. Es por ello, la necesidad de la aplicación de controles de seguridad que protege contra todo aquello que pueda causar un incidente de seguridad. Entre estos controles más recomendados se detallan en la Figura 2.

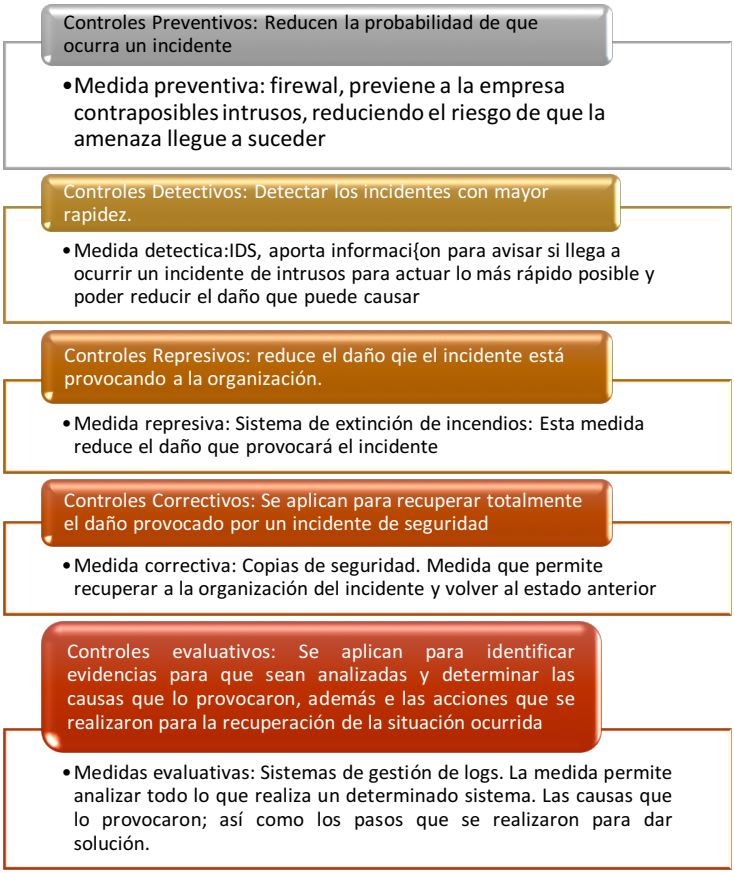


Figura 2. Controles de seguridad

1.6 Seguridad Pasiva

El fin de la seguridad pasiva es de minimizar los efectos causados voluntariamente o de un usuario o malware. Por ello se requiere que el personal de áreas tecnológicas realice algunas prácticas como, por ejemplo:

- ✓ Uso adecuado de hardware como: refrigeración del sistema, conexiones eléctricas adecuadas, dispositivos SAI
- ✓ Es importante realizar y utilizar copias de seguridad de datos y del sistema operativo.
- ✓ Crear particiones del disco duro, como particiones primarias y particiones extendidas. Las particiones primarias sirven para albergar sistemas operativos y datos de programa, todo disco duro tiene al menos una partición primaria y las particiones extendidas, las cuales se utilizan para alargar el número máximo de particiones.

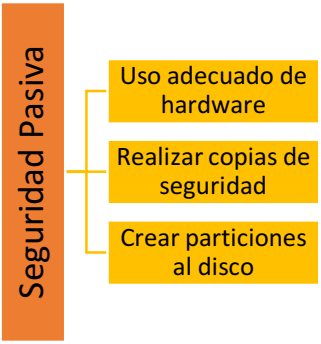


Figura 3. Actividades de la seguridad pasiva

1.7 Seguridad Lógica

La seguridad lógica informática es una referencia a la protección por el uso de software en una organización, e incluye identificación de usuarios y contraseñas de acceso, autenticación, derechos de acceso y

niveles de autoridad. Estas medidas son para asegurar que sólo los usuarios autorizados son capaces de realizar acciones o acceder a información en una red o un equipo concreto.(Universidad Internacional de Valencia, 2016)

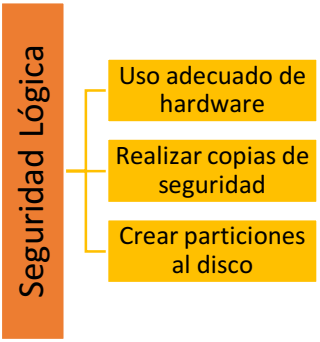


Figura 4. Actividades de la seguridad lógica

Características

Identificación y Autentificación: Es la primera línea de defensa para la mayoría de los sistemas informáticos, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios. Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.(SEGU.INFO, 2015).

Roles*:* El acceso a la información también puede controlarse a través de rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área, administrador del sistema, etc.

Transacciones*:* También pueden implementarse controles a través de las transacciones, por ejemplo, solicitando una clave al requerir el procesamiento de una transacción determinada.

Limitaciones a los servicios*:* Son las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que una organización disponga licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

Modalidad de Acceso*:* Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- ✓ Lectura: el usuario puede únicamente leer o visualizar la información. Pero no puede alterarla.
- ✓ Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.

- ✓ Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.
- ✓ Borrado: permite al usuario eliminar recursos del sistema como programas, campos de datos o archivos.

Funcionalidad

- ✓ Controles de acceso para salvaguardar la integridad de la información almacenada.
- ✓ Identificar individualmente a cada usuario y sus actividades en el sistema.
- ✓ Controlar y salvaguardar la información generada.

Consecuencias de no tener seguridad lógica

- ✓ Cambio de los datos antes o después del ingreso a la computadora.
- ✓ Copias de programas y /o información.
- ✓ Código oculto en un programa
- ✓ Entrada de virus
- ✓ Los programas pueden ser modificados.
- ✓ Robo de archivos, datos y programas.
- ✓ Manipulación de información si no es bien transmitida.

Áreas de Seguridad Lógica

Rutas de acceso: Las rutas de acceso son trayectorias las cuales pueden ser seguidas en el momento de acceso al sistema para identificar los puntos de

control de protección de datos en un sistema informático, los tipos de restricciones del sistema son:

- ✓ Solo lectura
- ✓ Solo consulta
- ✓ Lectura y consulta
- ✓ Lectura, escritura para crear, actualizar, borrar, ejecutar o copiar.

Claves de Acceso: Esta es un área importante en la seguridad lógica ya que las claves de acceso de los usuarios es un punto muy delicado. Existen diferentes métodos de identificación para el usuario:

- ✓ Password
- ✓ Código o llaves de acceso

Las claves de acceso pueden ser usadas para controlar el acceso a la computadora, a sus recursos, así como definir el nivel de acceso o funciones específicas, las llaves de acceso deben tener las siguientes características:

- ✓ El sistema debe verificar primero que el usuario tenga una llave de acceso valida.
- ✓ La llave de acceso debe ser de una longitud adecuada para ser un secreto.
- ✓ La llave de acceso no debe ser desplegada cuando es tecleada.
- ✓ Las llaves de acceso deben ser encintadas.

Software de control de acceso: El software de control de acceso debe tener las siguientes funciones:

- ✓ Definición de usuario.
- ✓ Definición de las funciones del usuario después de acceder al sistema.
- ✓ Establecimiento de auditoria a través del uso del sistema.

Tipos de Seguridad Lógica

Dentro de la seguridad lógica se ha creado diversos tipos:

Encriptamiento: Los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. Existen un emisor y un receptor los cuales son conocedores de la clave y la llegada del mensaje que se produce el descifrado. El cifrado de los datos o encriptación fortalece la confiabilidad, y generalmente se utiliza para proteger del robo de identidades, cuentas e banco, etc.

Firmas digitales: Se utiliza para la transmisión de mensajes telemáticos y en la gestión de documentación electrónica. Su finalidad es identificar de forma segura a la persona o al equipo que se hace responsable del mensaje o del documento. Protege la integridad y confidencialidad de información.

Certificados Digitales: Son documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es quien

dice ser, avalada por la verificación de su clave pública. Protege la integridad y la confidencialidad de la información.

Cortafuegos: se trata de uno o más dispositivos de software, de hardware o mixto que permiten, deniegan o restringen el acceso al sistema. Protege la integridad de la información.

Antivirus: Detectan e impiden la entrada de virus y otro software malicioso. En caso de infección tiene la capacidad de eliminarlos y corregir los daños que ocasionan en el sistema. Preventivo, detector y corrector. Protege la integridad de la información.

Control de acceso: Mediante nombre de usuario y contraseña.

Herramientas de Seguridad Lógica

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan crackers que buscan información sobre las vulnerabilidades de un host o de una red completa.

La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema controversial. Expertos

reconocidos como Alec Muffet (autor del adivinador de contraseñas Crack) han recibido enormes críticas por diseñar determinadas herramientas de seguridad para Unix. Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada Security through obscurity, se ha demostrado inservible en múltiples ocasiones. Si como administradores no utilizamos herramientas de seguridad que muestren las debilidades de nuestros sistemas (para corregirlas), tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas); por tanto, hemos de agradecer a los diseñadores de tales programas el esfuerzo que han realizado (y nos han ahorrado) en pro de sistemas más seguros.

Nessus: Es el escáner de vulnerabilidades más popular y es utilizado en más de 75.000 organizaciones en todo el mundo. Muchas organizaciones alrededor del mundo están dando cuenta de los importantes ahorros de costes que estas reciben mediante el uso de Nessus como herramienta de auditoría de sistemas de información para la búsqueda de fallas críticas de seguridad.

Ethereal: Es un analizador de protocolos de red para Unix y Windows, y es libre {free}. Nos permite examinar datos de una red

viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que queramos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Incluye una versión basada en texto llamada tethereal.

Snort: Es un sistema de detección de intrusiones de red de poco peso (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ej. buffer overflows, escaneos indetectables de puertos {"stealth port scans"}, ataques a CGI, pruebas de SMB {"SMB Probes"}, intentos de reconocimientos de sistema operativos {"OS fingerprinting"} y mucho más. Snort utilizar un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular. Mucha gente también sugirió que la Consola de Análisis para Bases de Datos de Intrusiones (Analysis Console for Intrusion Databases, ACID) sea utilizada con Snort.

Necat: Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Está diseñada

para ser una utilidad del tipo "back-end" confiable que pueda ser usada directamente o fácilmente manejada por otros programas y scripts. Al mismo tiempo, es una herramienta rica en características, útil para depurar {debug} y explorar, ya que puede crear casi cualquier tipo de conexión que podamos necesitar y tiene muchas habilidades incluidas.

Hping2: Ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado. También tiene un modo traceroute bastante útil y soporta fragmentación de IP. Esta herramienta es particularmente útil al tratar de utilizar funciones como las de traceroute/ping o analizar de otra manera, hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.

Saint: Security Administrator's Integrated Network Tool (Herramienta de red integrada para el Administrador de Seguridad). Saint es otra herramienta no-libre de evaluación de seguridad (al igual que ISS Internet Scanner o Retina de eEye). A diferencia de esas herramientas basadas exclusivamente en Windows, SAINT corre exclusivamente sobre UNIX. Saint solía ser gratuito y "open source" pero ahora es un producto no-libre.

DSniff: Este popular y bien diseñado set hecho por Dug Song incluye varias herramientas. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y

webspy monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante -- por ej. debido al uso de switches {"layer-2 switches"}. sshmitm y webmitm implementan ataques del tipo monkey-in-the-middle activos hacia sesiones redirigidas de SSH y HTTPS abusando de relaciones {"bindings"} débiles en sistemas con una infraestructura de llaves públicas {PKI} improvisados. Una versión para Windows mantenida por separado también está disponible.

SamSpade: Nos provee de una interfaz de usuario gráfica (GUI) consistente y de una implementación de varias tareas de investigación de red útiles. Fue diseñada con la idea de rastrear spammers en mente, pero puede ser útil para muchas otras tareas de exploración, administración y seguridad. Incluye herramientas como ping, nslookup, whois, dig, traceroute, finger, explorador de web crudo, transferencia de zona de DNS {"DNS zone transer"}, comprobación de "relay" de SMTP, búsqueda en sitios web, y más.

Tripwire: Un comprobador de integridad de archivos y directorios. Tripwire es una herramienta que ayuda a administradores y usuarios de sistemas monitoreando alguna posible modificación en algún set de archivos. Si se usa regularmente en los archivos de sistema (por ej.

diariamente), Tripwire puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo. Una version "Open Source" para Linux está disponible de manera gratuita en Tripwire.Org.

Nikto: Es un software de código abierto (GPL) para escanear vulnerabilidades en los servidores web. Esta herramienta tiene el potencial de detectar más de 3200 archivos potencialmente peligrosos / CGIs, versiones sobre más de 625 servidores, y los problemas específicos de la versión de más de 230 servidores. Los elementos de exploración y plugins pueden ser actualizado automáticamente.

Fragroute: Intercepta, modifica, y reescribe el tráfico de salida, implementando la mayoría de los ataques descriptos en el "IDS Evasion paper" de Secure Networks. Entre sus características, se encuentra un lenguaje de reglas simple para retrasar, duplicar, descartar, fragmentar, superponer, imprimir, reordenar, segmentar, especificar source-routing y otras operaciones más en todos los paquetes salientes destinados a un host en particular, con un mínimo soporte de comportamiento aleatorio o probabilístico. Esta herramienta fue escrita de buena fe para ayudar en el ensayo de sistemas de detección de intrusión, firewalls, y comportamiento básico

de implementaciones de TCP/IP. Al igual que Dsniff y Libdnet, esta excelente herramienta fue escrita por Dug Song.

Nemesis: E l Proyecto Nemesis está diseñado para ser una pila de IP ("IP stack") humana, portable y basada en línea de comandos para UNIX/Linux. El set está separado por protocolos, y debería permitir crear scripts útiles de flujos de paquetes inyectados desde simples scripts de shell. Si Nemesis es de nuestro agrado, quizás queramos mirar hping2. Se complementan mutuamente bastante bien.

GUFW: es un cortafuegos que viene ya pre-instalado en Ubuntu, y creo que también en Debian. Sin embargo, en ambos casos viene deshabilitado por defecto.

Sara: El Asistente de Investigación para el Auditor de Seguridad (Security Auditor's Research Assistant) es una herramienta de análisis de seguridad de tercera generación que está basada en el modelo de SATAN y distribuída bajo una licencia del estilo de la GNU GPL. Promueve un ambiente colaborativo y es actualizada periódicamente para tener en cuenta las últimas amenazas.

Metasploit: El Proyecto Metasploit es un proyecto de seguridad informática que proporciona información sobre las vulnerabilidades, ayuda en las pruebas de penetración y en la ejecución de la explotación de vulnerabilidades de seguridad. Metasploit representa un conjunto de herramientas que ayuda a los profesionales de seguridad y hacker a

llevar a cabo ataques informáticos de manera sistematizada y automatizada.

Nmap: Network Mapper, es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y la versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes o cortafuegos están en uso, y docenas de otras características. Nmap se ejecuta en la mayoría de los ordenadores y la consola y versiones gráficas están disponibles. Nmap es libre y de código abierto.

Hash-Resumen: Es una función para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.

Backtrack: Es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la

seguridad informática. Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu. Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Ophcrack: es una utilidad para recuperar contraseñas de Windows basado en tablas rainbow. Aunque se puede instalar en el mismo sistema operativo del cual se quiere averiguar la contraseña, Ophcrack resulta más eficaz e interesante ejecutándose desde otro sistema operativo, instalado en otra partición o disco duro. Ophcrack es capaz de recuperar el 99% de las contraseñas alfanuméricas en cuestión de segundos.

Wireshark: es un programa analizador de protocolos de red o sniffer, que le permite capturar y navegar de forma interactiva por los contenidos de los paquetes capturados en la red. El objetivo del proyecto fue crear un analizador de calidad comercial para Unix.

Funciona muy bien en Linux y Windows (con una interfaz gráfica de usuario), fácil de utilizar y puede reconstruir flujos TCP / IP y VoIP.

PAM cracklib: Es un mecanismo de autenticación flexible que permite abstraer las aplicaciones y otro software del proceso de identificación.

1.8 Seguridad en Redes Corporativas

La seguridad de redes es parte esencial de las redes informáticas, la seguridad de redes está compuesta por Protocolos, Tecnologías, Dispositivos, herramientas y técnicas que protegen los datos y disminuyan las amenazas. La seguridad ha sido y es una de las prioridades del ser humano moderno. Si a nuestras redes o sistemas informáticos no aplicamos políticas de seguridad podría tener vulnerabilidades que pueden ser explotadas por terceros para tener acceso a información confidencial y de mucha importancia para cualquier organización.

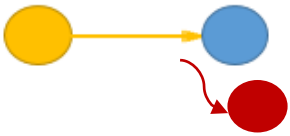
La preocupación de organizaciones o empresas, tanto públicas como privadas, por los inminentes ataques a la seguridad de sus redes corporativas es un escenario de extrema alerta en el cual las redes corporativas de alto impacto requieren de una estructura técnico-operativa de altísimo nivel de especialización en temas de seguridad, por lo que una organización muy bien estructurada permite afrontar los diferentes incidentes.

Amenazas en comunicaciones

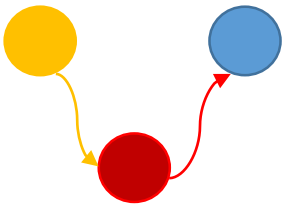
Estas amenazas se dividen en 4 grandes grupos las cuales pueden afectar de forma muy significativa nuestra red corporativa.

Interrupción: Es un servicio del sistema o los datos en una comunicación que puedan sufrir pérdidas y que no estén disponibles o inutilizables.

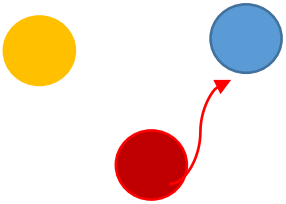
Interceptación: Es un elemento que no ha sido autorizado y que pueda tener un acceso a un determinado objeto.



Modificación: Consiste en tener acceso, modificar el objeto deseado o eliminar dicho objeto.



Fabricación: Es la modificación distinta para conseguir un objeto similar a que ha sido atacado, esta modificación puede ser difícil de distinguir entre el original o el creado.



Ataques

Entre las principales técnicas utilizadas para atacar a las redes corporativas tenemos las siguientes:

Ataque (DDOS): Generalmente, estos ataques se dividen en dos clases:

- ✓ Las denegaciones de servicio por saturación, que comprometen un equipo con solicitudes para que no pueda responder a las solicitudes reales.
- ✓ Las denegaciones de servicio por explotación de vulnerabilidades, que aprovechan una vulnerabilidad en el sistema para volverlo inestable.
- ✓ Este tipo de ataques atenta contra la posibilidad de que los usuarios autorizados tengan acceso a los recursos. Algunos de estos

métodos hacen uso de la fuerza bruta para ocasionar que el sistema se sobrecargue ante tantas peticiones, que no pueda atender a aquellas legítimas y dejar de lado aquellas que provienen de un ataque. (García Pagan, 2007)

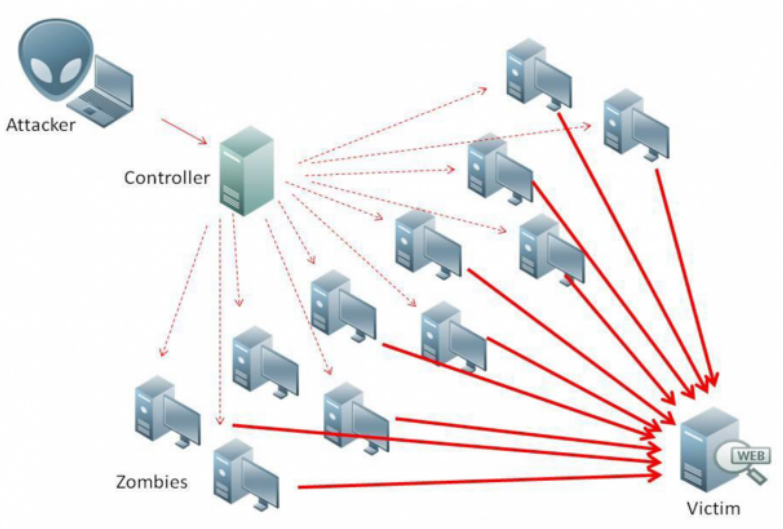


Figura 5. Diseño básico de un ataque DDoS.

Ataque de contraseñas: Una técnica simple usada por los hackers para obtener acceso ilegal a un sistema es conseguir, de cualquier manera, el nombre de usuario y la contraseña de un usuario del sistema; una vez dentro, y con las herramientas necesarias, es posible incrementar el nivel de acceso al sistema o usarlo como puente para un objetivo mucho más atractivo que se encuentre en la red. Un método más elaborado es el ataque de diccionario, el cual consiste en

una lista con miles de posibilidades de password, luego son encriptados con el mismo script usado para encriptar las claves, se comparan, y si se encuentra alguna coincidencia se conoce rápidamente el usuario y la clave, con lo que se obtiene el acceso al sistema. (García Pagan, 2007)

Ataque sniffing: Un sniffer es un programa que captura todo el tráfico que circula desde/a un equipo conectado a una red de ordenadores, hay de todos los tipos y para todos los sistemas operativos. Dependiendo de cuál sea la tipología de su red, un sniffer le permitirá interceptar todo el tráfico que circula por su red, incluido el de otros equipos, o solamente el tráfico que entra y sale de un computador. En las redes Ethernet, en las que los distintos equipos se conectan a un concentrador "HUB" cuando un equipo envía un paquete, éste llega a todos los ordenadores de la misma red. La cabecera del paquete contiene la dirección MAC de la tarjeta de red a la que va dirigido, de manera que sólo el equipo adecuado presta atención al paquete. (Álvarez Marañon & Pérez García, 2004)

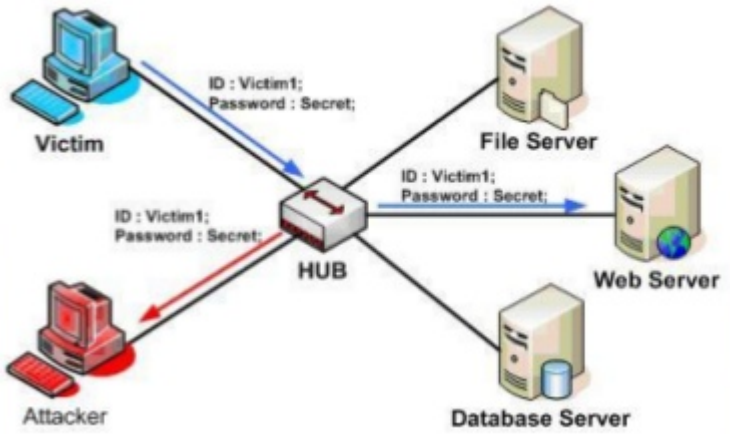


Figura 6. Diseño de Ataque Sniffing (Vverdu, 2012).

Spoofing: En redes de computadoras podemos distinguir dos tipos de ataques: pasivos y activos. En el primero, el atacante se dedica únicamente a escuchar de la red. Ésta es quizá la forma más habitual de penetración: un intruso que haya logrado acceso a un host de nuestra red, podría lanzar un programa sniffer y dedicarse a escuchar los 100 primeros bytes de todas las conexiones dirigidas a los puertos telnet, ftp, pop3, login y demás protocolos que pasen por la red nuestras contraseñas sin encriptar.

Para evitar esto han aparecido mejoras, como por ejemplo las contraseñas de un solo uso (one-time contraseñas), Kerberos, ... en donde el usuario tiene una lista de claves de acceso y usa una cada vez para registrarse en el sistema. De esta forma, si alguien logra ver

nuestra clave de acceso circulando por la red no podrá utilizarla, ya que habrá caducado.

Con esta solución hacemos más robusta la autenticación por medio de contraseñas. Pero ¿qué ocurre si por debajo de ésta se realiza una autenticación por dirección IP ?, es decir, ¿qué ocurre si dependiendo de la dirección IP de nuestro interlocutor actuamos de una forma u otra, pidiendo contraseña o no? Esto puede llegar a ser un problema grave y lo veremos en el siguiente texto.

El spoofing es una técnica que consiste en engañar a un computador haciéndole creer que está dialogando con un host cualquiera, cuando en realidad lo está haciendo con nosotros. Esto puede que no parezca una amenaza, ya que normalmente la autenticación se hace mediante contraseña, por lo que, aunque en nuestra conexión con un servidor suplantemos la identidad de otro host, tendremos que conocer la clave de acceso para hacer uso de un servicio dado.

El problema aparece cuando algunos de nuestros hosts establecen una relación de confianza: entonces, si alguien es capaz de engañarles diciendo que es uno del grupo, esto podría causar estragos en la seguridad de nuestra red. Pero, ¿cómo se plasman esas relaciones de confianza en la realidad?

En UNIX existen un par de archivos que permiten, por medio del comando rlogin, hacer conexiones sin necesidad de entrar ninguna contraseña. Estos archivos son los siguientes:

- ✓ $HOME/.rhosts
- ✓ /etc/host.equiv

Visto esto, el intruso podría optar por intentar adivinar el número de secuencia que va a elegir el servidor. Esto no parece muy difícil si el objetivo usa la regla 64K, pero es casi imposible si su generador de números de secuencia es aleatorio.

Supongamos ahora que el servidor utiliza la regla 64K. Esto se puede saber haciendo varias conexiones consecutivas: si los números de secuencia que recibimos difieren en 64,000 o en 192,000 sin duda estamos en este caso. Es entonces cuando el intruso empieza el ataque. Ahora su software se complica, debe averiguar, mediante la forma que hemos comentado antes, cuál va a ser el número de secuencia que el servidor elegirá.

Recibe los siguientes números de secuencia como respuesta a sus conexiones:

1. 1217261284 2. 1217325284 3. 1217389284 4. 1217581284

Vemos como la diferencia entre 1-2 , 2-3 es de 64,000 y entre 3-4 es de 192,000 por lo que es probable que el siguiente número de

secuencia elegido por el servidor sea 1217581284 + 64000, siempre y cuando el tiempo que tarda el paquete SYN en llegar al servidor sea de menos de un segundo. Así que el intruso prueba este número y envía estos paquetes separados por un pequeño instante de tiempo:

192.168.23.30.1177 > 192.168.23.1.login: S 712432833:712432833(0) win 32120 <mss1460, sackOK, timestamp 395512 0,nop,wscale 0> (DF)

192.168.23.30.1177 > 192.168.23.1.login: . ack 1217645284 win 32120 <nop,nop,timestamp 963931 53591392> (DF)

El primero inicia una conexión y el segundo confirma el número de secuencia elegido por el servidor. ¿Ahora bien, él cómo sabe el atacante si su intento de conexión ha tenido éxito? Simplemente no lo sabe, ya que nunca va a recibir ningún paquete procedente del servidor. El único que los recibirá será el legítimo cliente, el cual habrá sido adormilado mediante un SYN flooding o algo similar que consiga el mismo efecto. Después de esto, al cracker solo le resta enviar la misma información que usaba para emular el protocolo rlogin y esperar a que funcione.

Pero a primera vista puede parecer que algo se nos ha pasado por alto : ¿ qué ocurre con la información que envía el servidor ?. Si el atacante no puede ver ningún mensaje del servidor, acabará perdiendo la pista del número de ACK que debe enviarle para reconocerle que han

llegado sus segmentos TCP. Pero esto no tiene demasiada importancia, ya que cuando el servidor vea que no ha recibido ACK tras un tiempo dado, comenzará a retransmitir. Aunque el tipo de retransmisión depende del algoritmo utilizado, esto es algo que no interfiere con los segmentos del intruso, que serán todos aceptados.

Arp Spoofing: El Protocolo de Resolución de Direcciones (ARP) también puede ser utilizado para un ataque de spoofing. Veamos un ejemplo de cómo podría llevarse a cabo por un intruso: Supongamos que en nuestra LAN tenemos dos computadoras: sirio, un servidor, y algol,un PC Linux usado por satomi. El usuario satomi, también tiene una cuenta con el mismo nombre en sirio, y ha añadido en el archivo .rhosts de éste último la siguiente entrada:

algol satomi

Esto facilitará sus conexiónes por rlogin. Además, como los administradores son un poco paranoicos, para evitar el IP spoofing toda la red está formada por conmutadores y el servidor tiene un generador de números de secuencia aleatorios.

En nuestra LAN también existen otros hosts, y uno de ellos está siendo utilizado por un trabajador descontento para lanzar un ataque sobre sirio. El intruso conoce la existencia en sirio del ½chero .rhosts de satomi, y también conoce las medidas de seguridad que los

administradores han adoptado. Es entonces cuando se le ocurre lanzar un ataque de spoo½ng ARP contra sirio suplantando a algol.

El ataque consiste en enviar a sirio información ARP falsa diciendo que la dirección MAC del host del atacante corresponde con la dirección IP de algol. ¾ Cómo se puede hacer esto? Muchas implementaciones de ARP, cuando escuchan una consulta ARP (recordemos que la consulta es broadcast), fichan esa dirección MAC aunque ellos no sean los buscados. Lo que podría hacer el intruso sería enviar una consulta ARP buscando a un host inexistente y, dentro del paquete ARP, cambiar su dirección MAC por la dirección MAC dealgol. Tan solo tiene que hacerlo dentro del paquete y no en la cabecera MAC porque lo que recibe el software ARP de sirio es la consulta libre de la cabecera MAC, que fue eliminada por la capa de nivel de enlace.

Una vez hecha la consulta, sirio incorporará en su cache ARP esta información, y cuando se quiera comunicar con algol sus paquetes irán dirigidos a la dirección IP de algol pero a la dirección MAC del intruso, y éste se podría aprovechar la relación de con½anza que existe entre el sirio y algol.

Una forma de frustrar este ataque es establecer asignaciones estáticas de direcciones hardware, pero si se inventó ARP fue precisamente para evitar esto. En redes pequeñas quizá pueda llevarse a cabo, pero

cuando una LAN es demasiado grande esto puede requerir mucho tiempo y esfuerzo.

Otra solución menos incomoda sería el ARPWATCH, un programa que vigila los cambios en la cache ARP y nos informa a través del correo electrónico y ½cheros de log de posibles variaciones.

DNS Spoofing: Este es quizá el menos habitual de los ataques de spoofing, pero conviene conocerlo. El ½n del intruso es engañar a un host con una correspondencia 'nombre del host-dirección IP' falsa. Esto se puede conseguir de tres formas:

1. Falsificando una respuesta del DNS al host que se quiere atacar, de tal forma que la información alterada quede en su cache.
2. Modificando una transferencia de zona de un servidor de nombres primario a uno secundario.
3. Logrando acceso al DNS primario y modificando su base de datos para que una consulta posterior por parte del host a atacar le devuelva información falsa.

Siguiendo con el ejemplo anterior, supongamos ahora que los administradores de sirio han detectado ataques ARP spoofing con la ayuda del ARPWATCH y deciden hacer permanente la cache ARP solamente en este servidor. El intruso se da cuenta de esto y, conociendo una vulnerabilidad del DNS, logra acceso a él. Entonces

modifica la entrada de algol cambiando la dirección IP que había por la suya.

Cuando sirio reciba una conexión del intruso como usuario satomi, mirará el archivo .rhosts de satomi y vera que si la conexión se hace desde algol no requerirá passsword. Hace una consulta al DNS para conocer la dirección IP de algol y el servidor de nombres le responde con la IP del intruso. sirio comprueba el origen de la conexión rlogin y ve que coincide con la IP devuelta por el DNS, por lo que acepta su conexión y no le pide ningún tipo de contraseña.

Este ataque también se podría haber llevado a cabo sin haber conseguido acceso al servidor de nombres, simplemente falsificando la respuesta del DNS ante la consulta que hace sirio o modificando una transferencia de zona de un primario a un secundario en el caso de que la consulta de sirio fuese al secundario.

Si el DNS tiene contacto directo con la red externa, para evitar que un intruso pueda explotar un fallo en su implementación o en su configuración podríamos aislarlo de la red. Podemos conseguir este aislamiento utilizando dos servidores de nombres y un cortafuego. El cortafuego se situaría entre nuestra red y la red exterior, y colocaríamos un DNS al frente del cortafuego y otro detrás. El de detrás del cortafuego almacenaría todos los nombres y direcciones IP de nuestra red, y sería el encargado de responder consultas a hosts

internos. El que se encuentra al frente estaría vacío de información y se dedicaría a responder consultas de hosts externos preguntando al DNS interno. Así, nuestro cortafuego filtraría las conexiones externas al servidor de nombres interno y tan solo permitiría consultas de fuera que viniesen del DNS al frente, evitando cualquier intento de irrumpir en el servidor de nombres que contiene toda la información de nuestra red.

Si además configuramos nuestro router de entrada para que no deje pasar paquetes de fuera con una dirección origen perteneciente a nuestra red, evitaremos cualquier intento de spoo½ng sobre el DNS interno suplantando al externo.

Ataque de fuerza bruta : La semilla de 32 bits que utiliza el PRNG es obtenida a partir de la passphrase. La passphrase normalmente contiene caracteres ASCII, por lo cual el bit más alto de cada carácter siempre es cero. El resultado de la operación XOR de estos bits también es cero y esto provoca una reducción de la entropía de la fuente, es decir, las semillas sólo podrán ir desde 00:00:00:00 hasta 7F:7F:7F:7F en lugar de hasta FF:FF:FF:FF.

El uso del PRNG con esta semilla también reduce la entropía. De la semilla de 32 bits sólo utiliza n los bits del 16 al 23. El generador es un generador lineal congruente (LGC: linear congruential generator) de módulo 2^32, esto provoca que los bits más bajos sean “menos

aleatorios" que los altos, es decir, el bit 0 tiene una longitud de ciclo de 2^1, el bit 1 de 2^2, el bit 2 de 2^3, etc. La longitud de ciclo del resultado será por tanto 2^24. Con esta longitud de ciclo sólo las semillas que vayan de 00:00:00:00 a 00:FF:FF:FF producirán llaves únicas.

Como las semillas sólo llegan hasta 7F:7F:7F:7F y la última semilla que tiene en cuenta el PRNG es 00:FF:FF:FF, sólo se debe considerar las semillas desde 00:00:00:00 hasta 00:7F:7F:7F por lo que la entropía total queda reducida a 21 bits.

El conocimiento de estos datos nos permite hacer ataques de fuerza bruta contra la encriptación WEP generando llaves de forma secuencial utilizando las semillas desde

00:00:00:00 hasta 00:7F:7F:7F. Utilizando este proceso, un procesador PIII a 500MHZ tardaría aproximadamente 210 días en encontrar la llave, aunque se puede usar computación en paralelo para obtener la llave en un tiempo más razonable.

También existe la posibilidad de utilizar un diccionario para generar sólo las semillas de las palabras (o frases) que aparezcan en el diccionario, con lo que si la passphrase utilizada está en el diccionario conseguiríamos reducir sustancialmente el tiempo necesario para encontrarla.

Descubrir essid ocultados: Como hemos comentado anteriormente, para que un cliente y un AP se puedan comunicar, ambos deben tener configurado el mismo ESSID, es decir, deben pertenecer a la misma red wireless.

Una medida de seguridad bastante común es "ocultar" el ESID, es decir, hacer que el AP no mande BEACON FRAMES, o en su defecto no incluya el ESSID en éstos.

En este caso, para descubrir el ESSID deberíamos esnifar y esperar a que un cliente se conectara, y veríamos el ESSID en la trama PROVE REQUEST del cliente (en el caso de que no se manden BEACON FRAMES), o en la trama PROVE RESPONSE del AP. Pero también podemos "provocar" la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de desasociación o de desautenticación en lugar de mandarlas repetidamente, es decir, nos ponemos la dirección física del AP y mandamos una trama DEAUTH o DISASSOC a la dirección MAC del cliente (o a la de broadcast), entonces el cliente intentará volver a asociarse o autenticarse, con lo que podremos ver el ESSID en los *management frames*.

Para implementar el ataque podemos usar la herramienta essid-jack, que también pertenece al paquete de utilidades air-jack para Linux (http://802.11ninja.net).

Ataque Man In the Middle: El ataque de *Man in the middle*, también conocido como *Monkey in the middle* consiste en convencer al cliente (la víctima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente.

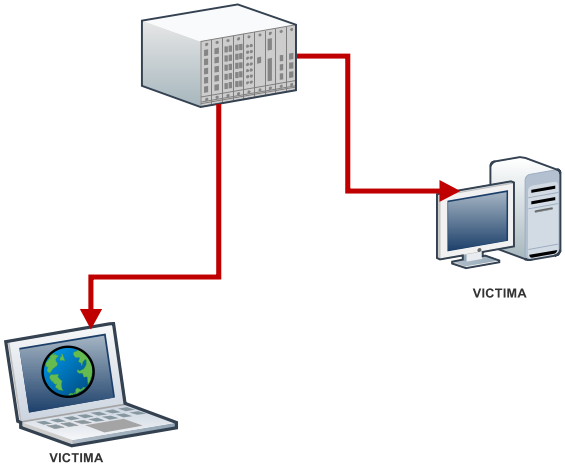


Figura 7. WLAN antes del ataque

Para realizar este ataque, primero debemos esnifar para obtener:

- ✓ El ESSID de la red (si esta ocultado, usaremos el método anterior)
- ✓ La dirección MAC del AP
- ✓ La dirección MAC de la víctima

Una vez conocemos estos datos, utilizamos el mismo método que en el ataque DoS, para desautenticar a la víctima del AP real, es decir, el

atacante spoofea su MAC haciéndose pasar por el AP y manda tramas DEAUTH a la víctima. La tarjeta wi-fi de la víctima empezará entonces a escanear canales en busca de un AP para poderse autenticar, y ahí es donde entra en juego el atacante. El atacante hace creer a la víctima que él es el AP real, utilizando la misma MAC y el mismo ESSID que el AP al que la víctima estaba autenticada anteriormente, pero operando por un canal distinto. Para realizar esto la tarjeta wi-fi del atacante debe estar en modo master. Por otra parte, el atacante debe asociarse con el AP real, utilizando la dirección MAC de la víctima. De esta manera hemos conseguido insertar al atacante entre la víctima y el AP, veamos cómo quedaría la WLAN después de realizar el ataque.

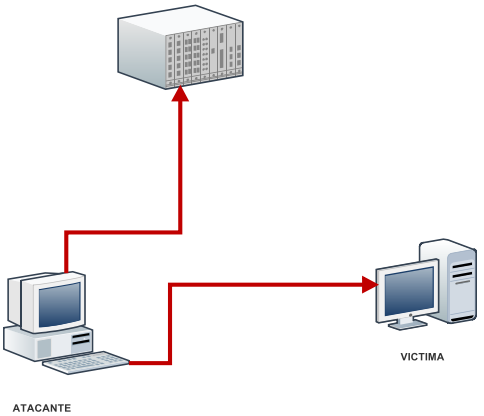


Figura 8. WLAN despés del ataque

De esta manera todos los datos que viajan entre la víctima y el AP pasan a través del atacante. Como el ataque ha sido realizado a nivel de enlace (nivel 2), el atacante puede ver, capturar e incluso modificar las tramas en los niveles superiores del modelo OSI. Es muy fácil implementar este tipo de ataques utilizando el driver air-jack con la herramienta monkey-jack.

Hay que tener en cuenta que muchas soluciones de seguridad están pensadas asumiendo que las capas 1 y 2 son seguras, esto como hemos visto es incierto para las redes wireless y por tanto el uso de según qué tipo de solución podría no ser adecuado para estas redes. Hay que ir con mucho cuidado sobre todo en implementaciones de VPN que no realizan las comprobaciones necesarias de autenticación para protegerse de ataques *Man in the middle* en redes wireless.

VPN (Virtual Private Network): Una red privada virtual es la interconexión de varias redes locales que están separadas físicamente y que realizan una transmisión de datos entre ellas de un volumen considerable. De forma habitual, lo que se pretende es que dicho grupo de redes locales se comporten como si se trataran de una única red local, aunque por diversos motivos, fundamentalmente de índole económica, la interconexión entre dichas redes LAN se efectúa a través de medios potencialmente hostiles o inseguros (Internet, Red telefónica conmutada o RTC a través de módem, Líneas alquiladas,

RDSI o ISDN, X.25, Frame Relay, ATM,...), de forma que hay que articular diversos mecanismos, especialmente de encriptación y de firma digital, para garantizar la seguridad de los sistemas.

Certificación: Cada uno de los gateways que pretendan unirse a la VPN debe garantizar de alguna forma que está autorizado. Esto se hace a través de algún mecanismo de firma digital, normalmente a través de una autoridad de certificación (Certification Authority). Esta certificación suele ser doble, e incluye un elemento electrónico y un número de identificación personal o PIN (Personal Identification Number). De esta manera, el usuario debe poseer de alguna forma un código electrónico, bien sea una tarjeta magnética o un archivo en un ordenador, y memorizar otra parte del código. Esto reduce drásticamente el problema de que alguien pueda falsear una identidad para entrar al sistema, puesto que debe poseer ambos elementos.

Encriptación: Una vez dentro de la VPN, cada uno de los gateways envían su clave pública a todos los demás gateways pertenecientes al sistema. Con el uso de sistemas de encriptación simétricos, de clave pública y clave privada, la información se encripta matemáticamente de tal forma que es extremadamente complejo desencriptar la información sin poseer las claves. Existe un proceso de gestión de dichas claves (Key management) que se encarga de su distribución, su refresco cada cierto tiempo, y revocarlas cuando sea necesario hacerlo.

Se ha de conseguir un balance entre los intervalos de intercambio de las claves y la cantidad de información que se transfiere: Un intervalo demasiado corto sobrecargaría los servidores de la VPN con la generación de claves, mientras que uno excesivamente largo podría comprometer la clave y la información que esta protege.

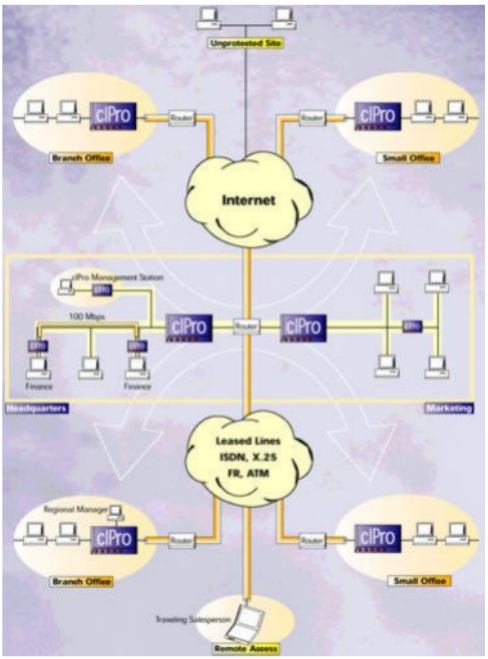


Figura 9. Esquema habitual de una VPN

Consejos para garantizar la seguridad de la red corporativa: Entre los principales tenemos los siguientes.

- ✓ Los dispositivos deben actualizarse constantemente.

- ✓ Con la criptografía y las contraseñas de acceso, toda la información será leída apenas por el interesado.
- ✓ Los profesionales de TI deben estar atentos cuando se trata de seguridad y de la infraestructura contratada.

2 RIESGOS

En el mundo empresarial todas las actividades de administración giran en torno al procesamiento de diferentes datos sobre infraestructuras y sistemas que son utilizados todo el tiempo, en las organizaciones la información que se maneja es vital para el funcionamiento de la misma, por ello si se perdieran datos o si personas malintencionadas tuvieran acceso a ellos sería una catástrofe para dicha institución, entonces se debe proteger este recurso aplicando opciones de seguridad a las TICS.

No podemos tratar de solucionar un problema si no tenemos un punto de partida, como aplicamos medidas de seguridad sin antes medir el nivel de protección que tenemos, para ello nace la auditoria informática donde su objetivo general es "evaluar e informar sobre la eficiencia y la eficacia son los controles para salvaguardar los recursos, es decir, los sistemas críticos, aplicaciones, datos e infraestructura dentro de las políticas, procedimientos, leyes y reglamentos aplicables. La auditoría se realiza para recoger y evaluar la evidencia de que el Sistema Informático están funcionando de una manera eficiente y eficaz para alcanzar el objetivo (s) de la organización " (4100, EEUU)

La auditoría de sistemas de información ayuda en los riesgos y por lo tanto mejora el sistema de seguridad de la organización mediante la

evaluación de los procesos y controles de los sistemas de una organización en contra de un proceso estándar o documentado que se establece anteriormente. (INTECO, 2014) las organizaciones deben abordar cuatro tipos principales de riesgos de TIC y son los riesgos de seguridad, riesgos de disponibilidad, los riesgos de desempeño y los riesgos de cumplimiento. (SYMANTEC, 2016)

El crecimiento en la cantidad de incidentes puede deberse a múltiples factores, entre ellos: tendencias mundiales de ataques y fraudes cibernéticos; a la implementación de nuevos sistemas de detección y al aumento de confianza en CERTuy por parte de los actores de la comunidad objetivo.(AGESIC, 2017). En la Figura 10 se presentan resultado de un estudio sobre incidentes informáticos durante el año 2016.

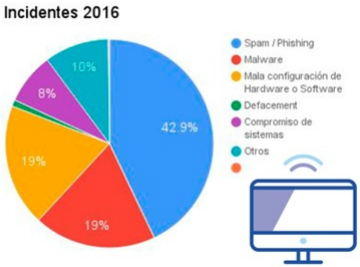


Figura 10. Estadísticas de incidentes informáticos.
Fuente: (AGESIC, 2017)

2.1 Conceptos generales

Sistema Informático: Está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos, y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos) y con una frecuencia se incluyen también los elementos humanos (personal experto que maneja el software y hardware).(Muñoz Razo, 2012)

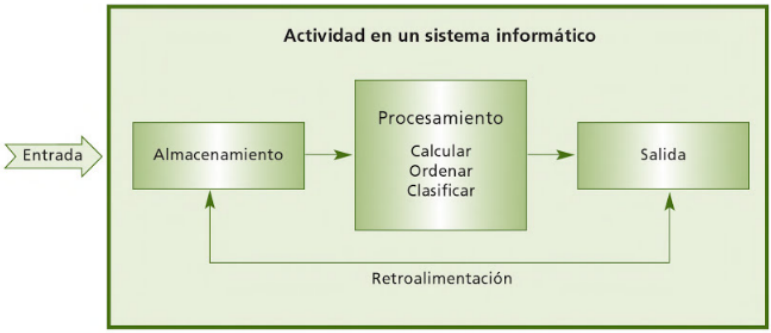


Figura 11. Proceso básico de un sistema informático

Auditoría de Sistemas: es la revisión y evaluación de los controles, sistemas y procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información, de los equipos, del recurso humano, se mejoren los procesos y se logre de manera integrada una

organización ágil, dinámica, controlada y segura.(Echenique García, 2012). Los objetivos de la auditoría de sistemas son los siguientes:

- ✓ Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.
- ✓ Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.
- ✓ Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.
- ✓ Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.
- ✓ Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.

- ✓ Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoria y de la paquetería que sirve de soporte para el desarrollo de auditorías por medio del computador. (Muñoz Razo, 2012)

2.2 Riesgos de TI

La administración de riesgos es un término aplicado a métodos tanto lógicos como sistemáticos que permitirán identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades", (AS/NZS 4360:1999, 1999), con el objetivo de poder controlar y mitigar los riesgos. (Medina-García, 2016)

Para ello es importante que se conozca que la mayoría de riesgos a los que nos vemos afectados hoy en día tienen mucho que ver a riesgos tecnológicos y las organizaciones deben estar preparadas con el único fin de mejorar los procesos organizacionales. Siendo de vital importancia seguir un marco de referencia como el Risk IT, que provee una serie de requisitos que son aplicables a cualquier tipo de organización. El universo de riesgos de TI destaca la necesidad de contar con una estrategia alineada para manejar las 10 amplias categorías de riesgos.(Mazzinghi, 2011)

No es necesario que cuenten con un amplio conocimiento sobre TI para poder identificar estas preguntas importantes y reveladoras. Únicamente necesitan tener dos cosas en claro:

- ✓ Qué tanto depende su compañía de sistemas de TI rentables, ininterrumpidos y seguros (TI defensiva)
- ✓ Qué tanto depende esta de lograr una ventaja competitiva a través de las TI (TI ofensiva) o de ambas.

Figura 12. Categorías de riesgos informáticos.

Fuente: (Medina-García, 2016)

2.3 Análisis de riesgos

Definición

El Análisis y Gestión de Riesgos son procedimientos formales para encontrar los riesgos que existen en un Sistema de Información y mediante un estudio responsable, recomienda medidas apropiadas que deberían acogerse para controlarlos.(Echenique García, 2012). El Análisis de Riesgos busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.(Piattini & Del Peso, 2011). Aun así, existe un acuerdo sobre las características comunes que debe tener todo riesgo informático:

Incertidumbre: el evento que caracteriza al riesgo puede ocurrir o no ocurrir, no hay certeza sobre su ocurrencia.

Pérdida: en caso de materializarse el riesgo, habría varias consecuencias negativas para la organización. Si no hay efectos negativos, no hay riesgo en sí.

Objetivo del Análisis de riesgos

El análisis de una serie de elementos importantes del sistema de información: los elementos más vulnerables ante posibles amenazas y aquellos cuyo deterioro pueda suponer un daño mayor en el sistema.

A continuación, se describen los principales elementos del análisis a tener en cuenta en el proceso de gestión de riesgos.

Activo: es un recurso del sistema de información, necesario para garantizar el correcto funcionamiento de los procesos de la organización. Los activos también son fundamentales para lograr los objetivos definidos por la organización y requieren de una especial protección: cualquier amenaza que pueda afectar a un activo puede poner en peligro la actividad de la organización y su servicio al cliente.

Amenaza: es cualquier evento que puede afectar al activo de un sistema de información, provocando un incidente de seguridad y produciendo efectos adversos (materiales o inmateriales) o pérdidas de información. Las amenazas afectan directamente a las propiedades de la información: integridad, disponibilidad, confidencialidad y autenticidad.

Vulnerabilidad: consiste en alguna característica o capacidad de un activo del sistema de información que lo hace susceptible a amenazas. También se define como la capacidad de actuación o reacción de un sistema de información ante la aparición de amenazas, además de la capacidad de recuperación de los daños ocasionados.

Riesgo: Como se ha mencionado anteriormente, un riesgo es la posibilidad de que una amenaza se materialice causando efectos negativos o positivos.

Control atenuante: aquellos activos y medidas que consiguen reducir las posibilidades de amenazas y, por tanto, el nivel de riesgo del sistema de información de la organización.

Impacto: es la magnitud del daño que provoca un ataque exitoso en el que se han perjudicado la confidencialidad, la disponibilidad, la integridad y la autenticidad de la información del sistema. Dependiendo de los daños causados y los activos afectados, el impacto será mayor o menor: es posible que una amenaza comprometa a un activo prescindible del sistema (causando un impacto bajo) o que, sin embargo, comprometa a un activo importante, ocasionando efectos graves en el correcto funcionamiento de una organización (causando un impacto muy elevado).(Abogacía Española - Incibe, 2016)

Probabilidad: se define como la estimación de posibilidades de que se materialice el riesgo o, lo que es lo mismo, que se produzca una amenaza real.

Fases del análisis de riesgos

El proceso de análisis y gestión de riesgos está formado por una serie de fases.(CCN-CERT-Libro I, 2012)

Identificación de los activos: El activo más importante que maneja una organización es, sin duda, la información. No obstante, no hay que

olvidar otros activos que también pueden ser relevantes, como, por ejemplo:

- ✓ Los servicios prestados con la utilización de dicha información.
- ✓ Los servicios necesarios para poder utilizar y tratar la información.
- ✓ Los equipos y soportes de información que permiten almacenar la información: ordenadores, dispositivos de almacenamiento externos, etc.
- ✓ Los equipos informáticos que permiten la gestión de la información.
- ✓ Las aplicaciones que permiten gestionar la información y los servicios que se proporcionan a través de esta.
- ✓ Las redes de comunicaciones que permiten y facilitan el intercambio de información.
- ✓ Las instalaciones en las que se ubican y protegen los equipos informáticos, dispositivos, sistemas de almacenamiento y redes de comunicaciones necesarios para gestionar la información y ofrecer el servicio.
- ✓ Los recursos humanos que utilizan todos los elementos anteriores.

Valoración de los activos: viene definida como el coste que implicaría recuperarse de un fallo del activo provocado por alguna incidencia. La valoración de un activo, del mismo modo que la metodología de gestión de riesgos, puede realizarse de dos modos:

Valoración cuantitativa: se calcula el valor del activo utilizando cantidades numéricas, valores exactos.

Valoración cualitativa: se asigna el valor a los activos, utilizando una escala de niveles. Por ejemplo: puede utilizarse una escala tipo "valor nulo, valor bajo, valor medio, valor alto, valor muy alto" para clasificar los distintos activos en cada uno de los niveles de valoración. Esta valoración depende de muchos factores que variarán, por supuesto, según la organización y el sistema de información implantado. Los factores más importantes a considerar son:

- ✓ Coste del personal especializado necesario para recuperar el activo (coste de mano de obra).
- ✓ Los ingresos perdidos por el fallo del activo.
- ✓ Coste de adquisición e instalación de un activo nuevo en caso de que el anterior haya resultado inservible (coste de reposición).
- ✓ Pérdida de percepción de confianza y calidad de los clientes y proveedores provocados por una interrupción del servicio provocada por el fallo del activo.
- ✓ Infracciones cometidas y sanciones correspondientes al incumplimiento de requerimientos legales o de obligaciones contractuales debidas al fallo del activo.
- ✓ Daños y efectos perjudiciales provocados por el activo a otros activos, tanto propios como ajenos a la organización.

- ✓ Daños medioambientales causados por el activo.
- ✓ Daños a otras personas causados por el activo.

Identificación de las amenazas: hay que tener en cuenta que pueden ser accidentales o, por el contrario, provocadas deliberadamente. Como ejemplos de amenazas accidentales se pueden citar amenazas naturales (terremotos, inundaciones, etc.), amenazas industriales (fallos eléctricos, fallos de comunicación, etc.) o amenazas humanas (errores provocados sin deliberación previa u omisiones de acciones que son importantes para el funcionamiento del sistema). Por otro lado, las amenazas deliberadas se realizan con intencionalidad y la mayoría son penalizadas por las leyes. Algunos ejemplos son la intrusión, el espionaje, el robo de información, el fraude, etc.

Determinación del impacto de una amenaza: Cuando se produce una amenaza, los efectos sobre los activos no son igual de perjudiciales para todas sus dimensiones, pudiendo, por ejemplo, afectar gravemente a la integridad de la información, pero no tener efectos sobre su confidencialidad.

- ✓ Su valoración se calculará tomando como referencia los siguientes elementos:
- ✓ Daños producidos en los activos de la organización.
- ✓ Capacidad de reproducción y expansión de la amenaza a otros activos del sistema.

- ✓ Capacidad de explotación de la amenaza.
- ✓ Usuarios que se pueden ver afectados en caso de producirse la amenaza.
- ✓ Capacidad de detección y descubrimiento de la amenaza cuando esta se produzca.

Determinación del Riesgo: Un documento formalizado que contiene los objetivos de la auditoría, las metodologías utilizadas, los resultados obtenidos y las conclusiones y recomendaciones aportadas por los auditores. El informe tiene que ser claro, conciso, oportuno, objetivo e imparcial y debe ser elaborado por auditores independientes. En cuanto a la gestión de riesgos, el informe de auditoría deberá contener también los activos de la organización y su valoración, junto con las vulnerabilidades, amenazas y riesgos detectados en el sistema de información detectado. Además, deberán formularse recomendaciones de políticas y medidas correctivas que permitan la reducción del riesgo y de posibles vulnerabilidades, además de proponer salvaguardas que reduzcan la incidencia de vulnerabilidades.

Establecimiento de salvaguardas: Las medidas de salvaguarda o de seguridad son medidas cuya función fundamental es reducir o eliminar un riesgo de dos formas:

- ✓ La reducción de la probabilidad de materialización de las amenazas: son también salvaguardas preventivas. La salvaguarda

ideal sería aquella que impidiese completamente que se materializara cualquier tipo de amenaza.

- ✓ La reducción del impacto de las amenazas sobre la organización: hay salvaguardas que limitan o reducen la degradación del activo ante la presencia de alguna amenaza, impidiendo que el daño ocasionado se expanda. En otras ocasiones, ciertas amenazas también pueden llegar a restaurar el sistema cuando alguna amenaza lo ha puesto en peligro o ha dañado alguno de sus activos. Para que estas salvaguardas actúen, debe haberse materializado la incidencia o amenaza y, en cualquier caso, la salvaguarda limita los efectos nocivos y su expansión sobre los activos que forman parte del sistema dañado.

Estas medidas de salvaguarda se clasifican en varios tipos, atendiendo a criterios diferentes. La primera de las clasificaciones es atendiendo al momento de actuación de la salvaguarda, distinguiendo:

- ✓ Salvaguardas activas: aquellas que reducen o eliminan el riesgo de una amenaza.
- ✓ Salvaguardas pasivas: aquellas que reducen el impacto sobre la organización, una vez ya se ha producido el incidente de seguridad.
- ✓ Por otra parte, otra clasificación de las salvaguardas hace referencia a su composición y al tipo de protección que ofrecen

- ✓ Salvaguardas físicas: aquellas que protegen el acceso físico a los activos y las condiciones ambientales en las que estos se utilizan.
- ✓ Salvaguardas lógicas: se encargan de proteger los activos a través de herramientas, técnicas y programas informáticos.

Revisión del impacto y determinación del impacto residual: El impacto residual, al contrario que el impacto potencial, tiene en cuenta la actuación de las salvaguardas sobre el riesgo del sistema de información. Se define el impacto residual como los daños a los que se expone el sistema de información cuando este está protegido por las salvaguardas implantadas.

De este modo, para su estimación se añade un elemento más al cálculo, siendo sus elementos principales:

- ✓ La identificación y valoración de los activos.
- ✓ La identificación y valoración de las amenazas.
- ✓ La identificación y valoración de las salvaguardas.

Revisión del riesgo y determinación del riesgo residual: Cuando ya se han categorizado los pares activos/amenaza y establecidos los distintos niveles de impacto y probabilidad de una amenaza, el siguiente paso es la estimación del riesgo. Los datos de entrada que se deberán utilizar para la estimación del riesgo serán los siguientes:

- ✓ Identificación y valoración de los activos.

- ✓ Identificación y valoración de las amenazas.
- ✓ Identificación y valoración de las salvaguardas.
- ✓ Impacto estimado con los pares activo/amenaza identificados.

Del mismo modo que con los impactos, la estimación del riesgo puede ser de riesgo residual o de riesgo potencial:

- ✓ El riesgo potencial será el riesgo al que está sometido el sistema de información sin contar con las salvaguardas establecidas. Solo se tienen en cuenta los activos, las amenazas y el impacto potencial.
- ✓ El riesgo residual, por el contrario, se estimará tomando como factores de cálculo las salvaguardas establecidas en el sistema y el impacto residual, además de los activos y las amenazas.

2.4 Gestión de riesgos

La gestión de riesgos se define como el conjunto de procesos desarrollados por una organización con el fin de disminuir la probabilidad y ocurrencia de amenazas y de aumentar la probabilidad y ocurrencia de oportunidades con efectos negativos. Se trata de una metodología o conjunto de metodologías encaminadas a gestionar correctamente las incertidumbres de una amenaza. (CCN-CERT-Libro II, 2012)

En el ámbito de la gestión de riesgos, entra en juego el concepto de seguridad de la información: la seguridad se define como el conjunto de medidas y capacidades de los sistemas de información para resistir a las amenazas manteniendo la disponibilidad, autenticidad, integridad y confidencialidad de los datos.

Fases de la Gestión de Riesgos

La norma ISO 31000 establece, después de introducir los principios de gestión del riesgo y el marco de trabajo, un proceso de gestión del riesgo con un conjunto de fases y pasos recomendados para que las organizaciones lo adapten e implanten correctamente, consiguiendo mejoras en la efectividad y precisión ante posibles amenazas.(Cuenca, Javier, & Villalba, 2011)

El proceso de gestión de riesgos definido por la norma ISO 31000 propone una serie de fases o procesos como se detalla en la Figura 13.

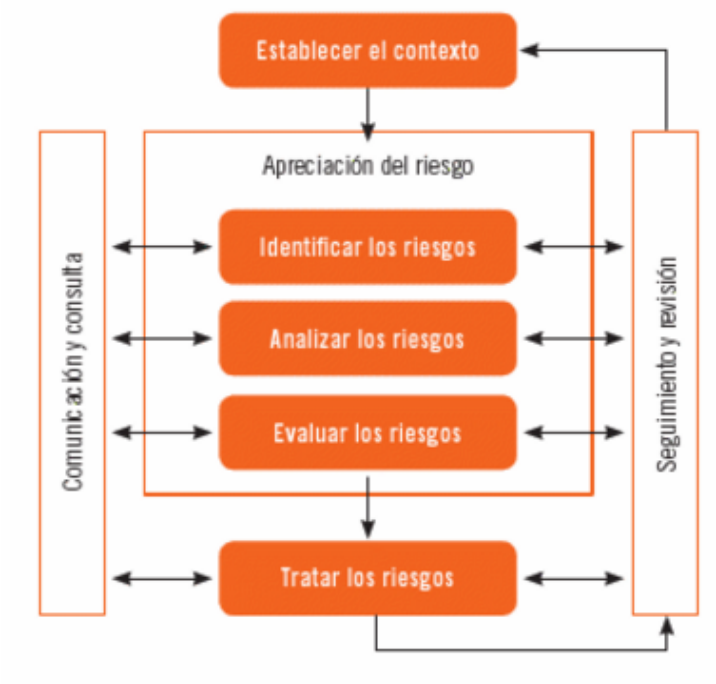


Figura 13. Fases del proceso de gestión de riesgos

Establecimiento del entorno y del contexto: en un primer momento, deberán analizarse todas las peculiaridades de la organización, del entorno y de sus sistemas de información para desarrollar una estrategia de gestión de riesgos que se adapte a sus necesidades.

Fase de apreciación del riesgo: consiste en una serie de tareas relacionadas con la detección e identificación de los riesgos de una

organización para su evaluación y categorización. Dentro de esta fase, se encuentran las subfases siguientes:

- ✓ Identificación del riesgo: una vez detectado el riesgo, habrá que proceder a identificarlo para conocer sus características básicas.
- ✓ Análisis del riesgo: cuando ya se ha identificado el riesgo, será necesario realizar un análisis más profundo y detallado para conocer sus características y comportamientos particulares.
- ✓ Evaluación del riesgo: después de conocer en profundidad el riesgo identificado, se tendrán que evaluar los potenciales daños y efectos negativos que puede ocasionar para determinar su importancia y magnitud.

Fase de tratamiento del riesgo: según lo determinado en el análisis y evaluación del riesgo, se tomarán una serie de decisiones y medidas que minimicen la probabilidad de su ocurrencia y su daño potencial.

Monitorización y revisión: cuando ya se ha decidido e implantado la metodología de detección, análisis, evaluación y tratamiento de riesgos, habrá que monitorizarla lo máximo posible para que se integre en la organización como un proceso automático. Además, requerirá revisiones periódicas para detectar posibles fallos y solucionarlos en el menor tiempo posible. Durante la implantación, también se recomienda ir realizando revisiones que garanticen su desarrollo correcto.

Comunicación y consulta: durante todas las fases de gestión del riesgo, la organización deberá estar en permanente contacto con los distintos agentes y participantes de su sistema de información con una serie de objetivos: (Chicano Tejada, 2017)

- ✓ Ayudar a establecer el contexto adecuadamente.
- ✓ Garantizar los intereses de las partes interesadas y asegurarse que están bien informadas.
- ✓ Ayudar a asegurar que los riesgos están identificados correctamente.
- ✓ Dar apoyo al sistema de gestión de riesgos.
- ✓ Desarrollar una correcta política de comunicación interna y externa de la organización, para que todos los agentes tengan la posibilidad de consultar los riesgos del sistema de información y sus consecuencias.

2.5 Política de Administración de Riesgos

A fin de que se cumpla de manera eficaz la administración de riesgos y de que se cumplan los objetivos de la organización es indispensable que el responsable de área de TI, desarrolle una política organizacional de administración de riesgos cuyo único objetivo sea llevar una estructura organizada ya que esta se convertirá en una meta estratégica para su organización, asegurándose que sea legalizada, socializada por

parte de los directivos y comprendida, implementada por parte del personal.(Abogacía Española - Incibe, 2016)

2.6 Software de Auditoría

Auditoria basada en riesgos: es un proceso, un acercamiento, una metodología y una actitud en torno al tema. La manera más simple de definir una auditoría basada en riesgos consiste en revisar las cosas que realmente importan en su organización. (Piattini & Del Peso, 2011).

Software de auditoria basada en riesgos: Esta técnica tiene como objetivo desarrollar programas informáticos cuyo objetivo es controlar la fiabilidad de las aplicaciones auditadas.

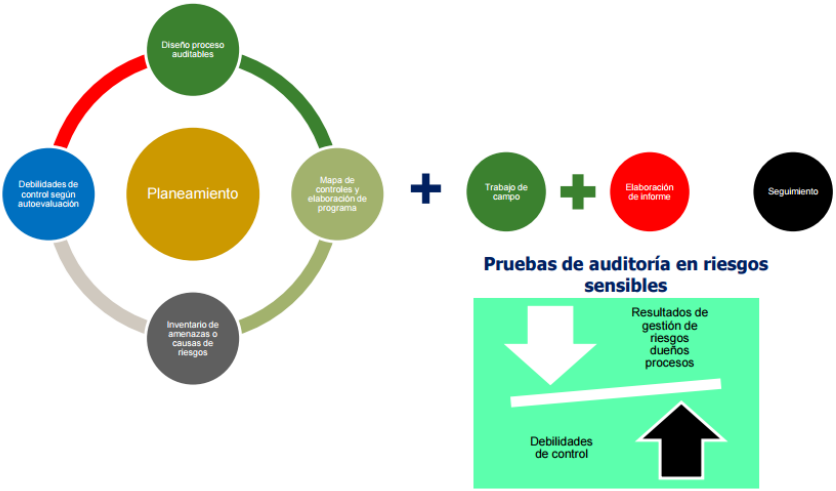


Figura 14. Fases del software de auditoría

2.7 Ejemplos de Software para la auditoria

Audirisk

Auditoría Basada en Riesgos para procesos y sistemas de información, es un software en tecnología Web (Cloud Computing) diseñado "por auditores para auditores", para conducir las siguientes actividades de las auditorías internas y externas, de conformidad con las normas y procedimientos de auditoría generalmente aceptados, con las normas de auditoría interna promulgadas por el Instituto de Auditores Internos (IIA) y las normas de auditoría de sistemas emitidas por la Asociación de Control y Auditoría de Sistemas (ISACA):

- ✓ Planeación Anual de la Auditoría Basada en "Valoración de la Exposición a Riesgos
- ✓ Desarrollo de auditorías a procesos y sistemas de información, "Basadas en Riesgos Críticos".
- ✓ Gestionar los Resultados de la Auditoría

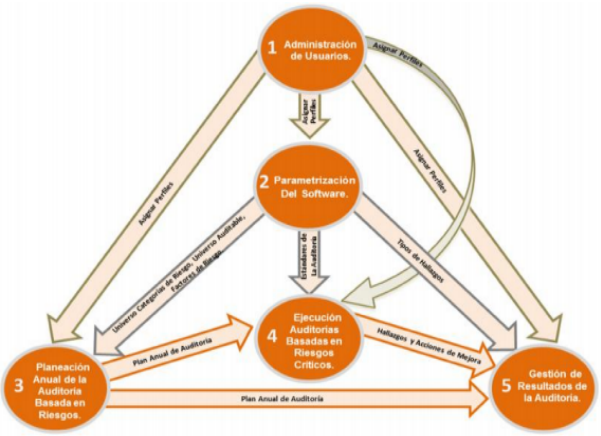


Figura 15. Proceso de auditoría con Audirisk

Mkinsight

Introduce las metodologías más flexibles de cualquier sistema de gestión de auditoría. Las mismas permiten a los equipos de auditoría llevar adelante una planificación anual basada en riesgo utilizando la metodología de evaluación de riesgo que prefieren.

Otra característica de la Planificación Anual de MKinsight consiste en que las Auditorías en múltiples ubicaciones pueden ser planificadas muy fácilmente, pudiendo al mismo tiempo planificar distintos tipos de Auditorías para cualquier parte del Universo de Auditoría.

Se pueden entonces usar para generar Informes de Desempeño, que comparan cualquier Plan Anual elegido con lo que ocurrió en los hechos durante dicho período. Además de registrar las Evaluaciones

de Riesgo, se puede almacenar también información adicional, como detalles de contacto e información de Archivo Permanente; esto puede incluir cualquier documento electrónico.

Este proceso culmina con la determinación de la próxima fecha de Auditoría para todas las entidades del Universo de Auditoría

WRM Resolver

Desarrollada para ayudar a las organizaciones a optimizar sus procesos relacionados con la Gobernabilidad, Administración del Riesgo, el Cumplimiento y la Auditoría, entre otros y variados sistemas y modelos de aseguramiento, integrando y compartiendo algunos o todos estos modelos a nivel corporativo.

- ✓ Administrar Prioridades del negocio
- ✓ Enfoque dinámico basado en riesgos
- ✓ Más tiempo para análisis
- ✓ Auditorias desde el principio hasta el fin
- ✓ Aplicar estándares internacionales
- ✓ Hacer mucho más con menos
- ✓ Segregación de deberes

Con WRM Resolver se ahorra tiempo y recursos, y se obtiene beneficios claves para las organizaciones tales como:

Flexibilidad: La terminología, metodología y estructuras de WRM RESOLVER se adaptan fácilmente a los requerimientos específicos de su área.

Estándares y modelos nacionales e internacionales: Diseñe distintas estructuras y modelos (ISO 31000, COSO ERM ISO 27000, ITIL, COBIT, PMBOOK, entre otras), cumpliendo también con normatividades locales sin preocupaciones. Con WRM: RESOLVER usted no se ajusta a la herramienta, es la herramienta la que se ajusta a sus requerimientos.

Más eficiencia, menos duplicación: Compartir información totalmente integrada entre todos los interesados claves: oficina de riesgos, división de auditoría, áreas de cumplimiento, unidades de negocio, áreas de tecnología, es el escenario ideal para cualquier organización sin pensar en módulos adicionales y desconectados para cada requerimiento.

Integridad y confidencialidad de los datos: Los grupos de usuarios y la seguridad basada en roles, le permite asignar y actualizar permisos de acceso a medida que evoluciona la organización. La confidencialidad de los datos es uno de los aspectos más sensibles en los procesos GRC, en donde solo los usuarios responsables tienen acceso al sistema, interactuando con múltiples usuarios para recolección y actualización de información.

Sherlock: aplicación que permite gestionar los diferentes Sistemas de administración de Riesgos, definidos por los diferentes organismos de vigilancia y control; tales como la Superintendencia Financiera de Colombia, Superintendencia de Salud, Superintendencia de Vigilancia, entre otras, bajo estándares y metodologías internacionales, que facilitan el desarrollo de la Gestión de Riesgos de las compañías.

- ✓ Desarrolla un esquema de auditoría basado en riesgos.
- ✓ Administra programas de auditoría.
- ✓ Genera informes y planes de acción automatizados.
- ✓ Planifica y controla tiempo de la auditoría y su equipo de trabajo.
- ✓ Crea grupos de auditoría con estructura jerárquica.
- ✓ Planes de acción por auditado.
- ✓ Revisión a las recomendaciones; hallazgos y riesgos (Jefe Auditor).
- ✓ Aprobar o rechazar cierre de planes de acción.
- ✓ Desarrolla todo el proceso de auditoría, desde la planeación, hasta la generación de informes de auditoría.
- ✓ Genera planes anuales de auditorías para ser presentados al Comité de Auditoría a la Alta Dirección.

3 ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1 La organización ISO y la Familia de Normas ISO

La organización Internacional de Estándares ISO, abreviado por sus siglas en inglés, International Organization for Standardization, se origina en la Federación Internacional de Asociaciones Nacionales de Normalización (1926 – 1939). En octubre de 1946, en Londres, se acordó su nombre por representantes de veintiocho países. La ISO, celebró su primera reunión en junio de 1947 en Zurich, Alemania, su sede se encuentra ubicada en Ginebra, Suiza. Su finalidad principal es la de promover el desarrollo de estándares internacionales y actividades relacionadas incluyendo la conformidad de los estatutos para facilitar el intercambio de bienes y servicios en todo el mundo. La ISO creó en 1987 la serie de estandarización ISO 9000 adoptando la mayor parte de los elementos de la norma británica BS 5750 que estudió en la lección 3. Ese mismo año la norma fue adoptada en los Estados Unidos como la serie ANSI/ASQC– Q90 (American Society for Quality Control); y la norma BS 5750 fue revisada con el objetivo de hacerla idéntica a la norma ISO 9000.(ISO 27000 Español, 2012)

Las normas ISO ofrecen soluciones y logra beneficios para casi todos los sectores de diferente actividad como la agricultura, construcción,

ingeniería mecánica, fabricación, distribución, transporte, medicina, dispositivos, tecnologías de información y comunicación, el medio ambiente, energía, gestión de calidad, evaluación de la conformidad y los servicios

3.2 Familia de normas ISO/IEC 27000:2013

Familia de estándares de ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporciona un marco para la gestión de la seguridad. Es el conjunto de normas que especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI.(Imbaquingo Esparza & Pusdá Chulde, 2015). Las normas se clasifican en:

- ✓ Normas base: 20001, 20002
- ✓ Normas complementarias: 20003, 20004, 20005

En la Tabla 1 se detalla la relación de las normas ISO/IEC 27000

Tabla 1: Relación de serie de las normas ISO/IEC 27000

Normas	Temática
ISO 27000	Gestión de la seguridad de la información (Fundamentos y vocabulario)
ISO 27001	Especificaciones para un SGSI
ISO 27002	Código de buenas prácticas
ISO 27003	Guía de implantación de un SGSI
ISO 27004	Sistema de métricas e indicadores
ISO 27005	Guía de análisis y gestión de riesgos
ISO 27006	Especificaciones para Organismos Certificadores de SGSI.
ISO 27007	Guía para auditar un SGSI.
ISO/IEC TR 27008	Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI
ISO/IEC 27010	Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.

Fuente: (ISO 27000 Español, 2012)

ISO/IEC 27001:2013

Norma que especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado dentro del contexto global de los riesgos de negocio de

la organización. Especifica los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de organizaciones individuales o partes de las mismas.(Imbaquingo Esparza & Pusdá Chulde, 2015). Especifica los requisitos a cumplir para:

- ✓ Implantar un SGSI certificable conforme a las normas 27000
- ✓ Define cómo es el SGSI, cómo se gestiona y cuáles son las responsabilidades de los participantes.
- ✓ Sigue un modelo PDCA (Plan-Do-Check-Act)
- ✓ Puntos clave: Gestión de riesgos + Mejora continua

Estructura: La estructura de ISO/IEC 27001:2013 ha sido desarrollado con base en el anexo SL de ISO/IEC del "Suplemento Consolidado de las Directivas ISO/IEC" (anteriormente publicado como "Guía ISO:83"), en el cual se proporciona un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión sin importar su enfoque empresarial, alineando bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia. (ISO 27000 Español, 2012)

El cambio más significativo en todo el apartado fue la eliminación de la sección "Enfoque del proceso" que contenía la versión 2005, en donde se describía el modelo PDCA, corazón del Sistema de Gestión

de Seguridad de la Información (SGSI). (González Trejo, 2013). La nueva estructura se detalla en la Figura 16

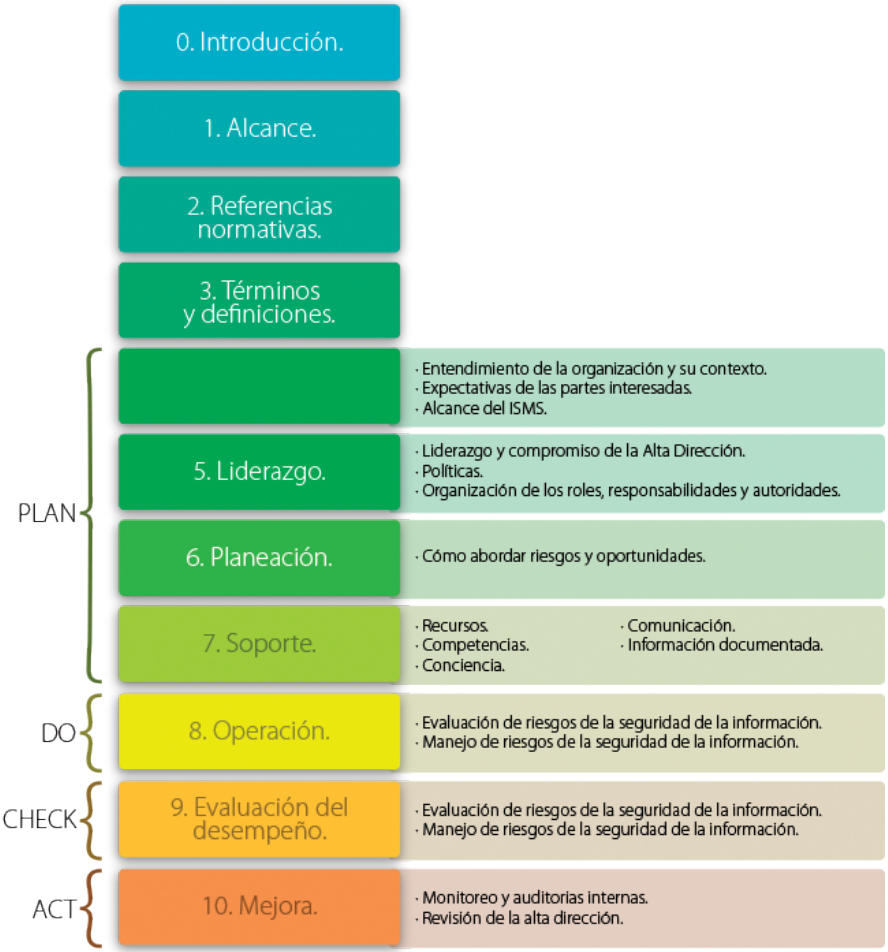


Figura 16. Estructura del estándar ISO/IEC 27001:2013

Fuente: (González Trejo, 2013)

Alcance: En esta sección se establece la obligatoriedad de cumplir con los requisitos especificados en los capítulos 4 a 10 del documento, para poder obtener la conformidad de cumplimiento y certificarse.

Referencias normativas: El estándar ISO-27002 ya no es una referencia normativa para ISO-27001:2013, aunque continúa considerándose necesario en el desarrollo de la declaración de aplicabilidad (SOA, por sus siglas en inglés). El estándar ISO 27000:2013 se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones.

Términos y definiciones: Los términos y definiciones que se manejaban en 27001:2005 los trasladaron y agruparon en la sección 3 de ISO 27000:2013 "Fundamentos y vocabulario" (lo cual se llevará a cabo en todos los documentos que forman parte de esta familia), con el objetivo de contar con una sola guía de términos y definiciones que sea consistente.

Contexto de la organización: Esta cláusula hace hincapié en identificar los problemas externos e internos que rodean a la organización. Instituye los requerimientos para definir el contexto del SGSI sin importar el tipo de organización y su alcance.

Introduce una nueva figura (las partes interesadas) como un elemento primordial para la definición del alcance del SGSI.

Establece la prioridad de identificar y definir formalmente las necesidades de las partes interesadas con relación a la seguridad de la información y sus expectativas con relación al SGSI, pues esto determinará las políticas de seguridad de la información y los objetivos a seguir para el proceso de gestión de riesgos.

Liderazgo: Ajusta la relación y responsabilidades de la Alta Dirección respecto al SGSI, destacando de manera puntual los siguientes compromisos:

- ✓ Garantizando que los objetivos del SGSI y "La política de seguridad de la información", anteriormente definida como "Política del SGSI", estén alineados con los objetivos del negocio.
- ✓ Garantizando la disponibilidad de los recursos para la implementación del SGSI (económicos, tecnológicos, etcétera).
- ✓ Garantizando que los roles y responsabilidades claves para la seguridad de la información se asignen y se comuniquen adecuadamente.

Planeación: Esta es una nueva sección enfocada en la definición de los objetivos de seguridad como un todo, los cuales deben ser claros y se debe contar con planes específicos para alcanzarlos. En esta sección se presentan grandes cambios en el proceso de evaluación de riesgos:

- ✓ El proceso para la evaluación de riesgos ya no está enfocado en los activos, las vulnerabilidades y las amenazas.
- ✓ Esta metodología se enfoca en el objetivo de identificar los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información.
- ✓ El nivel de riesgo se determina con base en la probabilidad de ocurrencia del riesgo y las consecuencias generadas (impacto), si el riesgo se materializa.
- ✓ Se ha eliminado el término "Propietario del activo" y se adopta el término "Propietario del riesgo".
- ✓ Los requerimientos del SOA no sufrieron transformaciones significativas.

Soporte: Marca los requerimientos de soporte para el establecimiento, implementación y mejora del SGSI, que incluye:

- ✓ Recursos
- ✓ Personal competente
- ✓ Conciencia y comunicación de las partes interesadas

Se incluye una nueva definición "información documentada" que sustituye a los términos "documentos" y "registros"; abarca el proceso de documentar, controlar, mantener y conservar la documentación

correspondiente al SGSI. El proceso de revisión se enfoca en el contenido de los documentos y no en la existencia de un determinado conjunto de estos.

Operación: Establece los requerimientos para medir el funcionamiento del SGSI, las expectativas de la Alta Dirección y su realimentación sobre estas, así como el cumplimiento con el del estándar. Además, plantea que la organización debe planear y controlar las operaciones y requerimientos de seguridad, erigiendo como el pilar de este proceso la ejecución de evaluaciones de riesgos de seguridad de la información de manera periódica por medio de un programa previamente elegido.

Los activos, vulnerabilidades y amenazas ya no son la base de la evaluación de riesgos. Solo se requiere para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.

Evaluación del desempeño: La base para identificar y medir la efectividad y desempeño del SGSI continúan siendo las auditorías internas y las revisiones del SGSI. Se debe considerar para estas revisiones el estado de los planes de acción para atender no conformidades anteriores y se establece la necesidad de definir quién y cuándo se deben realizar estas evaluaciones, así como quién debe analizar la información recolectada.

Mejora: El principal elemento del proceso de mejora son las no-conformidades identificadas, las cuales tienen que contabilizarse y compararse con las acciones correctivas para asegurar que no se repitan y que las acciones correctivas sean efectivas.

Aquí se incluye uno de los cambios más importantes porque las medidas preventivas se fusionarán con la evaluación y tratamiento del riesgo, algo más natural e intuitivo que permite enfrentar los riesgos y las oportunidades con base en cuándo estos se identifican y cómo se tratan. Además, se distingue entre las correcciones que se ejecutan como una respuesta directa a una "no conformidad", en oposición a las acciones correctoras que se realizan para eliminar la causa de la no conformidad.

Anexos: El "Anexo A – Referencia de objetivos y controles" continúa formando parte de este estándar, pero los anexos "B" y "C" se han eliminado. En la Figura 17 se detallan los anexos

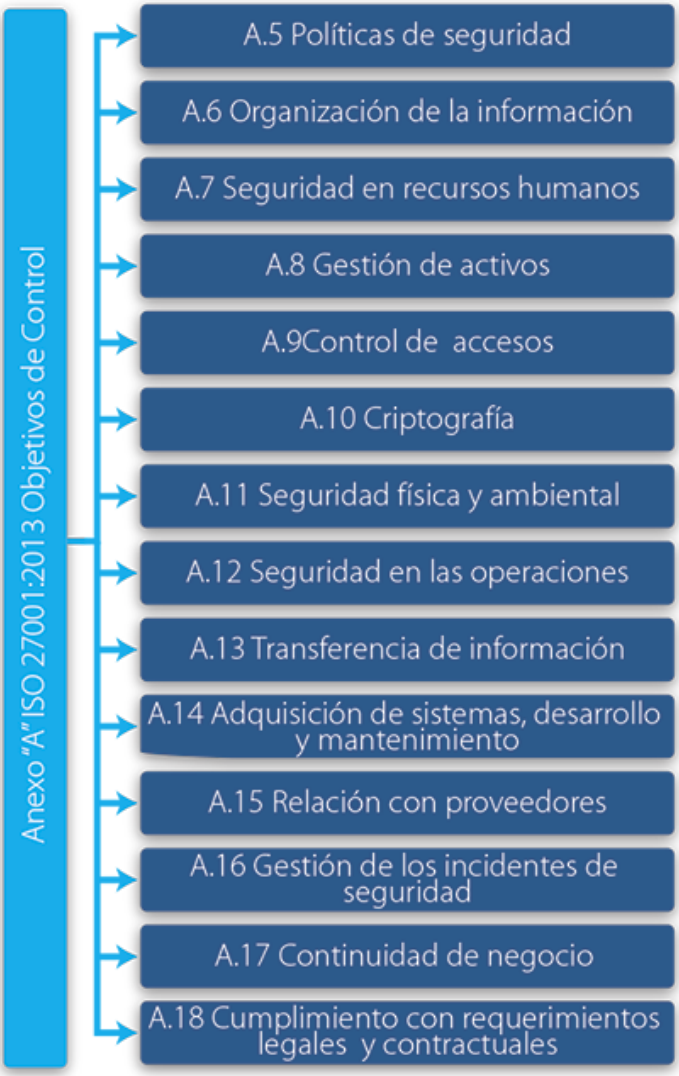


Figura 17. Dominios Anexo "A" de ISO 27001:2013

Fuente: (ISO 27000 Español, 2012)

La lista de controles que ya no forman parte del estándar se detallan en la Tabla 2

Tabla 2: Controles suprimidos de la norma ISO 27001:2013

Control	Descripción	Cambia por	Controles de la ISO 27001:2005
A.6.1.1	Comité de gestión para la seguridad de la información	Roles de la seguridad de la información y sus responsabilidades	A.6.1.3 y A.8.1.1
A.6.1.2	Coordinación de seguridad de la información	Contacto con autoridades	A.6.1.6
A.6.1.4	Procesos de autorización para instalaciones para procesamiento de información	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con agentes externos	Política de dispositivo móvil	A.11.7.1
A.6.2.2	Direccionamiento de seguridad al tratar con clientes	Trabajo a distancia	A.11.7.2
A.10.2.1	Entrega del servicio		
A.10.7.4	Seguridad del sistema de documentos		
A.10.8.5	Sistema de información de negocios		
A.10.10.2	Seguimiento al uso de sistema		
A.10.10.5	Falla en el registro		
A.11.4.2	Autenticación de usuarios para conexiones externas		
A.11.4.3	Identificación de equipos		
A.11.4.4	Puerto remoto de diagnóstico y configuración de protección		

A.11.4.6	Control para la conexión de redes		
A.11.6.2	Aislamiento del sistema sensible		
A.12.2.1	Validación de datos de entrada	Controles contra malware	A.10.4.1
A.12.2.2	Control de procesamiento interno		
A.12.2.3	Integridad de mensaje		
A.12.2.4	Validación de datos de salida		
A.12.5.4	Filtración de la información		
A.15.1.5	Prevención del uso indebido de las instalaciones para el procesamiento de información		
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información		

Fuente: (ISO 27000 Español, 2012)

Tabla 3: Nuevos controles propuestos.

Control	Descripción	Absorbe los controles de la ISO 27001:2005
A.6.1.4	Seguridad de la información en la gestión de proyectos	
A.12.6.2	Restricciones en la instalación de software	
A.14.2.1	Política de desarrollo de seguridad	
A.14.2.5	Desarrollo de procedimientos para el sistema	
A.14.2.6	Desarrollo de un entorno seguro	
A.14.2.8	Sistema de prueba de seguridad	
A.15.1.1	Información de seguridad para las relaciones de proveedores	A.6.2.3
A.15.1.3	Cadena de suministro ICT	
A.16.1.4	Evaluación y decisión de los eventos de seguridad de la información	
A.16.1.5	Respuesta a incidentes de seguridad de la información	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de las instalaciones para procesamiento de información.	

Fuente: (ISO 27000 Español, 2012)

ISO/IEC 27002:2013

Conjunto de recomendaciones sobre qué medidas tomar en las empresas para asegurar los Sistemas de Información. Código de buenas prácticas para la gestión de la seguridad.(ISO 27000 Español, 2012)

Los objetivos de seguridad recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa. Para conseguir cada uno de estos objetivos la norma propone una serie de medidas o recomendaciones (controles) que son los que se aplican en la gestión de riesgos.

Objetivos: Definir los aspectos prácticos/operativos de la implantación del SGSI en cada área o sección.

- ✓ Servir de punto de información de la serie de normas ISO 27000 y de la gestión de seguridad de la información mediante la aplicación de controles óptimos a las necesidades de las organizaciones en cada momento.
- ✓ Realizar la libre difusión de información en español en base a las investigaciones, conocimientos y búsquedas de los editores de la web.
- ✓ Responder a todas las consultas recibidas en relación a las normas de la serie ISO 27000, independientemente de su origen (empresas grandes, Pymes, organismos públicos, estudiantes, entre otros.

- ✓ Establecer contactos con todo tipo de organizaciones, desarrolladores y personas relacionadas con la norma, con el objetivo de intercambiar informaciones, opiniones, experiencias o conocimientos, e impulsar la colaboración en actividades de fomento y promoción de las buenas prácticas para la aplicación de controles para la seguridad de la información.

Características: La normativa presenta las siguientes:

- ✓ Recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización
- ✓ Describe los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especifica los controles recomendables a implantar (medidas a tomar)
- ✓ Antes ISO 17799, basado en estándar BS 7799 (en España norma UNE-ISO 17799)

Áreas/secciones sobre las que actuar:

- ✓ Política de seguridad
- ✓ Aspectos organizativos para la seguridad
- ✓ Clasificación y control de activos
- ✓ Seguridad ligada al personal
- ✓ Seguridad física y del entorno
- ✓ Gestión de comunicaciones y operaciones
- ✓ Control de accesos

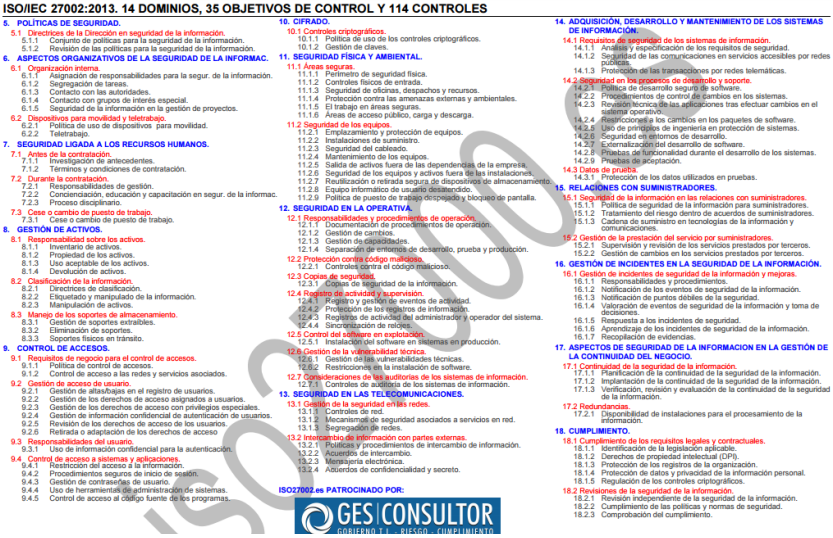
- ✓ Desarrollo y mantenimiento de sistemas
- ✓ Gestión de incidentes de seguridad de la información
- ✓ Gestión de continuidad de negocio
- ✓ Conformidad

Controles: "Mecanismos para asegurar los distintos objetivos de control (guía de buenas prácticas)" (ISO ESPAÑOL, 2014). Para cada control se incluye una guía para su implantación.

Con la actualización de esta norma las organizaciones pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información. En este sentido, hay que mencionar que esta actualización establece una nueva organización de las categorías, las cuales se mezclan y dan pie a la creación de otras para brindar una estructura más coherente, de tal forma que, en la nueva norma, se describen 14 dominios de control, 35 objetivos y 114 controles, aumentando por otra parte, los requisitos de gestión que pasan a ser 130. El contenido de la norma ISO 27002:2013 se detallan en la Figura 18 y Figura 19.

Figura 18. Contenidos de la norma ISO 27002:2013

Fuente: (UNIT, 2015)



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:
GES CONSULTOR
GOBIERNO T.I. · RIESGO · CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

Figura 19. Dominio, objetivos y controles de la norma ISO 27002:2013

Fuente: (ISO 27000 Español, 2012)

Políticas de seguridad: Un documento denominado "política" es aquel que expresa una intención e instrucción global en la manera que formalmente ha sido expresada por la Dirección de la organización.

Contenido: El contenido de las políticas se basa en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores.

Resumen: Política Resumen - Visión general de una extensión breve; una o dos frases y que pueden aparecer fusionadas con la introducción.

- ✓ Introducción: Breve explicación del asunto principal de la política.
- ✓ Ámbito de aplicación: Descripción de los departamentos, áreas o actividades de una organización a las que afecta/aplica la política. Cuando es relevante en este apartado se mencionan otras políticas relevantes a las que se pretende dar cobertura desde ésta.
- ✓ Objetivos: Descripción de la intención de la política.
- ✓ Principios: Descripción de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos. En algunos casos puede ser de utilidad identificar previamente los procesos clave asociados

con el asunto principal de la política para pasar posteriormente a identificar las reglas de operación de los procesos.

- ✓ Responsabilidades: Descripción de quién es responsable de qué acciones para cumplir con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, así como las responsabilidades de las personas con roles designados.
- ✓ Resultados clave: Descripción de los resultados relevantes para las actividades de la organización que se obtienen cuando se cumplen los objetivos.
- ✓ Políticas relacionadas: Descripción de otras políticas relevantes para el cumplimiento de los objetivos, usualmente se indican detalles adicionales en relación a temas específicos. La política de alto nivel (más genérica) habitualmente relacionada con el sistema de gestión para la seguridad de la información (SGSI) suele estar apoyada por políticas de bajo nivel, específicas a aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, uso aceptable de activos, escritorio y pantallas libres de información sensible, dispositivos móviles y teletrabajo, backups, protección contra el malware, entre otros.

Objetivo: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

- ✓ **Directrices de la Dirección en seguridad de la información**: La gerencia debería establecer de forma clara las líneas de las políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en toda la organización.

Actividades de control del riesgo

- ✓ **Políticas para la seguridad de la información:** Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados, así como a todas las partes externas relevantes.
- ✓ **Revisión de las políticas para la seguridad de la información:** Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.

ISO/IEC 27003

Guía de implementación de SGSI e información acerca del uso del modelo PDCA (Plan-Do-Check-Act) y de los requerimientos de sus

diferentes fases (en desarrollo, pendiente de publicación). (ISO 27000 Español, 2012)

ISO/IEC 27004

Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados (en desarrollo, pendiente de publicación). Permite la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA. (ISO 27000 Español, 2012)

ISO/IEC 27005

Gestión de riesgos de seguridad de la información (recomendaciones, métodos y técnicas para evaluación de riesgos de seguridad). (ISO 27000 Español, 2012)

ISO/IEC 27006

Requisitos a cumplir por las organizaciones encargadas de emitir certificaciones. ISO/IEC 27001, requisitos para la acreditación de las entidades de auditoria y certificación. (ISO 27000 Español, 2012)

ISO/IEC 27007

Guía de actuación para auditar los SGSI conforme a las normas 27000. (ISO 27000 Español, 2012)

3.3 MAGERIT VERSIÓN 3

Introducción

Magerit es el acrónimo de (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), creado por el Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España. (CCN-CERT-Libro I, 2012)

Magerit mide la vulnerabilidad por la frecuencia histórica cuantitativa de la materialización de la amenaza sobre el activo, cuando es factible (fiabilidad de un componente hardware, número de fallos de software); o bien por la potencialidad cualitativa de dicha materialización, cuya primera aproximación lleva a emplear una escala vista en las amenazas potenciales (consideradas ahora reales, o sea agresiones). Magerit está dirigido a los medios electrónicos, informáticos y telemáticos, lo cual ha dado lugar al origen de ciertos riesgos que se deben de evitar con medidas preventivas para lograr tener confianza en utilizarlos. No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a los riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas).

Historia y Evolución

En la actualidad se encuentra en la versión 3.0, pero el tiempo ha pasado desde la primera publicación de Magerit en 1997, y la segunda publicación en 2005, donde el análisis de riesgos se ha venido consolidando como eje central para la gestión de la seguridad. Los 7 libros de Magerit versión 1, han evolucionado como se detalla en la Tabla 4

Tabla 4: Evolución Magerit libro 1 a la versión 3

Magerit versión 1	Magerit versión 3
Libro I. Guía de aproximación a la seguridad de los sistemas de información.	Libro I – Método
Libro II. Guía de procedimientos	Libro I – Método
Libro III. Guía de técnicas	Guía de Técnicas
Libro IV. Guía para desarrolladores de aplicaciones	Libro I – Método / Capítulo 7 Desarrollo de sistemas de información
Libro V. Guía para responsables del dominio protegible	Libro I – Método Libro II – Catálogo de Elementos
Libro VI. Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos	Libro II – Catálogo de Elementos / formatos XML
Libro VII. Referencia de normas legales y técnicas	Libro I – Método / Apéndice 3. Marco legal

Fuente: (CCN-CERT-Libro I, 2012)

Objetivos de Magerit

En el libro I de la publicación de Magerit versión 3 persigue los siguientes objetivos:

Directos:

- ✓ Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- ✓ Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Marco de trabajo

Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados de uso de tecnologías de la información.

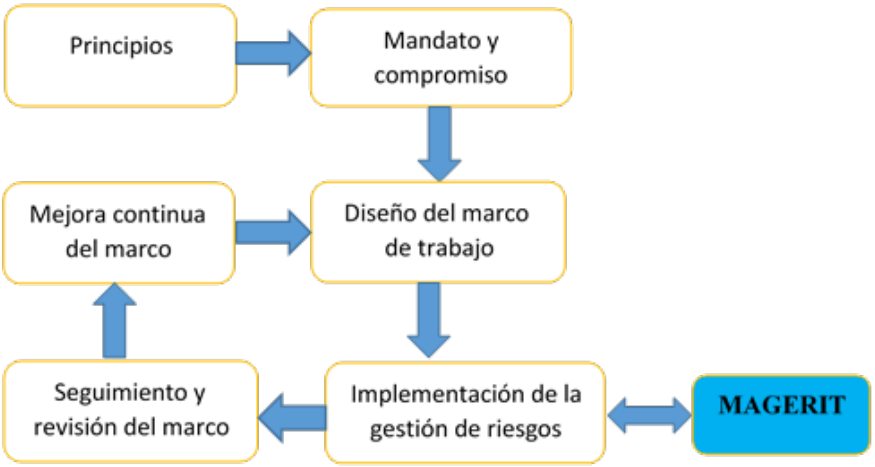


Figura 20. Marco de trabajo para la gestión de riesgos

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

Existen varias aproximaciones que sirven para analizar los riesgos que pueden sufrir sistemas y las tecnologías de la información y comunicación: guías formales, aproximaciones metódicas y herramientas de soporte. Todas ellas tienen como finalidad el saber cuan seguros o inseguros son los sistemas. Existen muchos elementos que hay que considerar para lograr tener buenos resultados. Es por ello que Magerit está basado sobre una aproximación metódica que no deja lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Organización de las Guías

La metodología consta de tres volúmenes:

Volumen I: Método

Volumen II: Catalogo de Elementos

Volumen III: Guía de Técnicas

Volumen I-Método: Este guía está estructurado de la siguiente manera:

Capítulo I: Es una fase introductoria a la metodología, pronunciando que organismos lo crearon

Capítulo II Visión de Conjunto: presenta los conceptos informalmente. Específicamente se enmarcan las actividades de análisis y tratamiento de riesgos para tener un proceso integral de gestión de riesgos.

El capítulo III Método de Análisis de Riesgos: es exclusivo solo para el Análisis de Riesgos donde explica detalladamente cada uno de los pasos que se van a realizar en este tipo de proyectos, donde va orientado para cualquier organización empresarial que lo requiera.

El capítulo IV Proceso de Gestión de Riesgos: describe todas las actividades que se hacen dentro de la Gestión de Riesgos.

El capítulo V Proyectos de Análisis de Riesgos: se centra en los Proyectos de Análisis de Riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y

eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

El capítulo VI Plan de Seguridad: determina cuáles serán las actividades para llevar a cabo un plan de seguridad, después de haber realizado el proyecto de Análisis y Gestión de Riesgos, de esta manera se escogen las decisiones apropiadas para el tratamiento de los riesgos.

El capítulo VII Desarrollo de Sistemas de Información: se centra la seguridad de los sistemas de información considerando varios puntos de vista para mitigar riesgos, además interviene el Análisis de Riesgos que tiene el mismo propósito asegurar la información.

El capítulo VIII Consejos Prácticos: ofrece recomendaciones prácticas para aplicarlos en las tareas del Análisis de Riesgos, lo que resulta muy conveniente para la persona que realiza este tipo de proyectos.

Los apéndices recogen material de consulta:

- ✓ Apéndice 1. Un glosario.
- ✓ Apéndice 2. Referencias bibliográficas consideradas para el desarrollo de esta metodología.
- ✓ Apéndice 3. Referencias al marco legal que incluye las tareas de análisis y gestión en la Administración Pública Española.
- ✓ Apéndice 4. El marco normativo de evaluación y certificación.

- ✓ Apéndice 5. Al realizar el Análisis de Riesgos comprende trabajar con cierta cantidad de información y uno de los primeros pasos es el de Identificar Activos, número de Amenazas y una cantidad determinados de Salvaguardas. Toda da como resultado el manejo de grandes cifras de datos y combinaciones entre ellos, lo que lleva naturalmente a buscar el apoyo de herramientas automáticas.
- ✓ Apéndice 6. Ofrece una guía comparativa de la evolución de Magerit versión

Volumen II: Catálogo de elementos, complementa el volumen I proporcionando tareas antes explicadas en el capítulo II que sirve para aplicación de esta metodología.

- ✓ Tipos de activos
- ✓ Dimensiones y criterios de valoración
- ✓ Amenazas
- ✓ Salvaguardas

En este libro se establecen dos objetivos:

- ✓ Facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

- ✓ Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Volumen III-Guía de Técnicas: El objetivo de este documento es describir algunas técnicas utilizadas en análisis y gestión de riesgos. Se considera técnica a un conjunto de heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos:

- ✓ Se explica brevemente el objetivo que se persigue al utilizarlas,
- ✓ Se describen los elementos básicos asociados,
- ✓ Se exponen los principios fundamentales de elaboración,
- ✓ Se presenta una notación textual y/o gráfica y
- ✓ Se citan las fuentes bibliográficas que, sin ser exhaustivas, se han estimado de interés para que el lector profundice en cada materia.

Las técnicas que recoge son:

- ✓ Análisis mediante tablas
- ✓ Análisis algorítmico
- ✓ Árboles de ataque
- ✓ Técnicas generales
- ✓ Análisis coste-beneficio
- ✓ Diagramas de flujo de datos (DFD)
- ✓ Diagramas de procesos
- ✓ Técnicas gráficas

- ✓ Planificación de proyectos
- ✓ Sesiones de trabajo: entrevistas, reuniones y presentaciones
- ✓ Valoración Delphi

4 ANÁLISIS Y GESTIÓN DE RIESGOS CON MAGERIT V3

4.1 Introducción

John Von Neumann expresa que la Gestión de Riesgos nace de la necesidad de organizar e interpretar datos científicos y otras informaciones, facilitando la toma de decisiones y los acuerdos. El interés por poder determinar con anticipación los eventos del futuro, supuso el pilar de un área de la matemática aplicada conocida inicialmente como Teoría de Juegos.

La Gestión del Riesgo para la Seguridad de la Información surge a partir del campo de la Gestión de Seguros, donde se empieza a forjar la relación coste-beneficio. Para las décadas de 80 y 90 se convierte en parte fundamental en las empresas en su planificación y estrategias.

A finales del siglo XX se comienza a conocer los riesgos informáticos dentro de una empresa están cada vez más presentes por tal motivo que se deben tomar las acciones necesarias para evitarlos. Po tal motivo en el año 1995 se crean estándares de Seguridad de la Información (BS 7799-1) adoptando precisamente en el año 2000

como es estándar ISO/IEC 17799, descubriendo ya la gestión del riesgo como parte del proceso de seguridad. (Cuenca et al., 2011)

Actualmente las tareas que se realizan en el Análisis y Gestión de Riesgos su principal función son de complementarse entre sí para llegar la Gestión de la Seguridad. Al seguir sistemáticamente cada uno de los pasos suele ser costoso tanto en tiempo como en recurso de personal y que debería realizarse basado en metodologías formales y a si puede ser posible apoyadas por las aplicaciones software.

4.2 Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- ✓ Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- ✓ Determinar a qué amenazas están expuestos aquellos activos.
- ✓ Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- ✓ Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- ✓ Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el desarrollo actual, las empresas dependen más de las Tecnologías de Información las cuales ayudan a realizar tareas cada vez más complejas y por ende corren con riesgos que pueden amenazar el buen desempeño de sus funciones. El análisis de riesgos surgen a partir de la necesidad de organizar e interpretar datos científicos, facilitando decisiones para llegar acuerdos en la empresa.

Además, es el primer paso de la seguridad informática; el mismo que busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

En este paso se estudian todos los controles de seguridad tanto físicos, como técnicos de una empresa ha definido con la finalidad de proteger el ambiente informático. Donde se pueden encontrar fallos de seguridad. Además, es esencial priorizar acciones para reducir la vulnerabilidad de los sistemas de información.

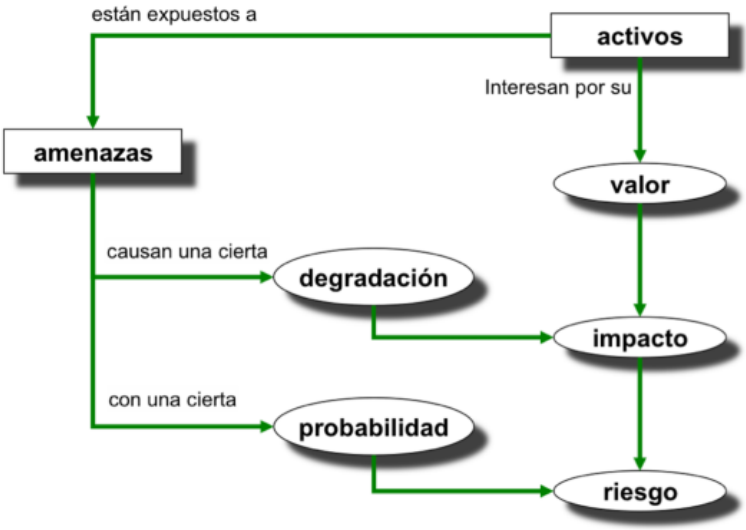


Figura 21. Elementos del análisis de riesgos potenciales

Fuente: (CCN-CERT-Libro II, 2012)

Es responsabilidad de los actores de seguridad que laboran en la empresa, realizar el Análisis de Riesgo con los directores de cada área, ellos saben a qué riesgos están expuestos y por ende pueden ayudar a mitigarlos. Para que los gerentes tengan un presupuesto de cuanto es la inversión que tendrán que realizar a la empresa según las necesidades de la misma.

Hay casos en que empresas han omitido realizar un análisis de riesgos por cuestiones de tiempo o de dinero, pero se suele optar solo por un estudio de vulnerabilidad, sin embargo, se deben considerar todas las alternativas para evitar posibles fallas en la seguridad.

Determinación de activos

Un activo es algo que representa un valor o una utilidad para cualquier organización. Los activos precisan protección para asegurar las operaciones del negocio y la continuidad de la empresa. (CCN-CERT-Libro II, 2012)

El ISO 17799:2005 (Código de Practica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera:

- ✓ Activos de Información: Bases de datos, archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo y planes de continuidad.
- ✓ Documentos Impresos: Documentos impresos, contratos, lineamientos, documentos de la compañía y documentos que contienen resultados importantes del negocio.
- ✓ Activos de Software: Software de aplicación, software de sistemas y herramientas de desarrollo.
- ✓ Activos Físicos: Equipos de computación y comunicación y otros equipos técnicos.
- ✓ Personas: Personal, clientes y suscriptores.
- ✓ Imagen y reputación de la compañía.
- ✓ Servicios: Servicios de computación y computación, otros servicios técnicos.

En el trabajo cada uno de empleados es el encargado de uno o más activos según el cargo que ocupe en la institución, deberá velar por la seguridad del activo. Sin embargo, no todos los activos tienen la misma importancia y por lo tanto los mecanismos de seguridad que utilizan dependerán de las amenazas a los que estén que se enfrentan los mismos.

Dependencias entre Activos: Existen activos que dependen unos de otros más significativos en los que están involucrados equipos, las comunicaciones entre otros. Por tal razón nace el término de "dependencias entre activos" que trata de decir es que si un activo superior se ve afectado por un incidente de seguridad en activo inferior. Las dependencias entre activos permiten relacionarse con los demás activos con datos y servicios. Se podría decir que se formaría un árbol de dependencias

Se podría decir que los activos inferiores son las bases de los activos superiores. Pero qué a medida que esta dependencia entre activos crece se deberán tomar las prevenciones más efectivas que los aseguren para no tener prejuicios que resulten perjudiciales para todos.

Capa 1: El Entorno: activos que se precisan para garantizar las siguientes capas

- ✓ Equipamiento y suministros: energía, climatización, comunicaciones

- ✓ Personal: dirección, de operación, de desarrollo, etc.
- ✓ Otros: edificios, mobiliario, etc.

Capa 2: El Sistema de Información

- ✓ Equipos informáticos(hardware)
- ✓ Aplicaciones(software)
- ✓ Comunicaciones
- ✓ Soportes de información: discos, cintas, etc.
- ✓ Capa 3: La Información
- ✓ Datos
- ✓ meta-datos: estructuras, índices, claves de cifra, etc.
- ✓ Capa 4: Las funciones de la Organización
- ✓ Objetivos y misión
- ✓ Bienes y servicios producidos

Capa 5: Otros activos

- ✓ Credibilidad o Solvencia

Valoración de activos: Una vez identificados todos los activos, el siguiente paso es valorarlos. Se refiere al valor que se asigne a cada activo de acuerdo al grado de importancia, además siempre resguardando la disponibilidad, integridad, confiabilidad y disponibilidad de cada uno de ellos.

La valoración de un activo puede ser cuantitativa (escala en una cantidad numérica) o cualitativa (escala de niveles), por ejemplo: nivel bajo, nivel medio, nivel alto o el rango numérico de 0 a 10.

Además, debe de ser lo más sea objetiva posible, se debería contar con la participación de todas las áreas de la organización para que se involucren en este proceso, aunque no sean las encargadas de realizar el Análisis de Riesgos, gracias a la ayudad de ellos se obtener un resultado lo más acercado a la realidad sobre los activos de la organización.

Es ventajoso puntualizar con anterioridad sobre que parámetros se va valorizar los activos para que los empleados puedan realizarlo de acuerdos a los criterios establecidos por la organización, para que se obtengan valores coherentes.

Los criterios hacia la valorización deben estar claros, concisos, además fácil de entender para todos los participantes, ya que final se puedan comparar valores, habiendo como resultado el reconocer cuáles son los activos que tienen mayor prioridad sobre otros, y así ponerles mayor atención en su seguridad.

Dimensiones de valoraciones: Otro punto fundamental que se debe de poner en consideración es saber las consecuencias traería se materializaría una amenaza.

De un activo es interesante saber qué hacer en diferentes dimensiones:

- ✓ Autenticidad: ¿Cuáles serían las consecuencias perjudiciales si descifraran las claves de los equipos de comunicación de una organización? Esta valorización va dirigida a la autenticidad de usuario cuando ocupa determinado equipo.
- ✓ Confidencialidad: ¿Cómo sería si personas no autorizadas accedan a la información? Esta valorización va dirigida si se fugara información a personas ajenas a la organización.
- ✓ Disponibilidad: ¿Qué hacer si no pueden acceder al sistema informático producido por un sabotaje? Esta valorización va dirigida a los servicios como web, móviles, etc.
- ✓ Integridad: ¿Qué hacer si la red de comunicaciones ha sido interceptada, para fines no éticos? Esta valorización va dirigida a la veracidad de la información para que no sufra ninguna transformación.

La mayoría de las dimensiones nombradas anteriormente permiten una valoración simple.

Una vez terminado este paso de la Determinación de Activos se procede a la Determinación de Amenazas.

Determinación de amenazas

Una amenaza es un perjuicio potencial provocado por un incidente deseado o no deseado, hacia todos los activos de una organización empresarial. (CCN-CERT-Libro II, 2012). Si se llegara a ejecutar la amenaza puede poner en peligro la integridad, confidencialidad, autenticidad y disponibilidad de un activo. Las amenazas pueden centrarse en un activo en concreto y reaccionar en cadena a través de las diversas relaciones de dependencia que este posee con el resto de activos.

Identificación de Amenazas: En la identificación de las amenazas se detallan las principales amenazas sobre cada uno de los activos. Pero también pueden dividirse en dos grupos según la intencionalidad del ataque en deliberadas y accidentales:

- ✓ Deliberadas: Son los ataques que ya fueron planificados con el único fin de causar daños hacia los demás. Como, por ejemplo: hurtos, fraudes, sabotajes, etc.
- ✓ Accidentales: Estas son cuando no existe ninguna intención de hacer algún daño, pero al final origina un perjuicio hacia algún activo. Como, por ejemplo: averías en el hardware, software o desastres naturales, etc.

En este proceso ayuda a establecer una relación directa entre un activo y una posible amenaza que le puede ocurrir.

Valoración de las amenazas: En este paso se equilibrarán todas las posibles amenazas que pueden afectar en alguna de las dimensiones de valoración de un activo. Para hacer una valoración más exacta es necesario estimar la frecuencia de ocurrencia y el porcentaje de degradación.

- ✓ Probabilidad de Ocurrencia: Representa la tasa anual de ocurrencia, de cada cuanto se materializa una amenaza.
- ✓ Porcentaje de Degradación: Significa el daño causado por un incidente.

Se determina el grado de degradación y la frecuencia de ocurrencia de cada amenaza sobre cada activo con el fin de saber el impacto y riesgo potencial de dicha amenaza sobre el activo. La frecuencia de ocurrencia se evalúa de acuerdo a los siguientes valores.

Tabla 5: . Probabilidad de Ocurrencia

MA	100	MUY FRECUENTE	A DIARIO
A	10	FRECUENTE	MENSUALMENTE
M	1	NORMAL	UNA VEZ AL AÑO
B	1/10	POCO FRECUENTE	CADA VARIOS AÑOS
MB	1/100	MUY POCO FRECUENTE	SIGLOS

Fuente: (CCN-CERT-Libro I, 2012)

Hay que considerar que la frecuencia de ocurrencia se debería diferenciar las amenazas intencionadas de las accidentales. El grado de degradación se detalla para cada activo relacionándolos con amenaza y dimensión, además se mide entre 0% y el 100%.

Estimación de impactos: Un impacto es el daño que se origina sobre el activo derivado de la materialización de una amenaza. Teniendo la valoración de los activos y el porcentaje de degradación que causan las amenazas, es directo derivar el impacto que tienen sobre los sistemas de información. La estimación de impactos de estos porcentajes se hace en función de varios factores, como son:

- ✓ La ejecución de una amenaza puede de perjudicar a todo un recurso de información o solo a una parte del mismo.
- ✓ Ante la materialización de una amenaza perjudica a partes claves o partes dependientes del recurso de información.
- ✓ Si la amenaza, una vez perpetrada, tiene consecuencias de forma temporal o de forma permanente hacia el recurso.

Las consecuencias indirectas que trae los impactos, pueden ser cualitativas o cuantitativas, como pérdidas económicas, perdida de inversión en el mercado o que los posibles clientes tengan una imagen negativa de la empresa.

Se puede llegar a establecer una proporción entre las consecuencias de los ataques y la cantidad de salvaguardas necesarias.

Se debe tomar en cuenta, también, la posible frecuencia de ocurrencia de realización de las amenazas; esto es especialmente cuando el daño causado por un ataque pequeño, pero el efecto global de muchos ataques en el tiempo, puede dar lugar a considerables pérdidas o daños.

Impacto Acumulado: El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. El impacto será mayor cuanto más grande sea la degradación.

Una ventaja que se tiene al obtener el impacto acumulado es que podrán determinar que salvaguardas habrá que implementar dentro de la empresa.

Impacto Repercutido: Este calcula se basa en valor propio de activo. Se obtiene este valor de la siguiente manera que, por cada activo, por cada amenaza y en cada dimensión de valoración, todo en función del valor propio y la degradación. Lo que permite conocer qué consecuencias tiene los accidentes técnicos sobre los sistemas de información.

Estimación de vulnerabilidad de las amenazas sobre los activos

Las vulnerabilidades provocan debilidades en el sistema que pueden explotarse y dar lugar a consecuencias no deseadas. Sin embargo, aunque haya presencia de vulnerabilidades por misma no ocasionan

daños. Lo que resulta realmente peligroso es cuando están son explotadas por alguna amenaza.

Por eso hay que identificar todos los puntos débiles de una organización para establecer una propiedad de la relación entre un activo y una amenaza y se puede hacer una clasificación de acuerdo a este criterio.

La estimación de vulnerabilidad es un proceso necesario que solo lo deben hacer los entendidos en este tema que es la seguridad de la información en una empresa. Por eso requiere un grupo de expertos profesionales que se involucren para ello y deberán escoger una metodología, para realizar el Análisis de Riesgos. Para poder evaluar esta estimación se puede formular con un valor decimal. Que comprende una escala razonable de valores extremo 0 (la amenaza no perjudica al activo) y 1 (agresión permanente).

Debido a la creciente utilización de las TIC resulta muy complicado no relacionar con ellas considerables salvaguardas de protección contra amenazas de todo tipo.

Por tanto, la estimación de la vulnerabilidad debe siempre referirse a un estado dado de la tecnología que de por implícitas dichas protecciones y partir de dicho estado como base de cálculo de la vulnerabilidad intrínseca para cada amenaza pertinente. Este tipo de

vulnerabilidad para cuya estimación se requiere mayormente la contribución del Responsable de la Seguridad.

Sin embargo, la mayoría de proyectos de seguridad se refieren a una autoridad existente en los que el Responsable ya ha implantado mecanismo de salvaguarda. La Vulnerabilidad efectiva del Activo respecto a cada amenaza concreta tiene en cuenta esos mecanismos de salvaguarda como un factor que estima su eficacia global.

Calculo del nivel de riesgo

El objetivo que tiene este proceso es el identificar y valorar los riegos.

Identificación del Riesgo: Mediante la identificación del riesgo su función específica es de encontrar los riesgos potenciales que tiene cada empresa sobre cada uno de sus activos, utilizando variedad de técnicas o métodos sistemáticos como son:

- ✓ Método Delphi
- ✓ Arboles de Fallos
- ✓ Arboles de Eventos
- ✓ Análisis Probabilístico de Seguridad
- ✓ Entrevistas.
- ✓ Encuestas.
- ✓ Realización del FODA.

Valoración de Riesgos: Para la valorar los riesgos, como primer punto tenemos la identificación de los activos, segundo tenemos la identificación de cada amenaza sobre cada activo, y por último punto tenemos la estimación de la vulnerabilidad de las amenazas sobre cada activo, gracias a los resultados obtenidos por cada uno de estos pasos se puede llevar a cabo una evaluación sencilla para esta operación.

El nivel de riesgo este se divide en cuatro zonas:

- ✓ Bajo: El nivel de riesgo es bajo, y por lo tanto es necesario emplear salvaguardas adicionales.
- ✓ Medio: El nivel de riesgos es medio y se deberá de poner en consideración si se deben implantar salvaguardas para evitarlos.
- ✓ Alto: El nivel de riesgos es alto aquí es una obligación implantar las salvaguardas necesarias para mitigar riesgos.
- ✓ Crítico: Aquí el nivel de riesgo es crítico lo que realmente es preocupante porque se deben utilizar obligatoriamente salvaguardas adicionales para minimizarlos.

Para determinar los niveles riesgos se detalla en las Figuras 22 y Figura 23.

PROBABILIDAD DE OCURRENCIA	
Bajo	1
Medio	2
Ato	3

x

IMPORTANCIA DEL RIESGO	
Bajo	1
Normal	2
Alto	3
Crítico	4

=

NIVEL DE RIESGO	
Bajo	1
Bajo	2
Bajo	3
Medio	4
Medio	5
Medio	6
Alto	7
Alto	8
Alto	9
Crítico	10
Crítico	11
Crítico	12

Figura 22. Cálculo del Nivel de Riesgo

- 0 ≤ Nivel de riesgo Bajo ≤ 3
- 3 < Nivel de riesgo Medio ≤ 6
- 6 < Nivel de riesgo Alto ≤ 9
- 9 < Nivel de riesgo Crítico ≤ 12

Figura 23. Niveles de Riesgo

Fuente: (CCN-CERT-Libro III, 2012)

Para determinar el nivel de riesgo se aplica la siguiente formula:

$$\text{Niveles de Riego} = \frac{\sum_{i=1}^{n}(\text{Probabilidad de ocurrecia del riesgo(i)} * (\text{importancia del riesgo(i)}))}{n}$$

Muy a parte de la metodología que se escoja para realizar el Análisis de Riesgos, lo más importante será que obtendremos una lista de los riesgos correspondientes a cada activo y las consecuencias que tendrían si cada amenaza se cristalizara en cada uno de ellos.

Además, si los resultados son críticos se tendrá que tomar medidas específicas de prevención e intervención, también para los niveles de riesgos medio y alto, para evitar la materialización del mismo.

"El riesgo más peligroso es aquel que no esperamos y para el cual no nos hemos preparado, por ello aun no siendo prioritaria la puesta en práctica de medidas de atención a los mismos, no debemos omitir su existencia."

Beneficios del Análisis de Riesgo

Los Análisis de Riesgos datan de hace varias décadas y han tenido una gran aplicación en varias arias como la aeronáutica, en la industria química y petroquímica y hasta en el campo nuclear. Uno de sus mayores beneficios está en el hecho de que sus resultados constituyen un basamento científico para la toma de decisiones.

Si bien el Análisis de Riesgos en las compañías no es ninguna novedad, ha adquirido importancia, ya que la ejecución de todas las medidas necesarias seguidas por su mantenimiento, evolución y adaptación constante, gracias a la revisión periódica de los controles de seguridad establecidos, corrigiendo fallos de seguridad descubiertos, todo esto para combatir a los nuevos riesgos.

En un proyecto realizado para una empresa el Análisis de Riesgos, obtienen los siguientes beneficios:

- ✓ Listado de las amenazas existentes sobre cada uno de los activos permitiendo manejar apropiadamente los riesgos potenciales.
- ✓ Permite minimizar el impacto de riesgos para reducir costos.
- ✓ Exponer las medidas prácticas que deben ser implementadas para mitigar ataques y riesgos.
- ✓ Asegurar la continuidad operacional del negocio.
- ✓ Seleccionar las mejores decisiones en inversiones para la seguridad de la información.
- ✓ Adecuada Gestión de Riesgos para la Seguridad de la Información.

4.3 Gestión de Riesgos

Proceso

El Proceso de Gestión de Riesgos su principal objetivo es el de identificar y tratar urgentemente los riegos potenciales con elementos que se detallan en la Figura 24

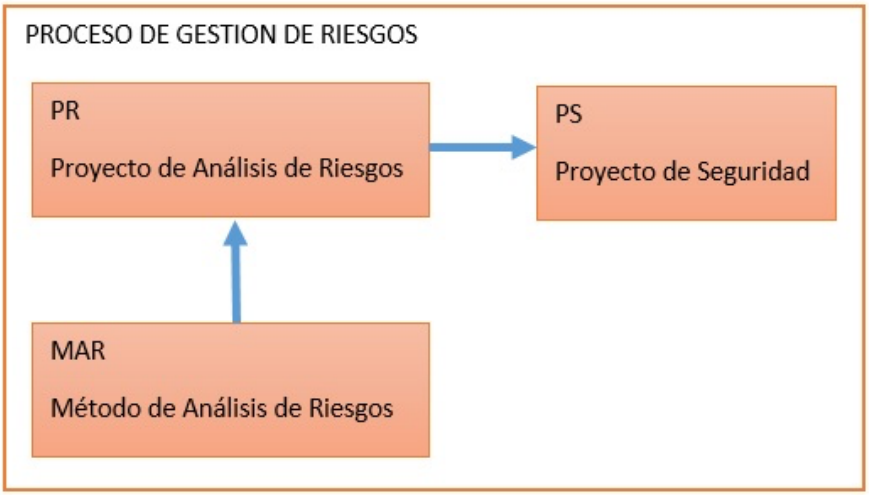


Figura 24. Actividades Formalizadas para la gestión de riesgos

La Gestión del Riesgo persigue lograr un conocimiento lo más realista posible de aquellas circunstancias que podrían afectar a los procesos o servicios, causando daños o pérdidas, de modo que se puedan establecer prioridades y asignar requisitos de seguridad para afrontar convenientemente dichas situaciones. Estos riesgos que pueden ser de muy diferente naturaleza, cobran especial importancia cuando afectan al ámbito de las tecnologías de la información, debido a su imbricación en gran cantidad de los servicios que regulan nuestra sociedad actual. Para la gestión de análisis y gestión de riesgos se realiza el proceso detallado en la Figura 25

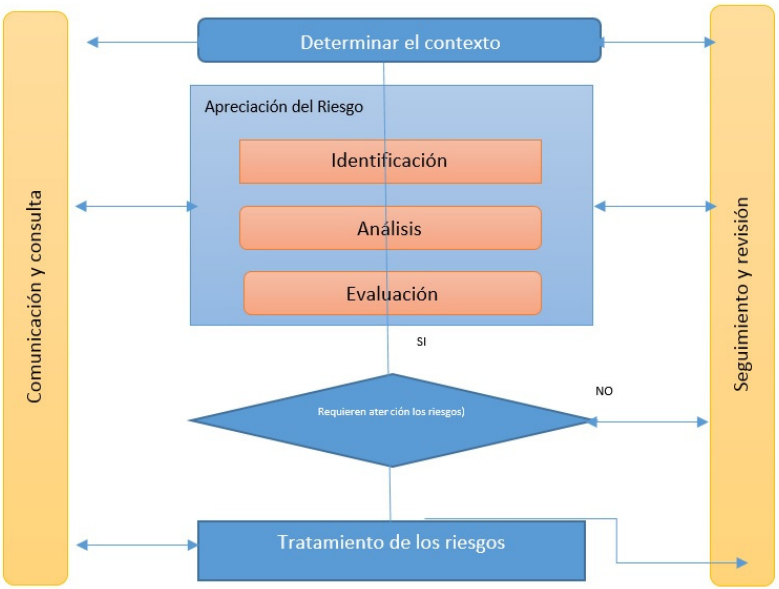


Figura 25. Proceso de gestión de riesgos

Fuente: (CCN-CERT-Libro II, 2012)

Determinación del contexto: Lleva a una determinación de los parámetros y condicionantes externos e internos que permiten delimitar una política que se seguirá para gestionar los riesgos.

Identificación de los riesgos: Busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa.

Análisis de riesgos: Busca calificar los riesgos identificados, bien cuantificando sus consecuencias ya sean cuantitativamente o

cualitativamente. De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

Evaluación de los riesgos: Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de que riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

Tratamiento de los riesgos: Recopila las actividades encaminadas a modificar la situación de riesgo.

Comunicación y consulta: Lo que se desea alcanzar un equilibrio entre la seguridad y productividad.

Seguimiento y revisión: Al finalizar el Análisis de Riesgos el resultado obtenido debe ponerse en práctica lo recomendado para evitar incidentes dentro del entorno del entorno organizacional

La Gestión de Riesgos se apoya en los resultados del Análisis de Riesgos, ya que se centra en la evaluación y el tratamiento del riesgo, para minimizar los costos asociados al riesgo. Para realizar este tipo de estudio no se lo hace de manera empírica sino se base en una aproximación científica del comportamiento de riesgo.

Aquí es donde se deben de examinar una serie de decisiones en torno a los riesgos, en donde debemos escoger la mejor estrategia para

mitigar el impacto, también determinar las salvaguardas oportunas para enfrentarlos. Plantearse un plan de seguridad que ordena y organiza las actuaciones encaminadas para llevar el impacto a niveles de riesgos aceptables.

Es fundamental optimizar la relación coste-beneficio, de modo que la inversión en seguridad no sea superior a la pérdida que el riesgo podría provocar en caso de materializarse, asumiéndose que es inevitable la necesidad de aceptar un nivel de riesgo, que debe ser conocido y limitado a un valor umbral.

Puesto que el riesgo es un concepto dinámico que varía con el transcurso del tiempo y con las modificaciones en los múltiples factores que definen dicho riesgo, la Gestión del Riesgo establece el seguimiento y el análisis continuo de su evolución. Esta reiterada aplicación de Análisis de Riesgos de cara a monitorizar los cambios surgidos, requiere que los análisis puedan ser contrastados manteniendo la necesaria coherencia para poder obtener resultados válidos de tal comparación.

Los estándares ISO 27000, que una adecuada Gestión del Riesgo deben de estar basada en Análisis de Riesgos. El proceso cuenta con fase de identificación- estimación-evaluación del riesgo, seguida de una de tratamiento del riesgo. La situación en relación al riesgo de ser adecuadamente comunicada a los efectos dentro de la organización de

moda que exista una apropiada concientización, mientras que se supervisa y revisa la evolución del riesgo en el tiempo, reiterando periódicamente el proceso.

Determinación de los criterios de aceptación del riesgo

Una técnica de Gestión de Riesgos que permite a la administración comparar el costo de disponer el riesgo contra el beneficio de reducirlo. La aceptación del riesgo es responsabilidad de la máxima autoridad jerárquica y la alta gerencia. La cantidad de riesgo aceptable debe ser determinado de antemano.

De acuerdo al criterio que se emplee en la metodología para el Análisis de Riesgos se debe de considerar el nivel de riego aceptable apropiado para la organización.

El estándar ISO 27001:2013, requiere que la organización en relación al tratamiento del riesgo siga cuatro posibles acciones:

- ✓ Aplicación de apropiados controles para reducir los riesgos.
- ✓ Acepar objetivamente los riesgos partiendo del supuesto que satisfacen la política de la organización y su criterio para la aceptación del riesgo.
- ✓ Evitar el riesgo.
- ✓ Transferir el riesgo asociado a otras partes.

Toda la información que se obtiene en este paso quedara en un informe que se presentara a los directivos de la empresa, para que ellos decidan las mejores medidas de seguridad que van adoptar, para conseguir el nivel de seguridad que desea alcanzar y como referencia para posteriores análisis.

Determinación de las medidas de seguridad necesarias

Una vez identificados todos los riesgos en cada uno de los activos, entonces se procede a tomar las medidas de seguridad de prevención para evitar daños hacia la empresa.

La norma ISO/IEC 27002 es una guía de buenas prácticas que ofrece una exhausta guía sobre los controles a implantar y que se debe seguir si se desea certificar el Sistema de Gestión de Seguridad de la Información de la organización con la norma UNE-ISO/IEC 27001.

Para el caso en que se desea mitigar el riesgo se deberían seguir los siguientes pasos:

- ✓ Seleccionar Controles
- ✓ Implantar Controles
- ✓ Verificar Controles
- ✓ Establecer Indicadores

Seleccionar Controles: Los controles son medidas que están orientadas para mitigar los riesgos que se encontraron en el Análisis

de Riesgos de manera que se encuentren por debajo del riesgo asumido por la organización. Existen dos tipos de controles Técnicos y Organizativos.

Controles Técnicos: Los controles ha adoptarse para la organización deben constar claramente en documento a través de procedimientos.

Entre los ejemplos que se tiene como controles técnicos están:

- ✓ Firewall
- ✓ Antivirus

Controles Organizativos: Los controles que se acojan para ser tomados en cuenta para la empresa también debe de estar presente en documento a través de procedimiento, normativas o políticas de seguridad. En el momento de seleccionar un control se debe de tener en consideración las siguientes cuestiones:

- ✓ Coste Control frente al Impacto: aquí si imaginaría si el activo pasara por un daño y el valor del activo.
- ✓ Necesidad de disponibilidad del control.
- ✓ Controles existentes.
- ✓ Inversión de costos de implantación y mantenimiento: Cuanto tuviera que gastar la empresa en recursos económicos como en humanos.

Una vez que ya concluyeron que controles son autorizados para la organización se procederá a su implantación. Declaración de Aplicabilidad (SOA) es el nombre que tiene el documento donde constan que controles se aplican y los que no aplican.

Implantación de Controles: En esta fase de la implantación de controles técnicos y de salvaguardas se necesita de la intervención de la persona encargada de la Seguridad de la empresa. Y para los controles organizativos participaran exclusivamente los gerentes o altos directivos que son los que tomaran las decisiones, además de formar y concientizar a toda la empresa.

No hay necesidad del desarrollo de un procedimiento o documento por cada uno de los controles que se escojan, sino que se aconseja agrupar diferentes controles para en uno solo para hacer más utilizable el sistema.

Verificar Controles: Es aconsejable revisar periódicamente los controles implantados para revisar si cumplen con el funcionamiento esperado. La persona que debe supervisar el activo es la persona encargada del mismo en función de la criticidad y el valor del mismo.

Establecer Indicadores: Para verificar el correcto funcionamiento de un control implantado es muy importante haber establecido previamente una serie de objetivos e indicadores que nos permitan la medición de dicho funcionamiento.

Estimación del nivel de riesgo residual.

Se considera que el riesgo residual es la pérdida que existe aun cuando se han implementado salvaguardas que han sido implantadas para proteger a los recursos de información de sus amenazas.

Para poder estimar el riesgo residual se debe:

- ✓ Determinar el valor de los activos de información.
- ✓ La exposición de los recursos de información a las amenazas, medida en términos de frecuencia y porcentaje de degradación.
- ✓ La eficacia de salvaguardas implantadas o planificadas para reducir la frecuencia o el impacto de las amenaza.

5 CASO PRÁCTICO MAGERIT V3 - PILAR

5.1 PILAR

PILAR, es el acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" (EAR / PILAR, 2014), es una herramienta desarrollada por el Centro Nacional de Inteligencia para soportar el Análisis de Riesgos de Sistemas de Información basado en la metodología Magerit.

Esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

- ✓ Determinación de Activos: Identificación, dependencias y valoración.
- ✓ Determinación de Amenazas
- ✓ Estimación de Impactos
- ✓ Determinación de los criterios de aceptación del riesgo
- ✓ Determinación de las medidas de seguridad necesarias o Salvaguardas.

Este software permite hacer un análisis de riesgos sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Además, nos ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema. (CCN-CERT, 2012). PILAR puede hacer análisis cuantitativo y cualitativo.

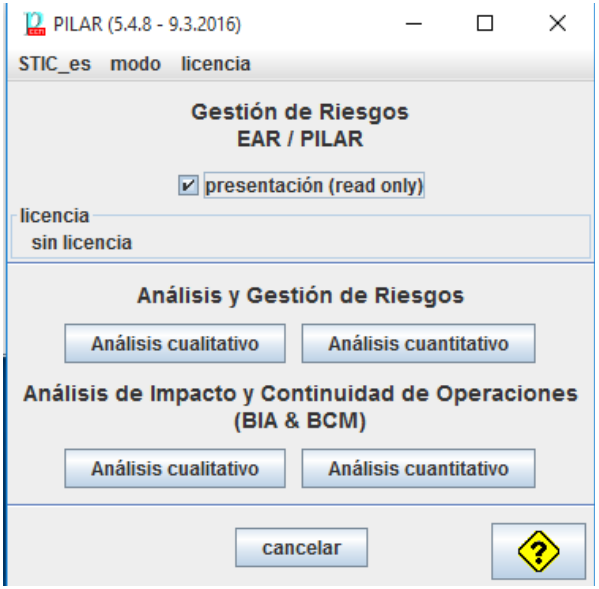


Figura 26. Pantalla Principal Pilar

Los resultados se presentan en diversos formatos como gráficas y tablas

5.2 Institución

Para el caso práctico se consideró la infraestructura tecnológica del departamento de informática de la UTN, relacionados con el Módulo de Gestión Académica del Sistema Integrado Universitario

5.3 Determinación de Activos

Listado de activos clasificados por su función

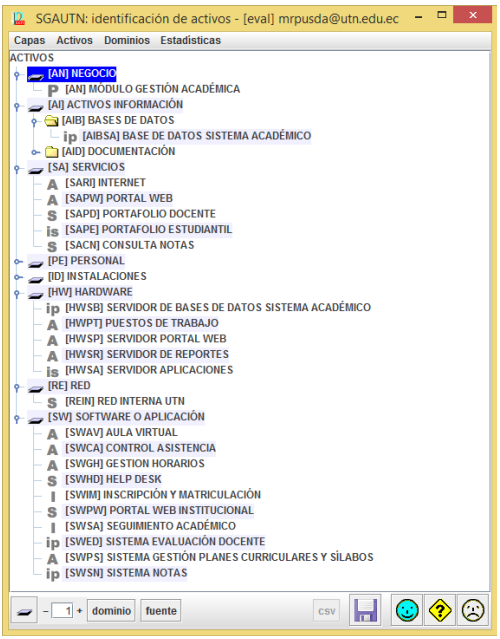


Figura 27. Listado de Activos Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

5.4 Dependencias entre Activos

Relaciones entre activos

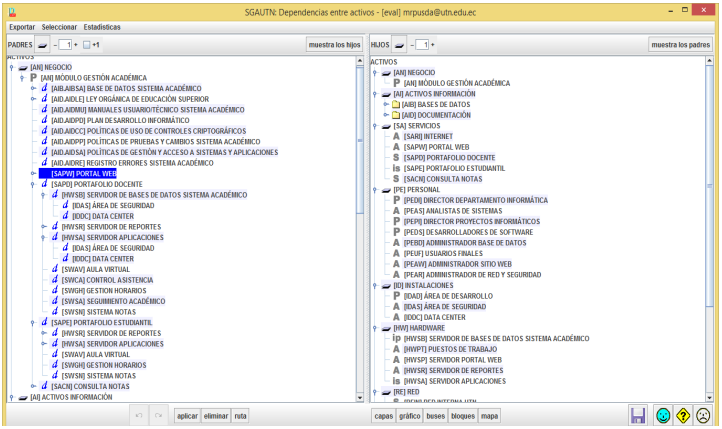


Figura 28. Dependencias Activos Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

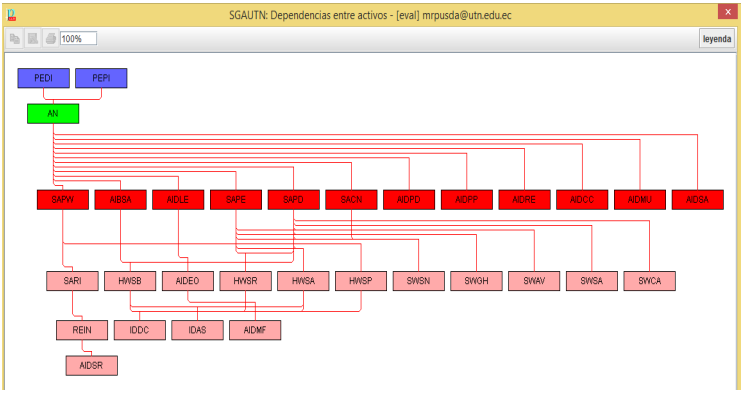


Figura 29. Mapa Dependencias Activos Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

5.5 Valoración de Activos

Criterios de valoración entre activos

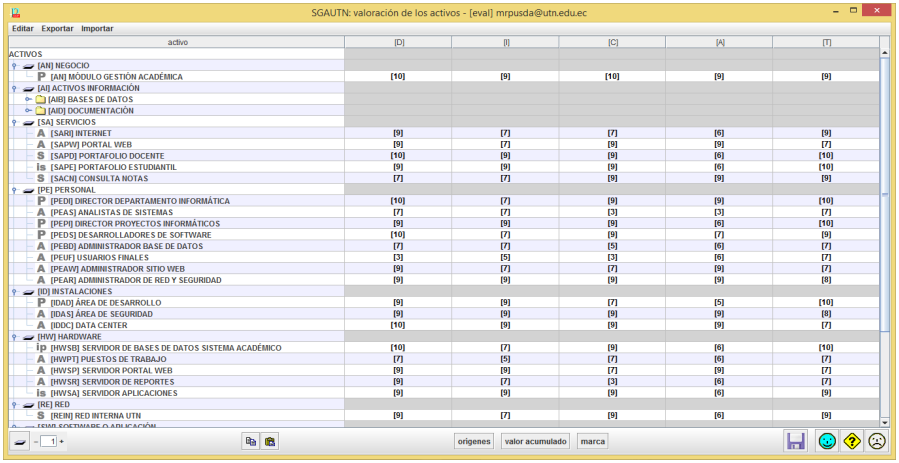


Figura 30. Valoración Activos Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

5.6 Identificación de Amenazas

Recomendaciones de Pilar asociadas a cada uno de los Activos

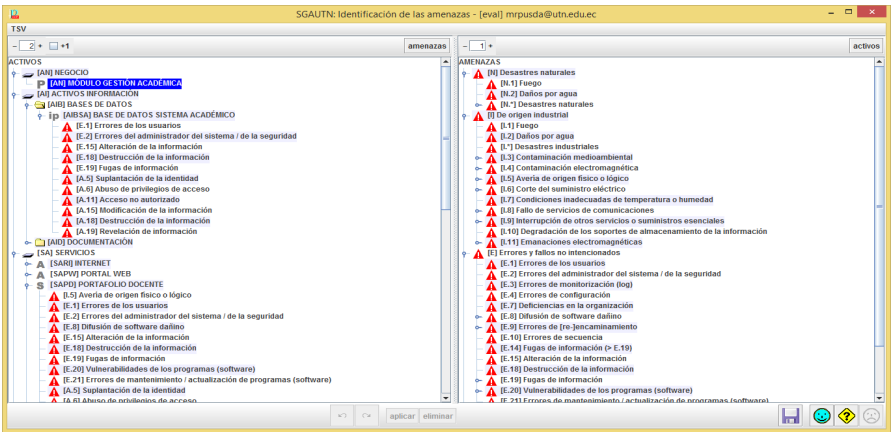


Figura 31. Amenazas Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

5.7 Valoración de Amenazas

Porcentajes de valoración recomendados por Pilar para los Activos

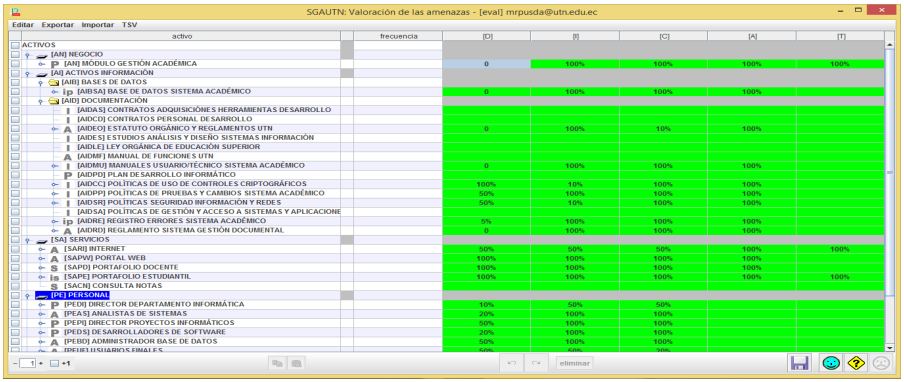


Figura 32. Valoración Amenazas Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

5.8 Impacto Acumulado

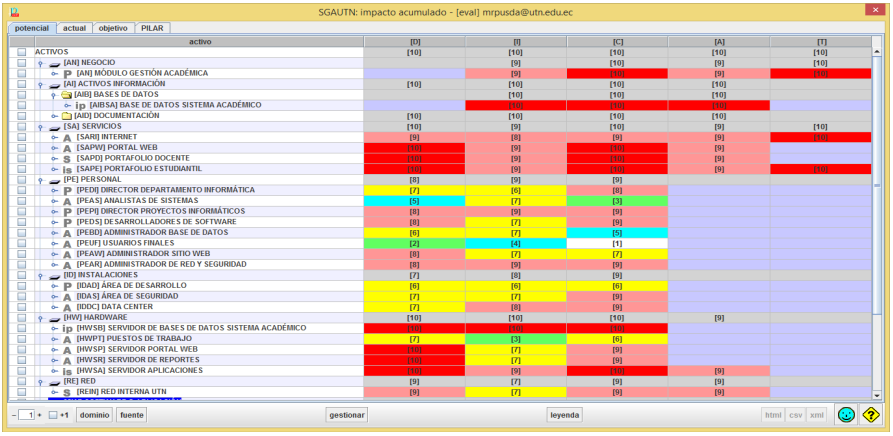


Figura 33. Impacto Acumulado Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

5.9 Riesgo Acumulado

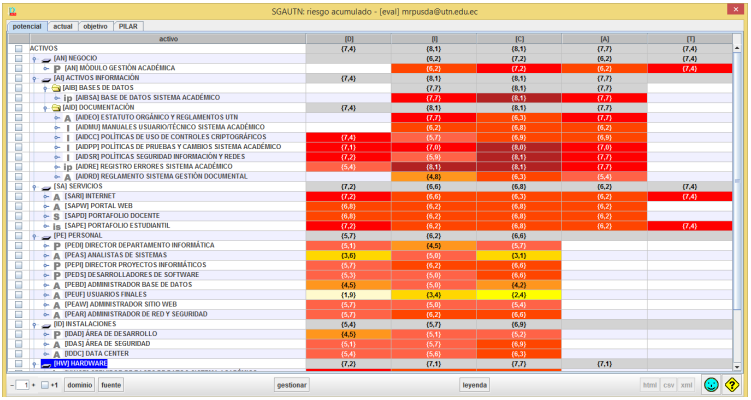


Figura 34. Riesgo Acumulado Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

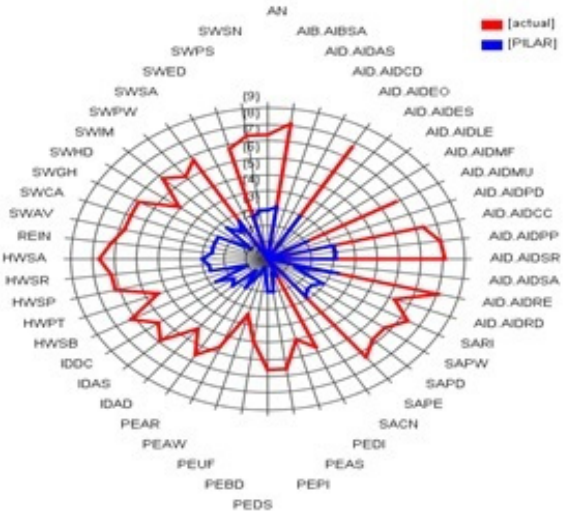


Figura 35. Situación Actual Riesgo Acumulado Módulo Gestión Académica

Fuente: (Imbaquingo Esparza & Pusdá Chulde, 2015)

6 CASO PRÁCTICO - WEKA

En la actualidad, debido a la gran cantidad de información que generamos y almacenamos día a día, el proceso de extracción de información útil requiere la aplicación de técnicas de análisis de datos automáticas que sean capaces de procesar grandes volúmenes de información.

Para ello debemos apoyarnos en herramientas tales como la minería de datos la cual se define como el proceso de aplicar metodologías basadas en algoritmos computacionales, conceptos estadísticos y de administración para extraer conocimiento útil de grandes volúmenes de información.

El paquete Weka contiene una colección de herramientas de visualización y algoritmos para análisis de datos y modelado predictivo, unidos a una interfaz gráfica de usuario para acceder fácilmente a sus funcionalidades. La versión original de Weka fue un front-end en TCL/TK para modelar algoritmos implementados en otros lenguajes de programación, más unas utilidades para pre procesamiento de datos desarrolladas en C para hacer experimentos de aprendizaje automático. Esta versión original se diseñó inicialmente como herramienta para analizar datos procedentes del dominio de la agricultura, pero la versión más reciente basada en Java (WEKA 3), que empezó a desarrollarse en 1997, se utiliza en muchas y muy

diferentes áreas, en particular con finalidades docentes y de investigación.

6.1 Utilización de la herramienta Weka

La herramienta Weka, está constituido por una serie de paquetes de código abierto con diferentes técnicas de pre-procesado, clasificación, agrupamiento, asociación, y visualización, de los datos, y para el desarrollo de esta investigación se trabajó con el diagnóstico realizado a los docentes y estudiantes de las Facultades de la Universidad Técnica del Norte, que fueron analizados con los algoritmos que cuenta la herramienta weka.

Figura 36. Pantalla de inicio herramienta Weka

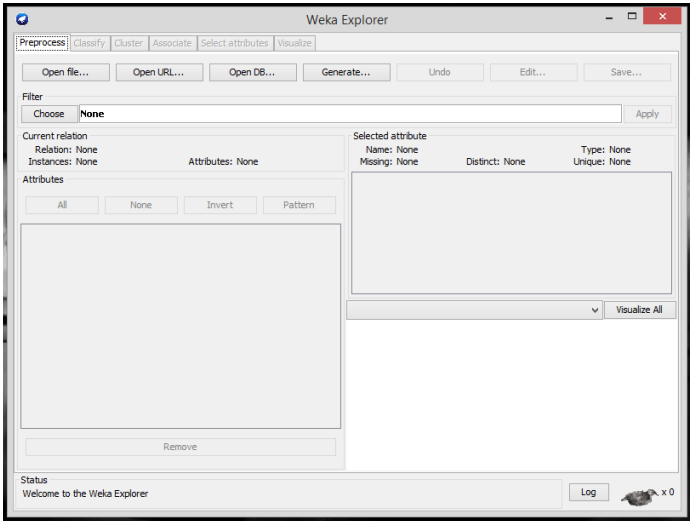


Figura 37. Pantalla para iniciar la carga de datos en Weka

Fuente: (Jácome León, 2016)

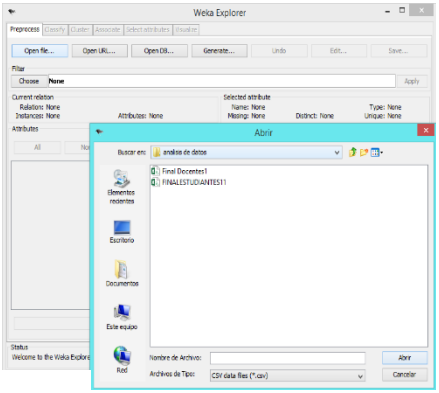


Figura 38. Pantalla para cargar los datos en Weka, Resultados de las encuestas a los Docentes

Fuente: (Jácome León, 2016)

Seleccionar la casilla de identificador para eliminar y luego dirigirse a la pestaña de Classify.

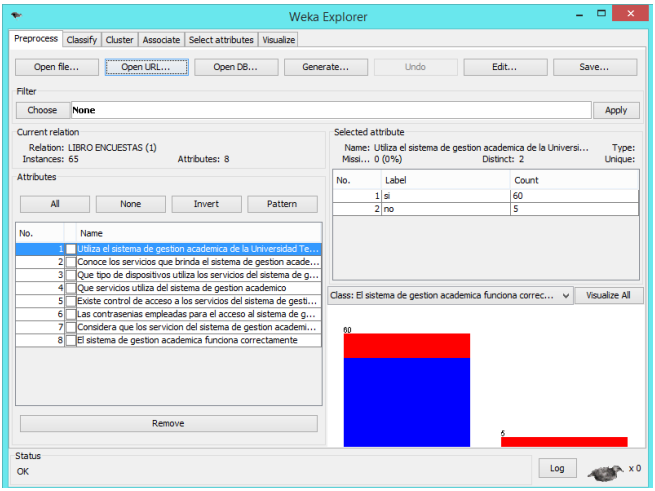


Figura 39. Pantalla de los datos cargados en Weka

Fuente: (Jácome León, 2016)

6.2 Algoritmo J48

El J48 es un algoritmo de aprendizaje que sigue un criterio de partición de las instancias; el espacio de instancias se va partiendo de arriba abajo, utilizando cada vez una partición, es decir, un conjunto de condiciones excluyentes y exhaustivas.

Permite trabajar con valores continuos para los atributos, separando los posibles resultados en dos ramas. Además, permite generar un árbol de decisión a partir de los datos mediante particiones realizadas recursivamente, según la estrategia de profundidad.

Seleccionar el algoritmo J48 y clic en Start.

- ✓ Representa el clasificador como un árbol.
- ✓ Es la implementación en el lenguaje de programación Java, del algoritmo C4.5, (Quinlan, 1993).
- ✓ Puede procesar datos Categóricos y Numéricos.
- ✓ Puede manejar instancias ponderadas por peso.
- ✓ El árbol generado por el algoritmo J48 debe ser aplicado a cada dato en forma secuencial hasta que los mismos caigan dentro de alguna categoría o clase.

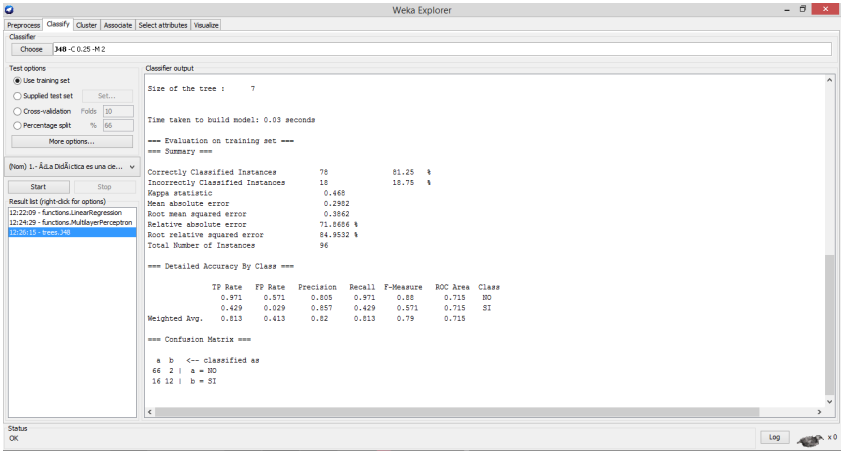


Figura 40. Análisis de datos con el algoritmo J48

Fuente: (Jácome León, 2016)

Ejemplo de análisis de datos Algoritmo J48

Las contraseñas empleadas para el acceso al sistema de gestión académica y sus servicios cuentan con requerimientos de seguridad = si: funciona (45.0)

Las contraseñas empleadas para el acceso al sistema de gestión académica y sus servicios cuentan con requerimientos de seguridad = no: no funciona (20.0/2.0)

Número de hojas: 2

Tamaño del tronco: 3

Tiempo necesario para construir el modelo: 0.01 segundos

Instancias correctamente clasificadas 63 96.9231%

Incorrectamente Clasificado Instancias 2 3.0769%

Estadística Kappa 0.9257

Error absoluto medio 0.0563

Error cuadrático medio 0,1735

Error absoluto relativo 13.9312%

Error relativo cuadrado cuadrado 38.6959%

Número total de instancias 65

=== Confusion Matrix ===

a b <-- clasificado como

45 2 | a = funciona

0 18 | b = no funciona

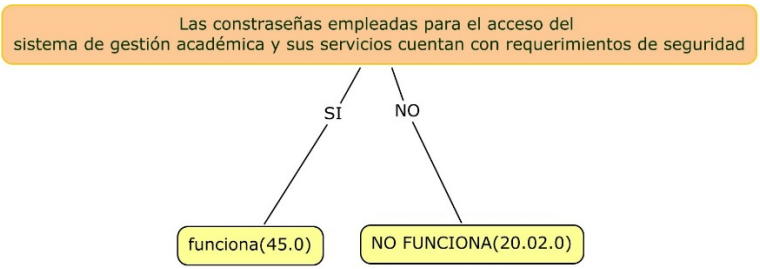


Figura 41. Resultado del Algoritmo J48 sobre la calidad del sistema Académico

Fuente: (Jácome León, 2016)

6.3 Algoritmo KMeans

Es un método de agrupamiento, que tiene como objetivo la partición de un conjunto de n observaciones en k grupos en el que cada observación pertenece al grupo cuyo valor medio es más cercano. Es un método utilizado en minería de datos.

Ejemplo

Número de iteraciones: 3

Dentro de la suma del grupo de errores al cuadrado: 71.0

Valores perdidos globalmente reemplazados por medio / modo

Centígrados de agrupamiento:

Atributo

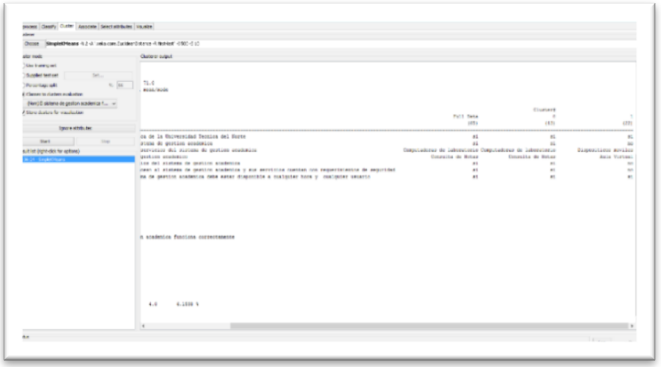


Figura 42. Características de los atributos

Fuente: (Jácome León, 2016)

Instancias agrupadas:

0 43 (66%)

1 22 (34%)

Atributo de clase: El sistema de gestión académica funciona correctamente

Clases a Clusters:

0 1 <- asignado a cluster

43 4 | Funciona

0 18 | No funciona

Clúster 0 <- funciona

Clúster 1 <- no funciona

Instancias de clúster incorrectamente: 4.0 6.1538%

A priori

Utilizado en minería de datos, sobre bases de datos transaccionales, que permite encontrar de forma eficiente "conjuntos de ítems frecuentes", los cuales sirven de base para generar reglas de asociación.

Generación de reglas.

Ejemplo

Soporte mínimo: 0,7 (45 casos)

Mínimo métrico <confianza>: 0,9

Número de ciclos realizados: 6

Conjuntos generados de grandes conjuntos de artículos:

Tamaño del conjunto de grandes conjuntos de artículos L (1): 4

Tamaño del conjunto de grandes conjuntos de artículos L (2): 6

Tamaño del conjunto de grandes conjuntos de artículos L (3): 4

Tamaño del conjunto de grandes conjuntos de artículos L (4): 1

Mejores reglas encontradas:

1. Considera que los servicios del sistema de gestión académica deben estar disponible a cualquier hora y cualquier usuario=si 60 ==>

Utiliza el sistema de gestión académica de la Universidad Técnica del Norte=si 60 conf:(1)

2. Utiliza el sistema de gestión académica de la Universidad Técnica del Norte=si 60 ==> Considera que los servicios del sistema de gestión académica deben estar disponible a cualquier hora y cualquier usuario=si 60 conf:(1)

3. El sistema de gestión académica funciona correctamente=funciona 47 ==> Utiliza el sistema de gestión académica de la Universidad Técnica del Norte=si 47 conf:(1)

4. El sistema de gestión académica funciona correctamente=funciona 47 ==> Considera que los servicios del sistema de gestión académica deben estar disponible a cualquier hora y cualquier usuario=si 47 conf:(1)

5. Considera que los servicios del sistema de gestión académica deben estar disponible a cualquier hora y cualquier usuario=si El sistema de gestión académica funciona correctamente=funciona 47 ==> Utiliza el sistema de gestión académica de la Universidad Técnica del Norte=si 47 conf:(1)

7 REFERENCIAS

Abogacía Española - Incibe. (2016). Gestión de Riesgos. *Incibe*. Retrieved from http://www.abogacia.es/wp-content/uploads/2016/03/ABOGACIA-riesgos-ebook-ok.pdf

AGESIC. (2017). Estadística de incidentes CERTuy 2016. Retrieved March 27, 2017, from https://www.agesic.gub.uy/innovaportal/v/6096/1/agesic/estadistica-de-incidentes-certuy-2016.html

Álvarez Marañon, G., & Pérez García, P. P. (2004). *Seguridad Informática* (1st ed.). McGraw-Hill.

Cano, J. J. (2011). La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes. Retrieved March 27, 2017, from https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx

CCN-CERT-Libro I. (2012). *Magerit Versión 3.0 - Método* (Vol. I).

CCN-CERT-Libro II. (2012). *Magerit Versión 3.0 - Catálogo*. Retrieved from http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

CCN-CERT-Libro III. (2012). *MAGERIT Versión 3.0 - Guía de Técnicas*. Retrieved from http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area descargas/Libro-III-Guia-de-Tecnicas.pdf?idIniciativa=184&idElemento=87&idioma=en

Cuenca, D. L., Javier, L., & Villalba, G. (2011). Análisis de Riesgos Dinámicos en Sistemas de Información. Retrieved from http://eprints.ucm.es/16931/1/PFM_2012_-_David_López_Cuenca_-_Análisis_de_Riesgos_Dinámicos_en_Sistemas_de_Información.pdf

Echenique García, J. A. (2012). *Auditoría en Informática* (2nd ed.). México: McGraw-Hill.

García Pagan, J. J. (2007). Seguridad en redes corporativas. *Interfaces*, 17–34.

González Trejo, D. (2013). ISO-27001:2013 ¿Qué hay de nuevo? | Magazcitum. Retrieved March 27, 2017, from http://www.magazcitum.com.mx/?p=2397#.WNkwevnhDIX

Imbaquingo Esparza, D. E., & Pusdá Chulde, M. R. (2015). EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL MÓDULO DE GESTIÓN ACADÉMICA - SISTEMA INFORMÁTICO INTEGRADO UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA DEL NORTE, APLICANDO ISO 27000. Universidad de las Fuerzas Armadas - ESPE.

INTECO. (2014). Implantación de un SGSI en la empresa. Retrieved from https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO 27000 Español. (2012). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved March 23, 2017, from http://iso27000.es/iso27002.html

Jácome León, J. G. (2016). *MINERÍA DE DATOS PARA PROPONER UN MODELO DIDÁCTICO ESTRUCTURAL DE APRENDIZAJE EN LA FACULTAD CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE*. Universidad de las Fuerzas Armadas - ESPE.

Mazzinghi, J. H. (2011). Gestión del riesgo en la seguridad informática, 1–11. Retrieved from https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

Medina-García, V. (2016). PERSPECTIVAS SOBRE LOS RIESGOS DE TI CAMBIOS EN EL PANORAMA DE LOS RIESGOS DE TI EL PORQUÉ Y EL CÓMO DE LA ACTUAL ADMINISTRACIÓN DE RIESGOS DE TI. - ppt descargar. Retrieved March 22, 2017, from http://slideplayer.es/slide/5543671/

Muñoz Razo, C. (2012). *Auditoría en Sistemas Computacionales* (1st

ed.). México: Prentice Hall.
Piattini, M., & Del Peso, E. (2011). *Auditoria Informática - Un enfoque práctico* (2nd ed.). Afaomega Ra-Ma. Retrieved from www.FreeLibros.me
SEGU.INFO. (2015). Seguridad Informatica / Seguridad Lógica - Identificación y Autentificación. Retrieved March 27, 2017, from http://www.segu-info.com.ar/logica/identificacion.htm
Suarez Sierra, L. P., & Amaya Tarazola, C. A. (2013). Sistema de Gestión de la Seguridad de la información SGSI.
SYMANTEC. (2016). Informe sobre las amenazas para la seguridad en Internet de 2016 | Symantec MX. Retrieved March 27, 2017, from https://www.symantec.com/es/mx/security-center/threat-report
UNIT, I. U. de N. T. (2015). UNIT - UNIT-ISO/IEC 27000. Retrieved March 27, 2017, from http://www.unit.org.uy/normalizacion/sistema/27000/
Universidad Internacional de Valencia. (2016). Conceptos sobre seguridad lógica informática - VIU – Tu Universidad Online | Grados y Másteres Online. Retrieved March 27, 2017, from http://www.viu.es/conceptos-seguridad-logica-informatica/

Daisy Elizabeth Imbaquingo Esparza

Magister en Evaluación y Auditoría de Sistemas Tecnológicos por Universidad de las Fuerzas Armadas –ESPE (2015). Ingeniera en Sistemas Informáticos y Computacionales por la Universidad Técnica del Norte (2007). Diplomado en Investigación y Dirección de Tesis por la Universidad Técnica del Norte (2009). Certificación Cobit 5.0 por APMG-Internacional (2015). Docente Investigador de la Universidad Técnica del Norte- Facultad de Ingeniería en Ciencias Aplicadas. Instructora Academia CISCO – UTN y YACHAY EP.

Marco Remigio Pusdá Chulde

Magister en Evaluación y Auditoría de Sistemas Tecnológicos por Universidad de las Fuerzas Armadas – ESPE (2015). Magister en Administración de Negocios por la Universidad Técnica del Norte (2013). Ingeniero en Sistemas Computacionales por la Universidad Técnica del Norte (2003). Certificación Cobit 5.0 por APMG-Internacional (2015). Docente Investigador de la Universidad Técnica del Norte Facultad de Ingeniería en Ciencias Aplicadas. Instructor Academia CISCO - UTN

José Guillermo Jácome León

Magister en Gestión de Sistemas de Información e Inteligencia de Negocios por Universidad de las Fuerzas Armadas – ESPE(2017) Ingeniero en Sistemas Computacionales por la Universidad Técnica del Norte (2009). QoA del Banco Centra del Ecuador, Departamento de Sistemas. Docente Investigador de la Universidad Técnica del Norte Facultad Ciencias Administrativas y Económicas

EDITORIAL UTN
IBARRA - ECUADOR

ISBN: 978-9942-984-18-0
9 789942 984180