Auditoría de Seguridad Informática

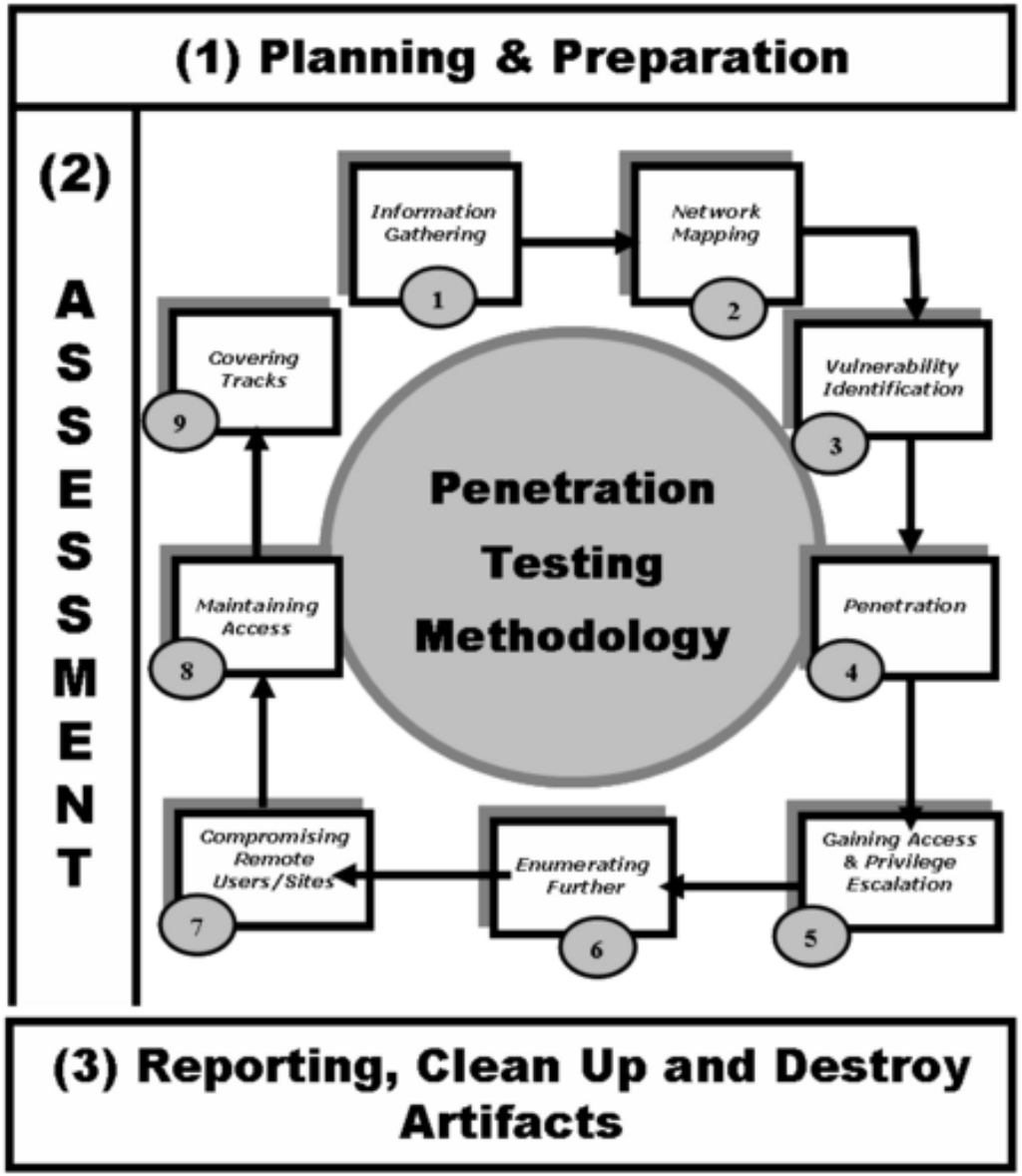
PhD. Félix Oscar Fernández Peña

OSSTMM

- ¿Descubrimiento o Verificación? → Principio la auditoría informática basada en OSSTMM para la verificación del cumplimiento de las normas de seguridad.
- Manual de pruebas de seguridad que genera hechos verificados.
- Metodología formal.

Busca mejorar la seguridad operacional

Approach & Methodology



INCIDENTES REALES
DE SEGURIDAD INFORMÁTICA

Denegación de Servicio

Una empresa de ventas minoristas fue atacada por un intruso que impidió la continuidad del negocio en sus casi 120 sucursales.

En un análisis preliminar de la situación se determinó que un intruso había dejado un programa que se ejecutó el día viernes a las 19:00hs que bloqueaba el acceso al sistema de Ventas.

Se comenzó a trabajar en dos líneas:

- Volver a la operación normal.
- Detección, análisis y rastreo del intruso.

Denegación de Servicio

Metodología de Investigación:

En relación a la vuelta a la operación normal:

1. Análisis forense inmediato de los equipos afectados.
2. Detección de programas que impedían el normal funcionamiento del Sistema de Ventas.
3. Análisis de programas y modificaciones realizadas por el intruso.
4. Planteo de soluciones.
5. Pruebas sobre una sucursal de los cambios.
6. Aplicación masiva de cambios y vuelta a la operación normal.

Denegación de Servicio

Metodología de investigación:

En relación a la detección, análisis y rastreo del intruso:

1. Ingeniería inversa de los programas que dejó el intruso.
2. Determinación de las actividades que realizó el intruso.
3. Detección de rastros (logs) de 4 días antes.
4. Determinación del perfil del intruso.
5. Análisis de los sistemas de acceso remoto.
6. Evaluación de las computadoras personales de los potenciales sospechosos.

Denegación de Servicio

Metodología de Investigación:

7. En el equipo de José se detectaron varios elementos (repetición del patrón de comportamiento del intruso por la forma en que ejecutaba los comandos).

8. Se detectó que otra computadora, que se encontraba al lado del equipo de José, misteriosamente fue formateada y re-instalada dos días después del incidente.

Denegación de Servicio

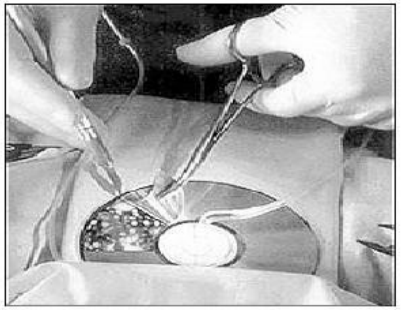
Se detectó la intrusión y se volvió la operación normal en el plazo inmediato.

De acuerdo a las características detectadas del patrón de comportamiento, información encontrada, re-instalación de un equipo, conocimiento de las claves de acceso necesarias, existe una gran probabilidad de que el intruso fuera José.

Extorsión

Un intruso extorsionaba a una Empresa exigiendo dinero a cambio de no hacer circular entre los Clientes de la misma información confidencial que había obtenido.

El intruso se comunicaba a través de mensajes de correo electrónico y en dos oportunidades envió documentos de Word escritos por él.



Extorsión

1. Se analizaron los mensajes de correo electrónico enviados por el intruso y se determinó que venían de Cybers.

2. Se analizaron los documentos de Word con herramientas para análisis a nivel binario y se obtuvo información sobre nombres de archivos internos, fechas de creación, unidades donde fue copiado (aparecía el directorio donde fue almacenado el fichero).

Extorsión

3. Se analizó la información de usuario en los metadatos de los ficheros Word enviados por correo electrónico.

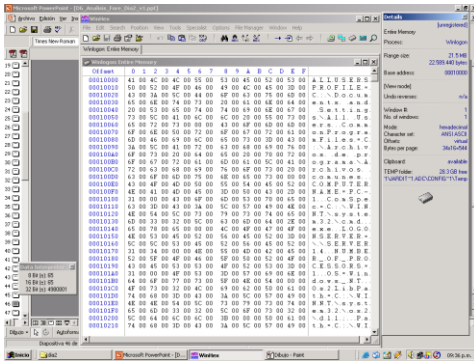
4. Se analizó el nombre del directorio y apareció lo siguiente: C:\Documents and Settings\oalvarez\Mis documentos\

5. Una de las personas que habían desvinculado de mala manera unos meses antes era “Omar Alvarez”.

Extorsión

Resultados obtenidos:

Se logró determinar que el intruso fue Omar Álvarez.



Modificación de Información

- Un intruso ingresó en la Base de Datos de personal y ejecutó un script.
- Aumentó el sueldo en un 70% a todo el personal el día 31 de Julio de 2005.
- Un día después, el sistema de gestión de pagos, generó las órdenes de pago.
- Se comenzó la investigación analizando el Servidor de Producción de Personal.

Modificación de Información

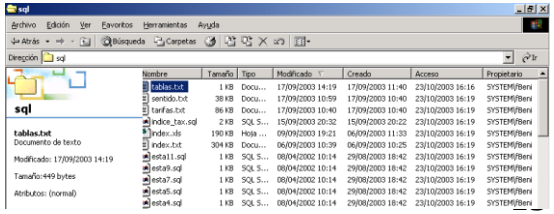
Metodología de Investigación:

1. Análisis del Servidor UNIX de Producción que contiene la Base de Datos.

2. Detección en el directorio principal del usuario María, lo que parecía ser el script SQL que se había ejecutado.

3. Restricción de las PC's de los usuarios que accedieron en ese momento.

4. Evaluación de 9 PC's de los usuarios buscando archivos creados, modificados y accedidos el día del incidente.



Modificación de Información

Metodología de Investigación:

5. Se detectó un solo equipo que tenía archivos relevantes, el del usuario Pedro. Se detectó dentro del directorio C:\temp, un archivo que contenía parte del script detectado en el directorio del usuario Maria. Ese archivo fue generado por la herramienta SQLPlus.
6. Se analizaron las conexiones al Servidor UNIX de Producción el día del incidente y se detectó que el usuario María había entrado desde el Servidor de Desarrollo y tuvo una sesión abierta de 3 horas.
7. Se investigó el Servidor de Desarrollo y se detectó que unos minutos antes de conectarse el usuario María al UNIX de Producción, el usuario Pedro había entrado a Desarrollo desde su PC.

Modificación de Información

Metodología de Investigación:

8. Se buscó en los registros de la cámara de vigilancia de la entrada del edificio y María se había retirado 1 hora antes del incidente.

Resultado Obtenido:

Se determinó que el intruso fue Pedro y que trató de incriminar al usuario María.

Adrian Bridgwater
June 28, 2016

Malware spawns botnet in 25,000 connected CCTV cameras

This article originally appeared on SC Magazine UK.

Share this content:

Tens of thousands of security cameras are the newest recruits to an DDoS botnet, noted for its powerful and unrelenting attacks

Could the so-called Internet of Things go bad, really bad? Could a globally connected network of CCTVs become infected with a strain of malware that results in a botnet swarming across as many as 25,000 malware-riddled CCTV cameras?


Often hackers will use anything with an IP address to add to the ranks of their botnet, even IoT devices.

American website security and web application firewall (WAF) specialist Sucuri thinks that this scenario is plausible because it has already happened. The Delaware-headquartered firm said it found the CCTV botnet during analysis it carried out in relation to an online assault against a 'bricks & mortar' jewelry store.

Layer 7-tsunami

The shop contacted Sucuri to help protect their site from a DDoS attack which had crippled its operations. Upon switching the customer's DNS to the Sucuri Network, researchers found a Layer 7 attack (HTTP Flood) generating close to 35,000 HTTP requests per second (RPS), more than the shop's web servers could handle.

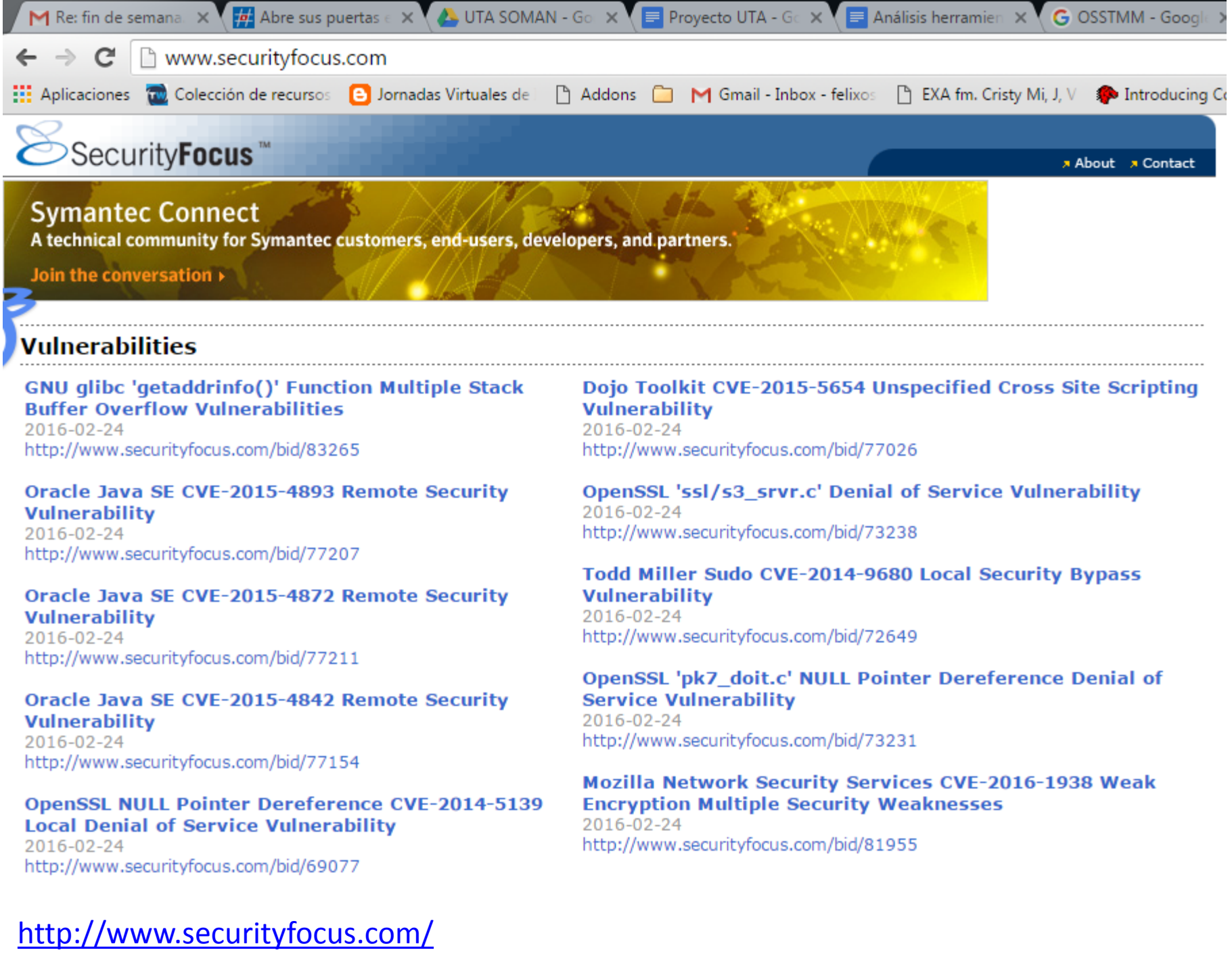
According to Sucuri's own account of events, "normally, this would be the end of the story. The attack would be mitigated, the attackers would move on after a few hours and the website owner would be happy. In this

SC MAGAZINE ARTICLES

Popular | Emailed | Recent

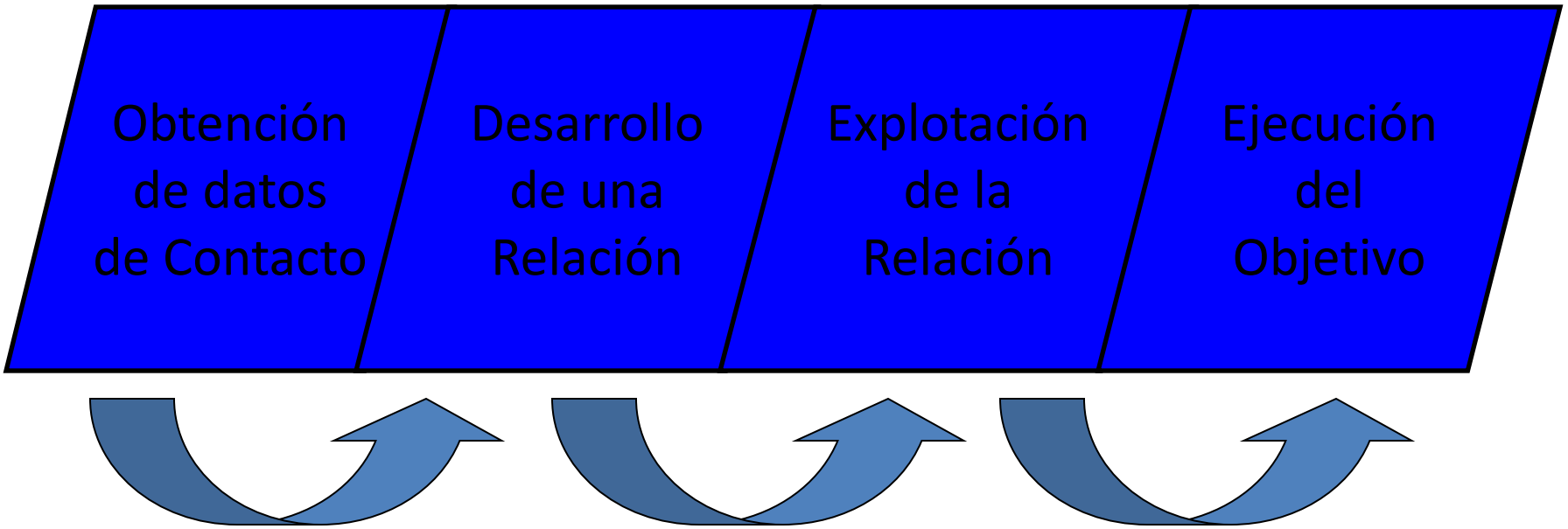
- Microsoft Office 365 hit with massive Cerber

http://www.scmagazine.com/malware-spawns-botnet-in-25000-connected-cctv-cameras/article/505945/



http://www.securityfocus.com/

Metodología de Ataque de Ing. Social



Estrategias de Defensa ante Ing. Social

- Educación y concientización.
- Políticas de seguridad informática.
- Sanciones duras y concretas.

Medidas de Seguridad a Validar

- No revelar contraseñas.
- Destruir documentos que se desechan y puedan contener información confidencial.
- No colocar contraseñas en lugares públicos.
- Denunciar correos electrónicos y otras notificaciones sospechosas.
- Denunciar la presencia de personas foráneas a la empresa.
- Proteger información confidencial impresa.

Tipos de Ataques

- Back Doors
- Brute Force
- Buffer Overflow
- Denial-of-service (DoS)
- IP Scan and Attack
- Mail-bombing
- Man-in-the-Middle
- Password Crack
- Simple Network Management Protocol
- Sniffers
- Social Engineering
- Spam
- Spoofing
- Timing Attack
- Unprotected Shares
- Virus, Worm, Trojan
- Web Browsing

Normas de Seguridad Informática

- Responsabilidades.
- Tratamiento de la Información.
- Administración de usuarios.
- Administración de recursos informáticos.
- Seguridad personal.
- Seguridad física.
- Seguridad en comunicaciones.
- Correo electrónico e internet.
- Desarrollo de software.
- Antivirus.
- Detección y rastreo de intrusos.

ISO 27002

http://iso-17799.safemode.org/

Convenios de Confidencialidad

- Firmados por todo el personal de la Organización y por terceros involucrados con esta.
- Restricciones para la distribución de la información de la organización.
- Política de terminación de un contrato de trabajo.
  - Cómo manejar la partida de un empleado.
  - El cierre de las cuentas de usuario.
  - Políticias para el reenvío del Correo Electrónico y el Buzón de voz.
  - Cambios de contraseñas en los sistemas.

Conclusiones

- Los estándares ISO-27001 e ISO-27002 y su relevancia en el mundo de la auditoría informática.
- Los requisitos de la auditoría informática variarán en función del contexto en que se lleve a cabo.
- La auditoría informática conlleva un estudio profundo de las condiciones de la entidad en la que se lleva a cabo.