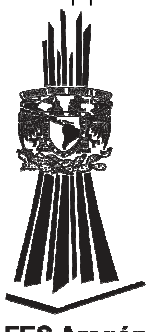
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

PREVENCIÓN DE INTRUSIONES Y ROBO DE INFORMACIÓN POR MEDIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

T R A B A J O E S C R I T O
EN LA MODALIDAD DE DESARROLLO DE UN CASO PRÁCTICO PARA OBTENER EL TÍTULO DE:
I N G E N I E R O E N C O M P U T A C I Ó N
P R E S E N T A :

BEATRIZ RODRIGUEZ COVARRUBIAS



FES Aragón

ASESORA: MTRA. SILVIA VEGA MUYTOY

MÉXICO, 2012.

INTRODUCCIÓN

Debido a la cantidad de información que se genera actualmente y que la gran mayoría es de carácter confidencial es necesario contar con los medios suficientes para mantenerla lejos del alcance de personas no autorizadas así como una adecuada configuración y administración de los equipos de cómputo donde es alojada. Por tal motivo es prudente realizar Análisis de Vulnerabilidades y Pruebas de Penetración frecuentemente que ayuden a las empresas, compañías, instituciones o dependencias a mantener su información integra y confidencial.

Además es importante seguir las recomendaciones emitidas en base a norma de seguridad ISO27001 a fin de reducir riesgos potenciales de intrusión así como el nivel de Impacto dentro del Hospital. Esto permitirá a las empresas acercarse gradualmente a la aplicación de mejores prácticas y a la posibilidad de que pueda obtener alguna certificación de acuerdo a la norma mencionada según lo requieran.

En el capitulo uno se describe la situación inicial del Hospital y los factores que determinan la realización de Análisis de Vulnerabilidades y Pruebas de Penetración con una diferencia de 6 meses durante 3 años.

En el capitulo dos se describen las metodologías utilizadas para los Análisis de Vulnerabilidades y Pruebas de Penetración, así como los vectores de ataque que se siguieron para obtener información confidencial, cuentas de correo electrónico, cuentas de administradores de red, servidores y aplicaciones.

En el tercer y último capítulo se detallan los hallazgos de los Análisis de Vulnerabilidades y Pruebas de Penetración, así como la evaluación del impacto, las recomendaciones y controles de seguridad sugeridos para corregir los puntos vulnerables en la infraestructura de red.

CAPITULO I

ANTECEDENTES

1. ANTECEDENTES

La seguridad desde tiempos inmemorables ha sido un tema ampliamente tratado, en aquellos lejanos tiempos la información más importante eran planes de guerra y expansión. Con el tiempo y los avances tecnológicos la información que hay que asegurar va desde una investigación científica y tecnológica, una innovación empresarial, o bien una base de datos de clientes con cualquier tipo de información, personal, financiera, o de salud.

La infraestructura computacional de una institución es una parte fundamental para el almacenamiento y gestión de la información, y actualmente es de suma importancia para el óptimo funcionamiento de la organización no importando cual sea el tipo de servicio que presta. De tal manera, que si del manejo eficiente de la información depende en gran medida el prestigio y eficiencia de la misma, los dueños de la infraestructura informática tienen que buscar los medios e instrumentos necesarios para garantizarla.

La función de la seguridad informática es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas técnicas o humanas, planes de robos, virus, incendios, intrusiones, boicot, desastres naturales o cualquier otro factor que atente contra la infraestructura informática.

Por otro lado, a cualquier institución le es de suma importancia la protección de la información que se genera en la misma y la que tiene que ver directamente con sus clientes, por lo que es prioritario buscar los procedimientos y herramientas necesarias para asegurar por cualquier medio tener el sistema de información lo más confiable posible. Las personas que se encargan de la estructura tecnológica, de las comunicaciones y que gestionan la información, deberán tener procedimientos específicos que aseguren a la organización el buen manejo de la información.

Las instituciones deberán establecer políticas bien definidas de seguridad informática donde se establezcan normas que minimicen los riesgos a la información o infraestructura informática. De acuerdo a la organización, dichas normas pueden incluir restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad minimizando al máximo el impacto en el desempeño de los funcionarios y de la organización en general.

Los sistemas informáticos son ampliamente utilizados en cualquier tipo de organización, desde una institución educativa, una de servicio bancario o una de transformación o producción de alimentos, así como en el sector salud. Y en todas ellas es indispensable tener las mejores prácticas de seguridad de la información.

El caso práctico que se desarrolla en este trabajo está enfocado al análisis de seguridad de la información y las buenas prácticas en este sentido de una Institución de Salud que para fines de este escrito será denominado como Hospital.

El Hospital de este trabajo ofrece servicios como Centro de Trasplantes, Centro de Nutrición, Obesidad y Alteraciones Metabólicas, Clínica de Nutrición, Medicina Preventiva, Cirugía Plástica y Reconstructiva, Centro Cardiovascular, Banco de Sangre, Urgencias, entre otros. Para otorgar dichos servicios el Hospital utiliza recursos de red, cómputo, servidores y diversas aplicaciones para análisis clínicos, administración de pacientes, expedientes médicos, administración de quirófanos y control de medicamentos. Por tanto es importante que todos los equipos funcionen adecuadamente y cumplan con controles de seguridad necesarios para el resguardo de los datos de pacientes y expedientes médicos. Para realizar dicha actividad ciertas instituciones cuentan con todo un departamento que se encargue de todos los aspectos informáticos que necesite la organización. Pero para una gran mayoría de empresas tener que realizar o tener un área que se encargue de dichos aspectos es muy complicado por el tipo de servicio que prestan y prefieren que consultorías o empresas externas se encarguen de realizar todo lo relativo a lo de sistemas informáticos.

Anteriormente el Hospital contaba con varios administradores de Sistemas, Redes y Servidores bajo un esquema de Outsourcing y el personal interno del área de Sistemas de Cómputo era muy reducido y no contaban con los conocimientos necesarios para poder controlar las actividades de los proveedores. Por tal motivo era muy probable que se registraran fugas de información confidencial o mal uso de los recursos.

A fin de comprobar actividades ilícitas dentro del Hospital se decide realizar Análisis de Vulnerabilidades y Pruebas de Penetración controladas y de forma totalmente confidencial, es decir sin el conocimiento de los proveedores. De esta forma el personal del Hospital podría comparar los resultados de dichos análisis con los reportes de los proveedores para así determinar la situación actual y real de la infraestructura de red y tomar las medidas necesarias para controlar las actividades de los proveedores y mitigar riesgos potenciales.

Los Análisis de Vulnerabilidades y Pruebas de Penetración están basados en la metodología OSSTMM de ISECOM y la certificación de CEH de EC-Council.

OSSTMM (Open Source Security Testing Methodology Manual) es un manual de metodologías para pruebas y análisis de seguridad publicado bajo licencia Creative Commons 3.0, lo cual permite el libre uso y distribución del mismo. A fin de organizar su contenido, la metodología se encuentra dividida en varias secciones, las cuales son:

- Seguridad de la Información;
- Seguridad de los Procesos;
- Seguridad en las tecnologías de Internet;
- Seguridad en las Comunicaciones;
- Seguridad Inalámbrica y
- Seguridad Física.

Segú la metodología para realizar un análisis apropiado de cualquier sección debe incluir los elementos de las otras secciones, directa o indirectamente.

CEH (Certified Ethical Hacker) no es precisamente una metodología, es una certificación. La cual es una herramienta que provee a un profesionista de habilidades para encontrar vulnerabilidades en los sistemas. Según el manual de trabajo de esta certificación, un Análisis de Vulnerabilidades y Pruebas de Penetración se realiza en 5 fases, las cuales son:

- Reconocimiento;
- Escaneo;
- Obtener acceso al sistema;
- Mantener el acceso en el sistema y
- Limpiar huellas.

El beneficio que tienen las organizaciones, instituciones o empresas, es que el consultor certificado que presta el servicio de Análisis de Vulnerabilidades y pruebas de penetración cuenta con los mismos conocimientos y herramientas de un un hacker malicioso, con la diferencia de que no interfiere con el trabajo operativo de la institución y notifica los puntos vulnerables para que puedan ser corregidos.

Ahora bien, en el caso del Hospital del trabajo en el siguiente capítulo se desglosa el desarrollo puntual del proceso realizado mediante la metodología mencionada, así como los resultados obtenidos mediante la aplicación para el caso presentado.

CAPITULO II

METODOLOGÍAS DE ANÁLISIS Y PRUEBAS DE PENETRACIÓN

2. METODOLOGÍAS DE ANÁLISIS Y PRUEBAS DE PENETRACIÓN

Los análisis de Vulnerabilidades y Pruebas de Penetración sirven para evaluar el estado de la seguridad en una organización como un todo, este tipo de pruebas ayudan y permiten a los administradores de red, de Sistemas y ejecutivos a revelar las consecuencias de que un atacante tenga acceso a la red interna del Hospital, incluso que alguna persona que trabaje dentro de él llegue a tener acceso a información confidencial de forma indebida. Así mismo, permiten encontrar debilidades que no se descubren con un escaneo de vulnerabilidades común. También se revisan posibles errores en la configuración de los servicios. Las fallas encontradas se evaluadas para medir el impacto de que se lleve a cabo una explotación de dicha vulnerabilidad y así poder generar un proceso de mitigación, un plan de contingencia o eliminar el riesgo por medio de una operación técnica.

Las metodologías ISECOM/OSSTMM y Ec-Council/CEH, pueden ser utilizadas parcial o totalmente dependiendo de los requerimientos de cada cliente.

2.1. OSSTMM (Open Source Security Testing Methodology Manual)

Representa un estándar de referencia imprescindible, para todo aquel que quiera llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional.

A fin de organizar su contenido, la metodología se encuentra dividida en varias secciones. Del mismo modo, es posible identificar en ella, una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión tal como se muestra en el mapa de seguridad de la **Imagen 2.1**

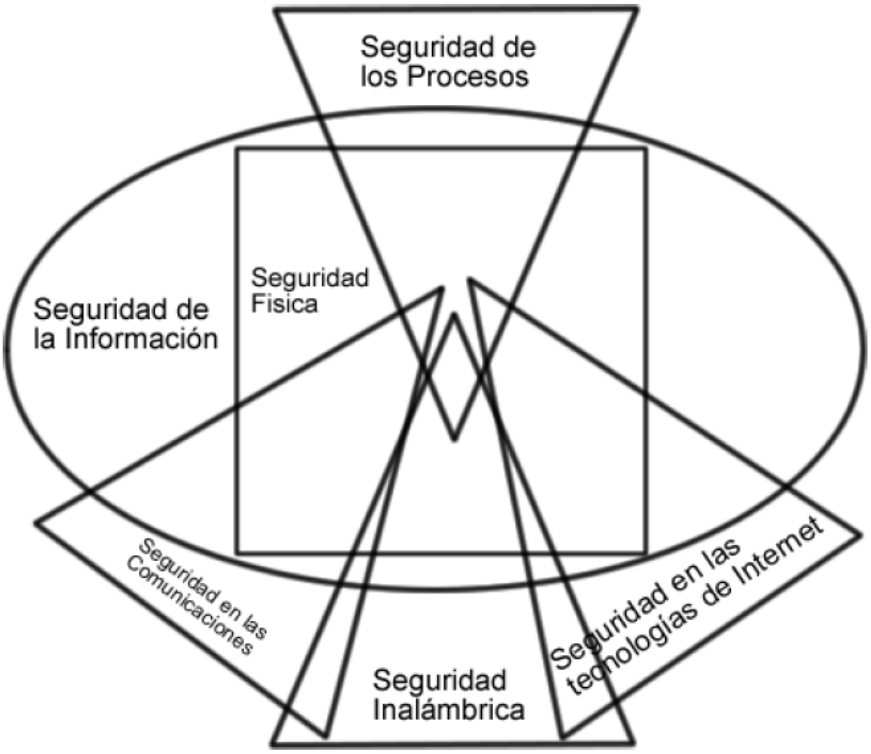


Imagen 2.1. Mapa de Seguridad de Metodología OSSTMM

El mapa de seguridad está compuesto por seis secciones que se superponen entre sí y contienen elementos de las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de las otras secciones, directa o indirectamente.

- Seguridad de la Información (presencia en Internet de cualquier tipo de información de una entidad, Revision de Privacidad, Recolección de Documentos).
- Seguridad de los Procesos (ingeniería social, "suggestion test").
- Seguridad en las tecnologías de Internet (IDS, firewall, router testing, DOS, passwork cracking, etc.).
- Seguridad en las Comunicaciones (Modem, FAX, PBX, etc.).
- Seguridad Inalámbrica (TEMPEST, hacking 802.11, bluetooth, infrarrojos, etc.).
- Seguridad Física (perímetro de seguridad, alarmas de seguridad, test de control de accesos, estudio del entorno, etc.).

OSSTMM no solo alcanza los ámbitos técnicos y de operación de seguridad tradicionales, sino que, se encarga de normar aspectos tales como: las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado, la forma en la que los resultados del mismo deben ser presentados, las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar el test, los tiempos que deberían ser tenidos en cuenta para cada una de las tareas, y por sobre todas las cosas, incorpora el concepto de RAVs (Valores de Evaluación de Riesgo) y con ellos la frecuencia con la cual la prueba debe ser ejecutada a fin de proveer más que una instantánea en el momento de su ejecución.

ISECOM aplica los términos a los diferentes tipos de sistemas y testeos de seguridad de redes, basados en tiempo y costo para el Testeo de Seguridad de Internet, así como se muestra en la **Imagen 2.2**.

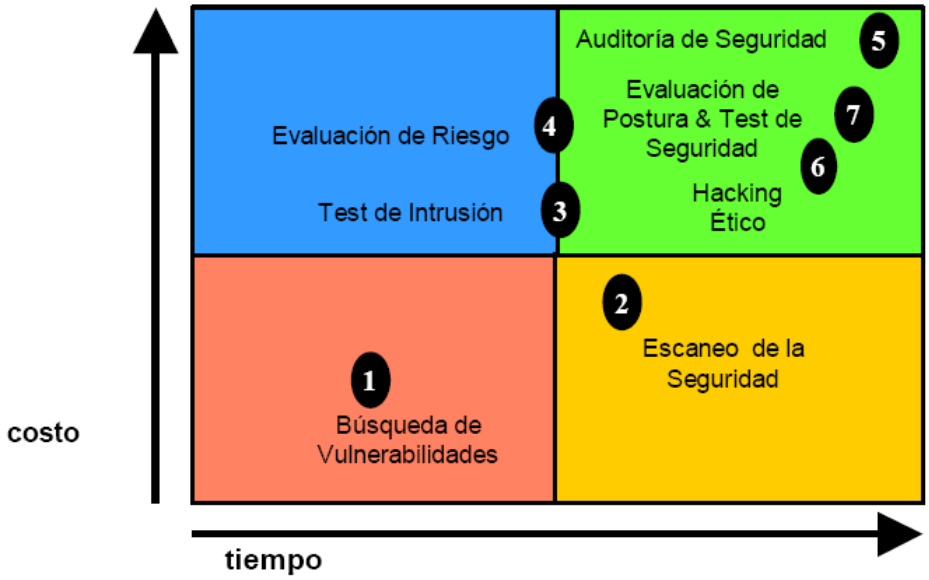


Imagen 2.2. Metodología OSSTMM

1. **Búsqueda de Vulnerabilidades:** se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.
2. **Escaneo de la Seguridad:** se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.
3. **Test de Intrusión:** se refiere en general a ganar acceso privilegiado con medios pre-condicionales.
4. **Evaluación de Riesgo:** se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación de negocios, las justificaciones legales y las justificaciones específicas de la industria.
5. **Auditoría de Seguridad:** hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.
6. **Hacking Ético:** se refiere generalmente a los tests de intrusión en los cuales el objetivo es obtener acceso privilegiado en la red dentro del tiempo predeterminado de duración del proyecto.
7. **Test de Seguridad:** es una evaluación de riesgo con orientación del proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad, donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

2.2. CEH (EC-Council, Certified Ethical Hacker)

CEH (Certified Ethical Hacker) no es precisamente una metodología, es una certificación que provee a un profesionista de habilidades para encontrar vulnerabilidades en los sistemas utilizando el mismo conocimiento y herramientas que un hacker malicioso con la diferencia de que no interfiere con el trabajo operativo y notifica los puntos vulnerables para que puedan ser corregidos. El objetivo del Hacker Ético es ayudar al Hospital a tomar medidas contra ataques maliciosos atacando al sistema mismo; todo dentro de límites legales. Según EC-Council CEH, los Análisis de Vulnerabilidades pueden ser de dos tipos:

- **Análisis de caja negra (Black Box Testing):** En este tipo de análisis no se tiene un conocimiento previo de la infraestructura de los sistemas, es decir que primero se debe determinar aspectos como la topología de la red, versiones de los sistemas operativos, servicios disponibles, etc., con el fin recoger la mayor cantidad de información posible. Esto ayuda a:
  - Conocer el tipo y la calidad de la información que es visible desde Internet.
  - Conocer los posibles puntos de ataque en cada uno de los servicios disponibles.
  - Realizar ataques informáticos desde el punto de vista de un atacante que se encuentre FUERA DE LA ORGANIZACIÓN.
- **Análisis de caja blanca (White Box Testing):** En este tipo de análisis se conoce completamente la infraestructura de los sistemas, diagramas y topología de la red, acceso al código de las aplicaciones, direccionamiento IP, etc. Esto ayuda a:
  - Conocer el nivel de daño que se puede causar a los sistemas IT al poseer dicha información.
  - Medir el nivel de acceso de los usuarios internos.
  - Realizar ataques informáticos desde el punto de vista de un atacante que se encuentre DENTRO DE LA ORGANIZACIÓN.

Las fases de un ataque son 5, se pueden visualizar en la **Imagen 2.3**.

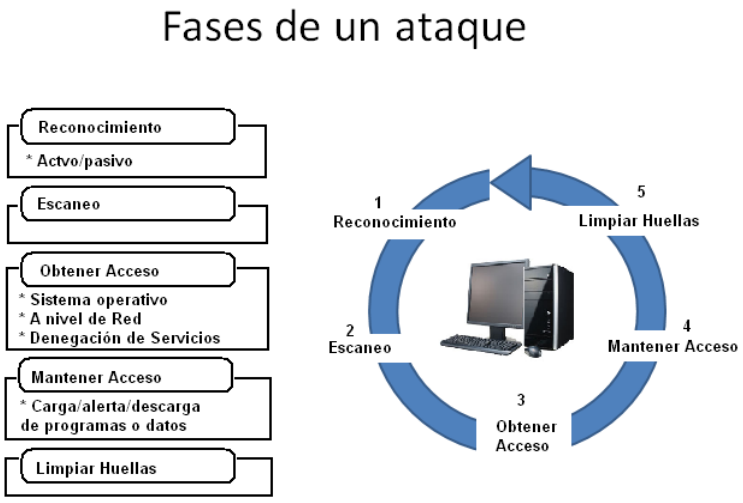


Imagen 2.3. Fases de un ataque según la Metodología CEH

- **Reconocimiento:** Se refiere a la fase preparatoria donde se obtiene la información necesaria de su objetivo o victima antes de lanzar un ataque. Esta fase puede incluir la Ingeniería Social, buscar en la basura (Dumpster diving), buscar los tipos de sistemas operativos y aplicaciones que son usadas por el objetivo o víctima, conocer los puertos que están abiertos, la ubicación de los routers (enrutadores), nombres de dominios, información de contacto, servidores de email y toda la información que se pueda extraer de los DNS (Domain Name Server).
- **Escaneo:** En esta fase se utiliza toda la información que se obtuvo en la Fase del Reconocimiento para identificar vulnerabilidades específicas. También se realiza un escaneo para identificar puertos abiertos y versiones de las aplicaciones que se alojan en el equipo objetivo, con la finalidad de definir el vector de ataque y seleccionar las herramientas que se van a utilizar.
- **Obtener acceso:** Esta es la fase más importante ya que se explotan las vulnerabilidades que se encuentran en la fase de Escaneo para comprometer servidores, dispositivos de red y/o aplicaciones. Se pueden incluir técnicas como buffer overflows (desbordamiento del buffer), denial-of-service (negación de servicios), sesión hijacking (secuestro de sesión), y password cracking (romper o adivinar claves usando varios métodos como: diccionary atack y brute forcé atack).
- **Mantener el acceso:** Después de que se logra tener acceso al sistema, la prioridad es mantener el acceso. En esta fase se usan los recursos del sistema como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas, también se usan programas llamados sniffers para capturar todo el trafico de la red que sea transmitido en texto claro incluyendo sesiones de telnet y FTP (File Transfer Protocol).
- **Limpiar huellas:** En esta fase el atacante limpia toda la evidencia de actividades ilícitas, la razón principal es que puede mantener el acceso y es probable que los administradores no tengan pistas claras de la intrusión, además de que así evita ser detectado por policías cibernéticos.

2.3. Metodología Utilizada por la Consultoría

En base a las metodologías descritas anteriormente, la Consultoría toma parte de ellas y las adapta según el alcance del proyecto y los equipos contemplados en el servicio para hacer un análisis a medida dependiendo de las necesidades del cliente. Así, los pasos a seguir durante un Análisis de Vulnerabilidades y Pruebas de Penetración son los siguientes:

1. Escaneo de Puertos: Para detectar servicios y versiones de Sistema Operativos y aplicaciones.
2. Escaneo de Vulnerabilidades: Para detectar los posibles equipos vulnerables de acuerdo a las versiones de Sistema Operativo y Aplicaciones.
3. Definición de Vectores de ataque: Para explotar Vulnerabilidades y descartar falsos positivos. Dichos vectores pueden contemplar las siguientes secciones, dependiendo de las vulnerabilidades detectadas:
    a. Seguridad de la Información

i. Revisión de Privacidad
ii. Recolección de Documentos
iii. Análisis de Archivos compartidos
iv. Archivos compartidos a través de sesiones nulas
v. Acceso a información de cuentas de correo

b. Seguridad de los Procesos
i. Ingeniería social
ii. Conexiones a servidores con contraseña de Administrador
iii. Carencia de política de cambio de contraseñas
iv. Equipos no actualizados
v. Impresoras sin control de acceso

c. Seguridad en las tecnologías de Internet
i. Enrutamiento
ii. Descifrado de Contraseñas
iii. Testeo de Denegación de Servicios
iv. Evaluación de Políticas de Seguridad
v. Protocolos inseguros
vi. Captura de contraseñas en la red
vii. Contraseñas por default en dispositivos de red
viii. Página Web de la Organización
ix. Contraseñas por default en aplicaciones Web

d. Seguridad en las Comunicaciones
i. Intercepción de comunicaciones telefónicas

e. Seguridad Inalámbrica
i. Conexiones no autorizadas a redes inalámbricas

4. Escalamiento de ataques exitosos.
5. Obtener evidencia de ataques exitosos.
6. Evaluación del Impacto
7. Selección de Controles de Seguridad Preventivos y Correctivos para mitigar los riesgos encontrados.

Las siguientes herramientas se utilizaron durante los Análisis de Vulnerabilidades y Pruebas de Penetración, están agrupadas de acuerdo a su función:

- **Obtener Información inicial de equipos y dominios:** Whois, Dig, Host.
- **Escaneo de la red:** Ping Sweep, Nmap, IPscan, Nessus, Open Vas, Eeye Retina Scanner, Wireshark, Tcpdump, Ethercap.
- **Enumeración de equipos y usuarios en la red:** NetBIOS, NBTScan, Sid2User, User2Sid, Cain & Abel, SNMPEnum.
- **Comprometer equipos:** PWDump, SMBDump.
- **Descifrado de contraseñas de usuarios:** Rainbow Tables, OphtCrack.
- **Ejecución de exploits:** Metasploit
- **Captura de contraseñas en la red por medio de Man in the Middle:** Ettercap, Cain & Abel.
- **Acceso remoto a sistemas:** VNC, Escritorio Remoto, SSH, TeamViewer
- **Obtener clave de redes inalámbricas:** Net Stumbler, Suite de aircrack, Metasploit-Meterpreter

2.3.1. Vectores de ataque

A continuación se describen algunos vectores de ataque con los cuales fue posible tener acceso a la red del Hospital.

2.3.1.1. Acceso a redes inalámbricas

Para tener acceso a redes inalámbricas es necesario realizar un escaneo e identificar cuales están disponibles y qué tipo de cifrado está configurado. Si es cifrado WEP son fácilmente comprometidas. La **Imagen 2.4** muestra un escaneo de las redes disponibles, de las cuales se tomará como objetivo la seleccionada por el recuadro amarillo.

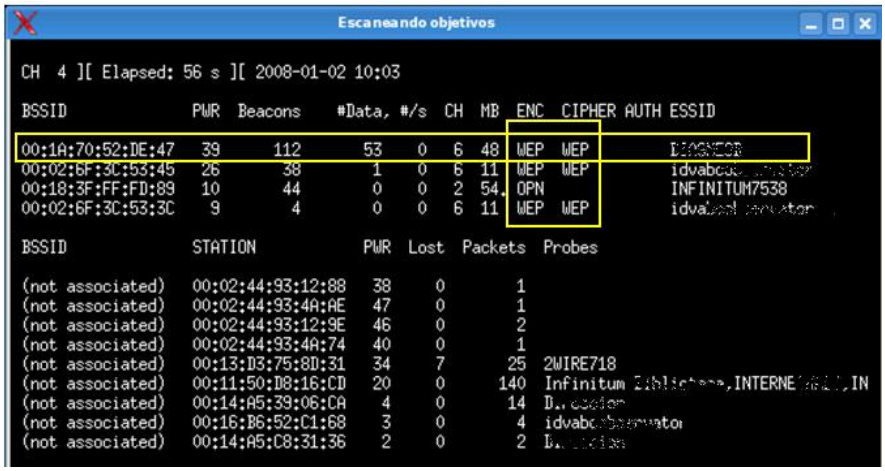


Imagen 2.4. Escaneo de redes inalámbricas

Antes de inyectar paquetes en la red inalámbrica se cambia la MAC de la máquina del atacante a fin de no ser detectada. La **Imagen 2.5**, en el primer recuadro, muestra la MAC atacante 11:22:33:44:55:66 asociada a la MAC del Access Point comprometido que es 00:1A:70:52:DE:47, en el segundo recuadro se muestra la inyección de paquetes para obtener la clave WEP.

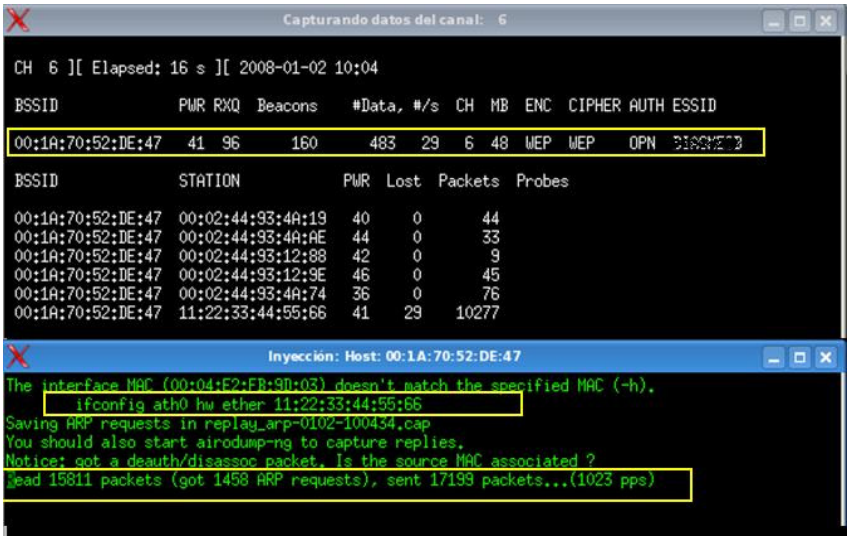


Imagen 2.5. Inyección de paquetes ARP a la red inalámbrica

La **Imagen 2.6** muestra la clave WEP de la red inalámbrica comprometida se necesitaron inyectar 44489 paquetes y el tiempo estimado de descifrado es de 1 hora y 20 min.

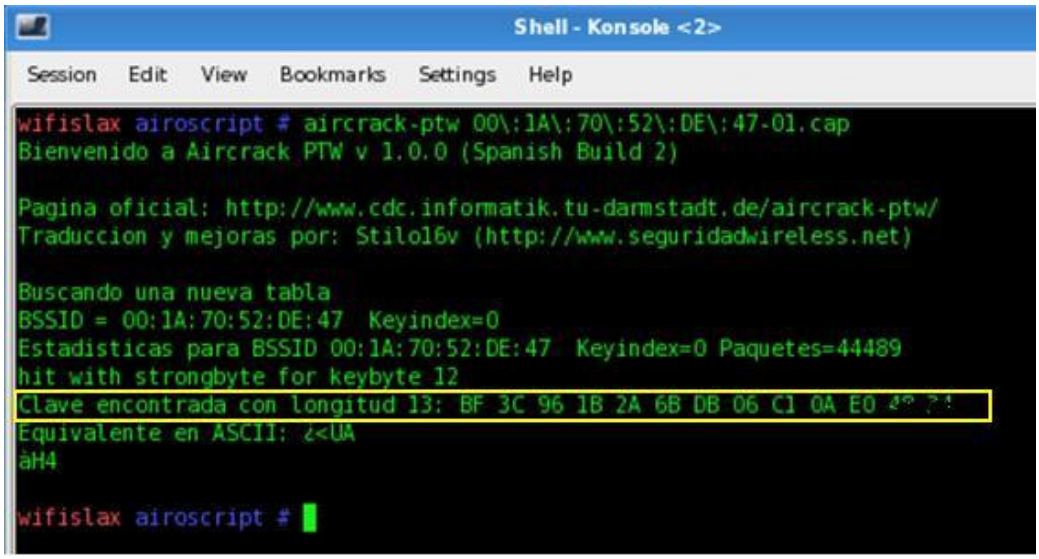


Imagen 2.6. Obtención de clave de la red inalámbrica

La **Imagen 2.7** muestra que clave obtenida es correcta y permite a la máquina atacante conectarse.

Imagen 2.7. Acceso a la red inalámbrica

Una vez conectado a la red inalámbrica un atacante puede realizar un escaneo de puertos en cualquier segmento de la red a fin de detectar los servicios que están activos y las versiones. También puede identificar vulnerabilidades y explotarlas para tener acceso a información confidencial.

2.3.1.2. Enumeración, obtención y descifrado de hash de cuentas de usuarios por medio de sesiones nulas

Una sesión nula se refiere a que existe configurado un registro con acceso anónimo en un equipo basado en Windows. Con este tipo de configuración es posible tener acceso a recursos compartidos, hash de cuentas de usuarios, grupos de usuarios, el registro, servicios y a la consola del equipo. La **Imagen 2.8** muestra un ejemplo de obtener hash de usuarios en un equipo con una sesión nula configurada.

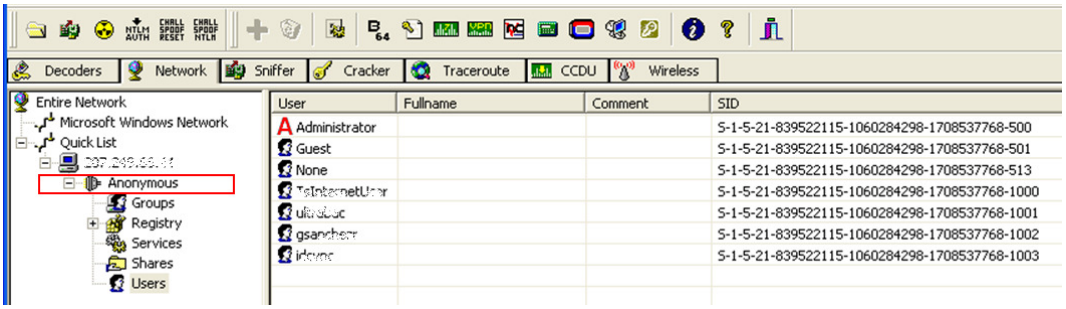


Imagen 2.8. Sesiones Nulas

Es posible tener cuentas de usuario de toda la red si el servidor de dominio tiene activada una sesión nula, tal como se muestra en la **Imagen 2.9.**

User	Fullname	Comment	SID	Req. Pass. Cha...	Pass Never Expire
Administrador	administrador	Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
Administrator		Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
[illegible]res	Agustin Flores	Consutor	S-1-5-21-84825569-1117726149-84...	No	Yes
db[illegible]des	db2des	Database Admi...	S-1-5-21-84825569-1117726149-84...	No	Yes
db[illegible]pro	db2pro	usuario de DB2 ...	S-1-5-21-84825569-1117726149-84...	No	Yes
des[illegible]	SAP System Administrator	SAP R/3 admini...	S-1-5-21-84825569-1117726149-84...	No	Yes
d[illegible]es	Daniel Torres Jacobo	Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
f[illegible]oja	Francisco Pantoja Vargas	Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
grivera	Guadalupe de Jesus	Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
grodrig	Gustavo Rodriguez	Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
Guest		Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
IUSR_SM[illegible]...	Internet Guest Account	Internet Server...	S-1-5-21-84825569-1117726149-84...	No	Yes
jromero	Juan Jose Romero		S-1-5-21-84825569-1117726149-84...	No	Yes
[illegible]sdm		Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
rb[illegible]esteros	Usuario temporal		S-1-5-21-84825569-1117726149-84...	No	No
s[illegible]3		Built-in account ...	S-1-5-21-84825569-1117726149-84...	No	Yes
saps[illegible]des	sapsedes	Standard SAP R...	S-1-5-21-84825569-1117726149-84...	No	Yes
sapsepro	sapsepro		S-1-5-21-84825569-1117726149-84...	No	Yes
SAPServicePRO	SAPServicePRO		S-1-5-21-84825569-1117726149-84...	No	Yes
SAPServiceWSD	SAPServiceWSD	Standard SAP S...	S-1-5-21-84825569-1117726149-84...	No	Yes
SAPServiceWSP	SAPServiceWSP	Standard SAP S...	S-1-5-21-84825569-1117726149-84...	No	Yes
server[illegible]alive		Usuario para m...	S-1-5-21-84825569-1117726149-84...	No	Yes
ver[illegible]tas	Usuario para respaldos		S-1-5-21-84825569-1117726149-84...	No	No
wsd[illegible]dm	wsdadm	SAP System Ad...	S-1-5-21-84825569-1117726149-84...	No	Yes

Imagen 2.9. Sesión Nula en Servidor de Dominio

Al obtener los hash de equipos con sesiones nulas configuradas, es posible descifrarlos tal como se muestra en la **Imagen 2.10.**

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	
Administrator		31d6cfe0d16ae931b73c59d7e0c089c0			empty
ASPNET	1cee2c26b700169e96489...	021ea6ea4256f89b0c0a8a7d5ed9881b			
Guest		31d6cfe0d16ae931b73c59d7e0c089c0			empty
RemoteMachine	6b41dd9530c9038baad3b...	efed447883b711926feaf0c7f4f482e8	14[illegible]	empty	147[illegible]
[illegible]		ce695a2e3bd6604436aad5e853915c4e			
ABC1		ce695a2e3bd6604436aad5e853915c4e			
Administrator	99fbf4555c5ece2caad3b4...	75cf9d630a71425d80997bb2606e2cd2	C[illegible]	empty	C[illegible]
ASPNET	bc9554f316c5dfd07311d...	e6cdb28f057a9b34763454594be00304	M[illegible]		
CMSGUEST		8c56ed521980d93cd781a3d05ba9b87e			
CN_Service		88efa8b38f6e1497fe33bea8abba9a65			
[illegible]		88efa8b38f6e1497fe33bea8abba9a65			
HelpAssistant		089ad402813405573810d15c46c05e3d			

Imagen 2.10. Descifrado de hash de usuarios

Una vez teniendo el nombre de usuario y la contraseña descifrada es posible tener acceso al sistema por medio de Remote Dessktop, tener información confidencial o usarlo para realizar algún escaneo o ataque hacia otros equipos en la red con los que tenga relaciones de confianza.

2.3.1.3. Ejecutando exploits en equipos no actualizados

Gran cantidad de equipos no actualizados son vulnerables a la ejecución del Exploit ms08_067_netapi, la cual podría permitir la ejecución remota de código si un sistema afectado recibe una solicitud RPC (Remote Procedure Call). En los sistemas Microsoft Windows 2000, Windows XP y Windows Server 2003, un atacante podría aprovechar esta vulnerabilidad sin autenticación para ejecutar código arbitrario.

Utilizando alguna herramienta como Metaesploit es posible explotar dicha vulnerabilidad y obtener cuentas de usuarios locales de la máquina comprometida, como se muestra en la **Imagen 2.11**.

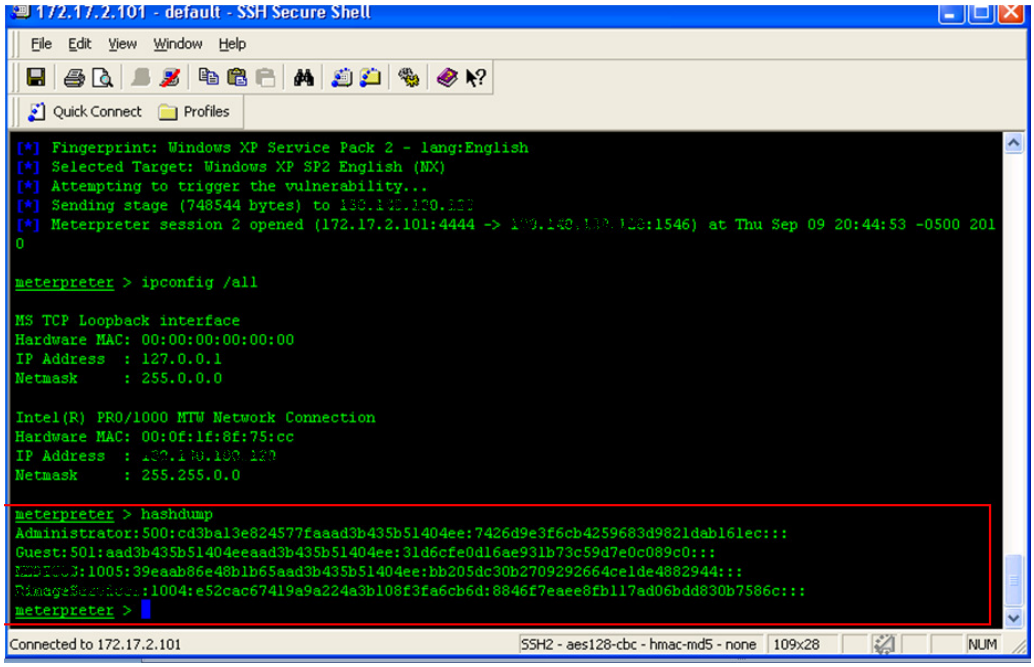


Imagen 2.11. Exploit ms08-067

Teniendo las cuentas de usuario de los equipos vulnerables, un atacante podría conectarse por Remote Desktop y robar información confidencial. En caso de que alguno de los equipos comprometidos sea un servidor el impacto sería mayor ya que se podría provocar una Denegación de Servicios y afectar por completo la operación y prestigio del Hospital.

2.3.1.4. Contraseñas por defecto a nivel aplicativo y dispositivos de red

Algunas veces es posible tener acceso a equipos por medio de aplicaciones con contraseña por default. Los administradores deben modificar los parámetros default que afecten a la aplicación o funcionamiento de la misma. La **Imagen 2.12** muestra un escaneo para detectar la contraseña por default en la aplicación tomcat.

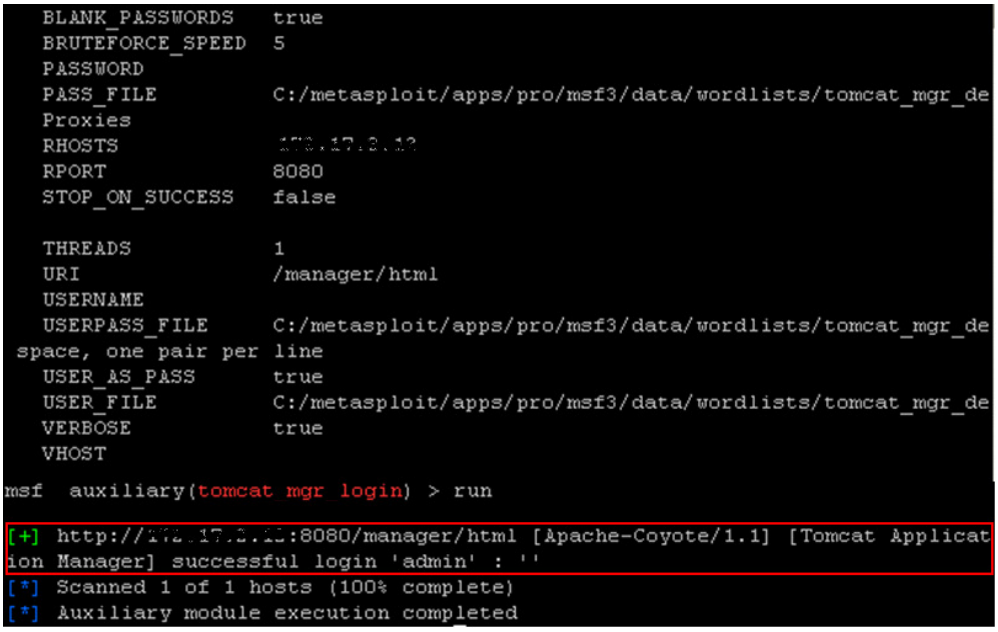


Imagen 2.12. Ejecución de exploit tomcat-mgr-login, para cotraseñas por default

El escaneo a la aplicación Tomcat indica que el usuario admin tiene contraseña en blanco por tanto es probable que sea vulnerable al exploit tomcat_mgr_deploy tal como lo muestra la **Imagen 2.13**.

Imagen 2.13. Ejecución exploit tomcat-mgr-deploy, para contraseñas por default

La **Imagen 2.14** muestra que el equipo es vulnerable y comprometido, se pueden tener los hash de las cuentas de usuario.

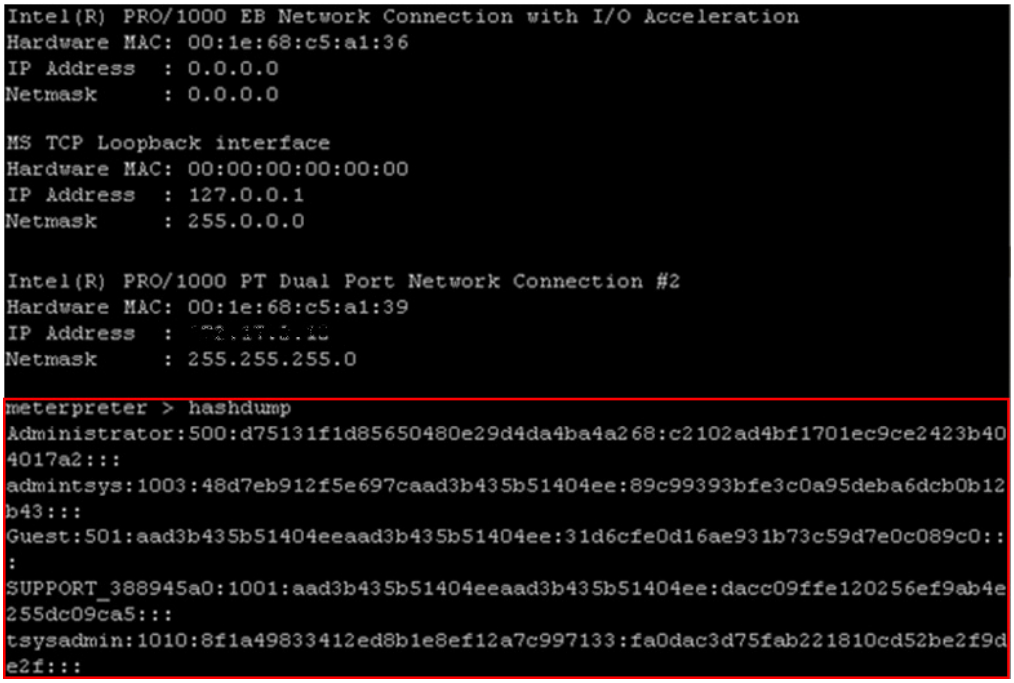


Imagen 2.14. Obtención de hash de usuario a través de contraseñas por default

Con las cuentas de usuario un atacante puede conectarse por Remote Desktop y tener acceso a una aplicación que controla todos los componentes de red en las diferentes instalaciones del Hospital debido a que la contraseña de la aplicación está en un block de notas en el escritorio como se muestra en la **Imagen 2.15**.

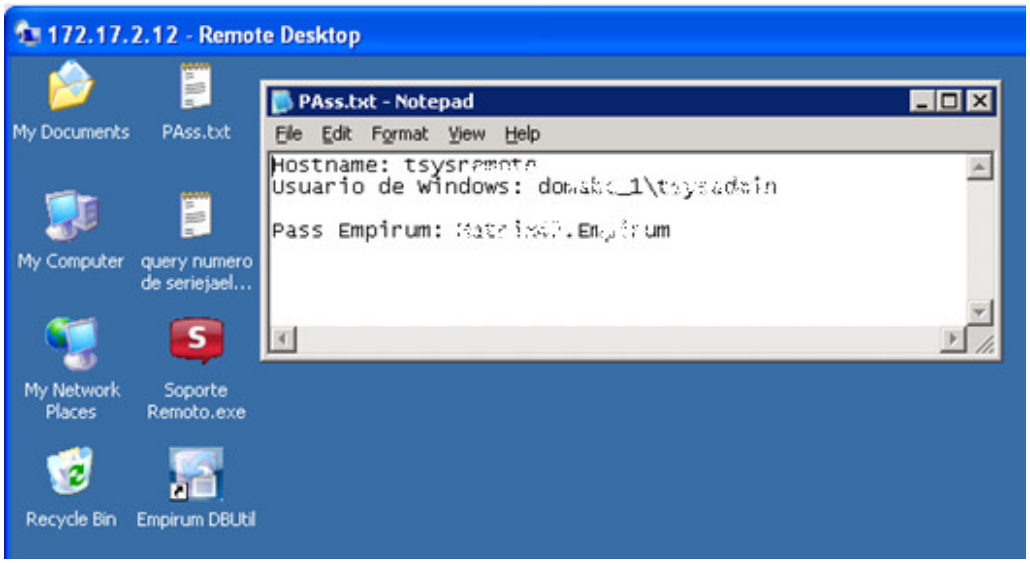


Imagen 2.15. Acceso a una Aplicación por medio de contraseñas por default

2.3.1.5. Detección de contraseñas por medio de archivos compartidos sin control de acceso

Al compartir archivos se debe establecer un control de acceso o no colocar información confidencial en ellos. De lo contrario, es muy probable que cualquier usuario pueda obtener información que no debería. En algunos casos es posible encontrar blocks de notas con contraseñas de acceso a servidores web, de correo, bases de datos o Access Point como se muestra en la **Imagen 2.16.**

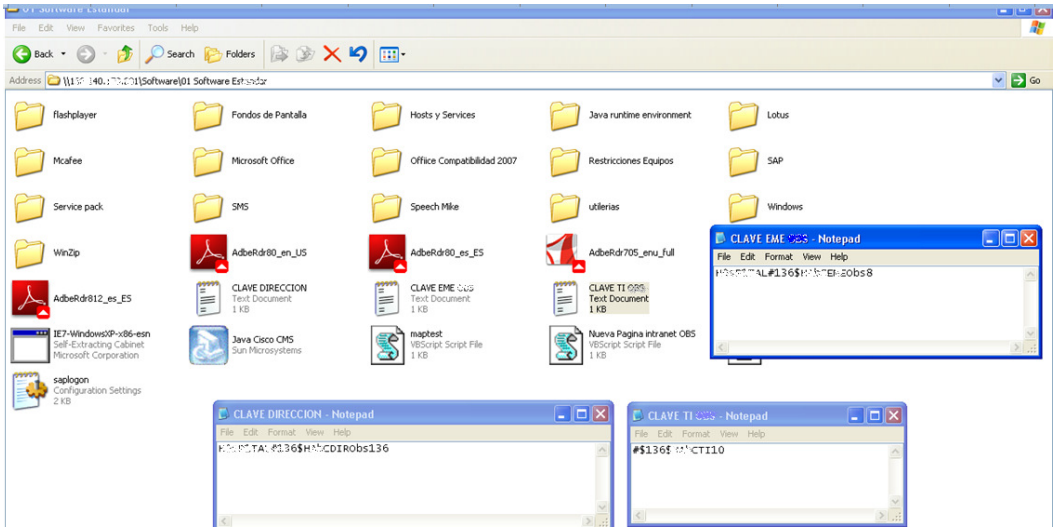


Imagen 2.16. Contraseña por archivos compartidos sin control de acceso

2.3.1.6. Captura de contraseñas en la red

El ataque Man in the Middle (hombre en el medio) es una técnica de hacking cuya finalidad es situar al equipo atacante en medio del equipo víctima y el router. Esto es necesario puesto que en una red que funciona con un switch, los paquetes viajan directamente entre el equipo víctima y el router, por lo tanto no basta con esnifar la red en modo promiscuo.

La manera en que el equipo víctima identifica el router, y viceversa, es usando el protocolo ARP, esto es: verificando la dirección MAC e IP de la tarjeta de red del otro equipo (en la tabla ARP). Siendo así, la técnica más común para llevar a cabo un ataque Man-in-the-middle es el **ARP** Spoofing, en la que el equipo atacante envenena la tabla ARP tanto del *equipo víctima* (haciéndose pasar por el router) como del *router* (haciéndose pasar como el equipo víctima), y por lo cual todos los paquetes que envíe o reciba la víctima circularán a través de la red del atacante.

Es importante que mientras se esté ejecutando un ataque man inthe middle, es necesario hacer un reenvío de paquetes. De lo contrario se dejaría sin conexión a la víctima y se estaría haciendo una Denegación de Servicios lo cual no es el objetivo de los análisis de vulnerabilidades y pruebas de penetración.

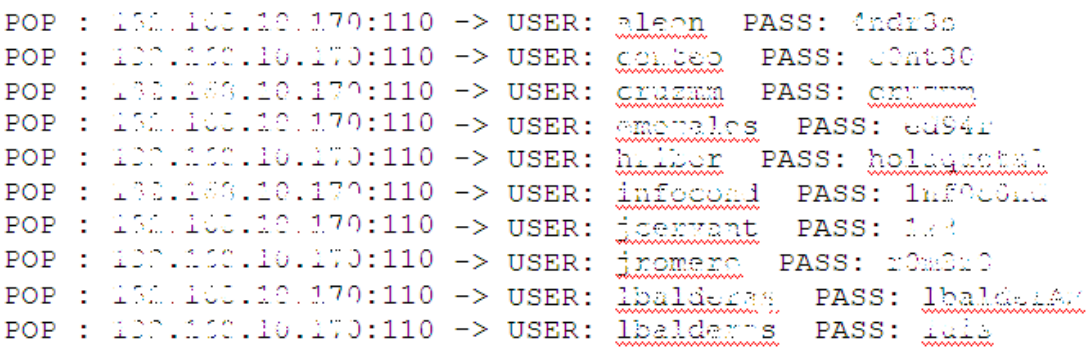


Imagen 2.17. Vista de Captura de contraseñas en texto claro

En la **Imagen 2.17** se muestra como es la captura de cuentas de usuario que viajan en texto claro en la red.

Imagen 2.18. Acceso a cuentas de correo electrónico

Con estas cuentas de correo un atacante puede disponer de la información contenida en el servidor o hacer uso del correo con algún fin malicioso. Es muy probable que haya información sensible del Hospital o personal que pueda poner en riesgo el prestigio de la misma o afectar directamente a los usuarios finales. Cabe mencionar que, con este ataque, no importa si la cuenta del usuario cuenta con una contraseña que cumpla con los requerimientos de seguridad de contraseñas, al viajar en texto claro eso queda en segundo plano. La **Imagen 2.18** muestra el acceso a cuentas de correo.

CAPITULO III

ANÁLISIS, IMPACTO Y RECOMENDACIONES

3. ANÁLISIS, IMPACTO Y RECOMENDACIONES

En este capítulo se detallan los hallazgos encontrados en cada análisis de Vulnerabilidades y Pruebas de Penetración, también se realiza un análisis del Impacto que tendría cada vulnerabilidad en caso de ser explotada por alguna persona externa al Hospital. Finalmente se mencionan las recomendaciones y controles de seguridad sugeridos para evitar el robo de información y mitigar el riesgo.

Los hallazgos están clasificados de acuerdo a las vulnerabilidades detectadas y comprobadas en donde se define la cantidad de equipos afectados por la misma, la problemática y un nivel de prioridad que va del 1-5, siendo 1 la prioridad menor y 5 la mayor. Este último valor es utilizado para el análisis del impacto que provoca la vulnerabilidad en la infraestructura del Hospital, tal como se muestra en la **Tabla 3.1**.

Campo	Descripción
Nombre de la Vulnerabilidad	Se describe la vulnerabilidad, debilidad o anomalía identificada.
Cantidad de Dispositivos Afectados (Denotado por "DA")	Identifica cuantos dispositivos están asociados a la vulnerabilidad.
Descripción de la Vulnerabilidad	Descripción de los riesgos que pueden materializarse a partir de la explotación de dicha vulnerabilidad. Este campo puede también contener una breve explicación de la forma en la que se podría explotar la vulnerabilidad en cuestión y su impacto en este contexto.
Calificación (Denotado con la letra "C")	Calificación asignada a la Vulnerabilidad según su criticidad.
Prioridad (denotado con la letra "P")	Prioridad de Atención a la Vulnerabilidad, está en función de la cantidad y tipo de dispositivos afectados.
Impacto (Denotado con la letra "I")	Impacto de la Vulnerabilidad que es la Suma de **C + P**.

Tabla 3.1. Clasificación de hallazgos

La calificación de las vulnerabilidades y la Prioridad de atención están determinadas conforme a la métrica que se muestra en la **Tabla 3.2**.

Valor	Métrica	Descripción
1	**Muy Bajo**	Una violación puede provocar una pérdida o daño insignificante
2	**Bajo**	Una violación puede provocar una pérdida o daño pequeño
3	**Medio**	Una violación puede provocar una pérdida o daño serio y el proceso de negocio puede verse afectado de forma negativa
4	**Alto**	Una violación puede provocar una pérdida o daño muy serio y el proceso de negocio puede fallar
5	**Muy Alto**	Una violación puede provocar una gran pérdida monetaria o en un daño a un individuo o a la organización como tal (en su bienestar, reputación, privacidad, posición competitiva) y que el proceso de negocio falle

Tabla 3.2. Métricas para análisis de Impacto de Vulnerabilidades

Tomando en cuenta la métrica anterior, la consultoría evalúa las vulnerabilidades según su criticidad quedando los valores como se muestran en la **Tabla 3.3**.

Vulnerabilidad	Calificación
Acceso a información por archivos compartidos	3
Contraseñas débiles	4
Acceso no Autorizado a Redes Inalámbricas del Hospital	5
Conexión directa y sin Restricción desde INTERNET a la red Corporativa del Hospital	5
Sesiones Nulas	5
Protocolos inseguros	4
Equipos no actualizados vulnerables a explotación y acceso remoto.	5
Contraseñas por defecto	5
VNC vulnerable	5
Acceso remoto al sistema con cuenta de Administrador	5
Captura de contraseñas en la red	5
Acceso con cuentas de correo	5
Impresoras sin control de acceso	2

Tabla 3.3. Calificación de Vulnerabilidades

El impacto de cada vulnerabilidad es calculado por la suma de la calificación y la prioridad de atención respecto a la cantidad de equipos afectados. La escala del impacto se puede visualizar en la **Tabla 3.4**. De igual forma se obtiene un valor final por análisis que es el promedio de las vulnerabilidades.

		IMPACTO				
Prioridad	**5**	6	7	8	9	10
	4	5	6	7	8	9
	3	4	5	6	7	8
	2	3	4	5	6	7
	1	2	3	4	5	6
		1	**2**	**3**	**4**	**5**
		Calificación de Vulnerabilidad				

Tabla 3.4. Valor del Impacto

La métrica que corresponde a cada valor esta detallado en la **Tabla 3.5**.

Valor	Métrica	Descripción
2	**Muy Bajo**	El daño es insignificante o nulo. Se podría considerar como un evento informativo.
3,4	**Bajo**	No existe una posible pérdida de confidencialidad, integridad y disponibilidad, sobre la organización, activos de información o personas.
5,6	**Medio**	Es posible que la pérdida de confidencialidad, integridad y disponibilidad sólo tenga un efecto limitado y adverso en la organización o las personas relacionadas a ella.
7,8	**Alto**	Es factible que la pérdida de confidencialidad, integridad y disponibilidad muestre un efecto serio y adverso en la organización o las personas vinculadas con ella.
9,10	**Muy Alto**	Es probable que la pérdida de confidencialidad, integridad y disponibilidad tenga un efecto catastrófico y adverso en la organización o las personas relacionadas con ella.

Tabla 3.5. Métrica del Impacto

3.1. Análisis del año 2010-1

En la **Tabla 3.6** se muestra las vulnerabilidades detectadas en el primer análisis que se realizó a inicios del año 2010.

Nombre de la Vulnerabilidad	DA	Descripción de la Vulnerabilidad	C	P	I
Acceso a información por archivos compartidos	11	A través de archivos compartidos o en algunos casos discos duros compartidos, es posible robar información extremadamente confidencial para el Hospital que pone en riesgo la imagen y el prestigio del mismo.	3	5	8
Contraseñas débiles	3	Es posible obtener la contraseña de algunos usuarios locales y de dominio ya que éstas no cuentan con un esquema de contraseñas fuertes. Tampoco existe la educación al usuario final de seguir con los lineamientos y políticas de seguridad que establece el Hospital. No hay una configuración en el servidor de Dominio para que defina el tiempo de caducidad de las contraseñas, ni que puedan ser reutilizadas.	4	5	9
Acceso no Autorizado a Redes Inalámbricas del Hospital	27	Es posible que cualquier persona externa al Hospital, obtenga la contraseña de acceso a la red inalámbrica debido a que los Access Point están configurados con un cifrado de clave muy débil (WEP). Aunado a la falta de segmentación de la red interna es visible toda la red.	5	5	10
Conexión directa y sin Restricción desde INTERNET a la red Corporativa del	2	Cada oficina puede conectar un Access Point para poder tener acceso a internet sin restricciones. El Hospital no ha gestionado la conexión de este tipo de dispositivos, ni ha	5	5	10

Hospital		verificado que su configuración sea la mínima requerida para evitar que cualquier persona ajena pueda tener acceso a la red interna y a la información confidencial.			
Sesiones Nulas	4	Es posible enumerar las cuentas de usuario de un equipo remoto sin conocer una cuenta válida en el mismo. Esto es debido a que tiene habilitada las sesiones nulas.	5	5	10
Protocolos inseguros	10	El uso de protocolos como FTP, Telnet o POP representa un riesgo ya que la información se transmite en texto claro, la cual puede ser interceptada por un atacante para obtener cuentas de usuarios.	4	5	9
Equipos no actualizados vulnerables a explotación y acceso remoto.	8	Es posible ingresar a equipos desactualizados de forma remota por medio de la explotación de vulnerabilidades conocidas. Una vez dentro es posible ejecutar comandos para obtener el archivo SAM donde se encuentran los usuarios y hashes de contraseñas.	5	5	10
Contraseñas por defecto	3	Este tipo de contraseña permite el acceso como administrador al equipo, dispositivo o aplicación.	5	5	10
VNC vulnerable	1	Es posible el acceso remoto al sistema sin autenticación por el uso de VNC vulnerable	5	5	10
Acceso remoto al sistema con cuenta de Administrador	9	Debido a que se carece de un esquema de contraseñas fuertes y controles de acceso es posible obtener la contraseña de usuarios de Administrador de dominio y locales, lo cual permite iniciar sesión por Remote Desktop en cualquier equipo y con cualquier usuario en la red.	5	5	10
Captura de contraseñas en la red	1	El servicio Ethernet proporcionado por los switches permite que cualquier persona dentro de la red del Hospital ejecute un envenenamiento a todos los hosts incluidos en la máscara de red 255.255.0.0, con ello el atacante puede interceptar la información de las comunicaciones sin cifrado, como son usuarios y contraseñas.	5	5	10
Acceso con cuentas de correo	30	Es posible que un atacante obtenga usuarios y contraseñas de los usuarios de correo que viajan por la red local del Hospital. Así como los mensajes de correo electrónico que viajen sin cifrado.	5	5	10
Impresoras sin control de acceso	5	Debido a la falta de control de acceso a las impresoras, es posible realizar modificaciones en la configuración, alterando su funcionamiento o causando Negación de Servicio.	2	2	4
				9.2	

Tabla 3.6. Análisis de Vulnerabilidades del año 2010-1

VALOR DEL IMPACTO: 9.2

MÉTRICA: Es probable que la pérdida de confidencialidad, integridad y disponibilidad tenga un efecto catastrófico y adverso en la organización o las personas relacionadas con ella.

3.1.1. IMPACTO

- Robo de información extremadamente confidencial, como expedientes médicos, análisis clínicos, información de pacientes y personal que labora en el Hospital lo cual impacta directamente en el prestigio del mismo.
- Obtención de todas las cuentas de usuario del dominio ya que el servidor de Active Directory es vulnerable a sesiones nulas y la mayoría de las contraseñas no cumplen con los requerimientos mínimos de seguridad.. Simplemente con el acceso a este servidor se tiene control total de la red.
- Cifrado WEP en Access Point lo cual los hace vulnerables y fácilmente comprometidos. Algunos de ellos están disponibles a los alrededores del Hospital, es decir que ni siquiera hay que estar, físicamente, dentro de las instalaciones para tener acceso a la información de carácter confidencial.
- Algunas personas dentro del Hospital colocan Access Point sin ninguna restricción y con una mala configuración lo cual representa un riesgo potencial, aunado a que la infraestructura de red carece de segmentación y controles de acceso, es posible que un atacante pueda tener acceso a toda la red comprometiendo alguno de estos Access Point.
- Acceso a información sensible por medio de un servidor de FTP con usuario anonymous, lo cual representa un riesgo potencial.
- Los servidores no actualizados impactan gravemente al Hospital ya que es posible explotar vulnerabilidades conocidas para obtener cuentas de usuario, conexiones remotas e información sensible.
- El poder llevar a cabo el ataque de Man in the middle con éxito ya representa un riesgo potencial en sí mismo, porque un atacante puede provocar una Denegación de Servicios, sin embargo para fines de este análisis sólo es pasivo. Aun así, fue posible interceptar cuentas de usuario del servidor de correo ya que se transfieren sin ser cifradas. Con estas cuentas es posible disponer libremente del servicio de correo electrónico.
- La página de administración de impresoras es totalmente visible y manipulable debido a que no está configurada la cuenta de administrador. Aunque no es crítico, esto podría provocar que cualquier persona modifique la configuración de dichos dispositivos e incluso hacer una denegación del servicio de impresión.

3.1.2. RECOMENDACIONES

Acceso a información por archivos compartidos: Se recomienda usar cifrado de información, creación de particiones cifradas para almacenamiento de información sensible.

Contraseñas por defecto, débiles y Acceso remoto al sistema con cuenta de Administrador: Se recomienda la creación de un esquema de contraseñas fuertes, con

más de 14 caracteres y haciendo uso de caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales. En el caso de contraseñas por defecto, después de la instalación de los aplicativos, es forzoso realizar la configuración correspondiente siguiendo con los lineamientos de seguridad y requerimientos del Hospital. En caso de no tenerlos definidos se debe considerar al menos el cambio de la contraseña.

Acceso no Autorizado a Redes Inalámbricas del Hospital y Conexión directa y sin Restricción desde INTERNET a la red Corporativa del Hospital: Se recomienda definir, establecer, implementar y divulgar una política de seguridad que garantice que:

a) El acceso a las redes inalámbricas de la Organización son controladas y accedidas por personal autorizado.
b) Las redes inalámbricas con acceso público no tengan comunicación con la red local de la Organización.

Sesiones Nulas: Un administrador puede configurar un equipo basado en Windows 2000 para evitar que un registro anónimo tenga acceso a todos los recursos, con la excepción de aquellos a los que se haya dado explícitamente acceso al usuario anónimo. Se debe tener en cuenta que si se están ejecutando Licencias de Terminal Server en el equipo basado en Windows 2000, otros servidores que tienen Terminal Services habilitado no podrán pedirle licencias. Es por ello que se recomienda hacer una evaluación del impacto que causaría deshabilitar dicho acceso anónimo en el Registro de Windows. http://support.microsoft.com/kb/246261

Protocolos inseguros: Se recomienda erradicar el servicio FTP ya que no maneja cifrado de tráfico y puede comprometer las credenciales de acceso. Se recomienda utilizar servicios seguros como Secure Shell.

Equipos no actualizados vulnerables a explotación y acceso remoto: Se recomienda aplicar la actualización para las vulnerabilidades MS08-067 y MS12-020 tal como lo menciona Microsoft Windows en su boletín de seguridad. Con esto se evita que alguna persona no autorizada pueda ejecutar código malicioso de forma remota utilizando solicitudes RPC (Remote Procedure Call o Llamada a Procedimiento Remoto). Dichas actualizaciones se consideran críticas para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003; y se consideran importantes para todas las ediciones compatibles de Windows Vista y Windows Server 2008. Se pueden descargar de las siguientes ligas:
http://technet.microsoft.com/es-mx/security/bulletin/ms08-067
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

VNC vulnerable: Se recomienda aplicar políticas de uso de software permitido en el Hospital y limitar el uso de software que permita la conectividad remota a equipos internos sino es sumamente necesario, de requerirse aplicar estrictos controles de seguridad lógica. Utilizar conexiones por servicio de VPN.

Captura de contraseñas en la red: Se recomienda definir, establecer, implementar y divulgar políticas de seguridad que contemplen:

- Revisión periódica de procesos críticos y tecnología soportada garantizando la encripción de la información transmitida.
- Activar en los switches Port Security o DHCP Snooping

Acceso con cuentas de correo: Se recomienda el fortalecimiento de contraseñas, así como realizar la clasificación de la información confidencial y adecuar los controles necesarios a cada tipo. Utilizar un protocolo seguro para la conexión con el servidor ya que el protocolo POP es visible por tanto es susceptible a captura de cuentas de usuarios.

Impresoras sin control de acceso: Se recomienda definir una contraseña fuerte a cada dispositivo de impresión para proteger el acceso a la página web de administración.

3.1.3. CONTROLES ISO17799-2005

11.4-Control de Acceso a la Red

a) Prevenir el acceso no autorizado a la red
b) Cambiar el cifrado WEP por uno más robusto (ejemplo: WPA2).
c) Cambiar el nombre de los SSID por nombres no relacionados a los departamentos de la organización.
d) Deshabilitar la difusión del SSID
e) Habilitar el filtrado por direcciones MAC
f) Realizar un inventario completo de todos los dispositivos inalámbricos de la red.
g) Deshabilitar las conexiones inalámbricas a los Access Points y sólo permitir Ethernet en medida de lo posible.

3.1.4. CONTROLES ISO 27001

A.7.2.1 Lineamientos de clasificación
A.7.2.2 Etiquetado y manejo de información.
A.8.2.2 Capacitación y educación en seguridad de la información.
A.8.2.3 Proceso disciplinario.
A.10.4.1 Controles contra software malicioso.
A.10.6.1 Controles de redes
A.10.7.3 Procedimientos de manejo de la información.
A.10.8.1 Procedimientos y políticas de información y software.
A.10.8.2 Acuerdos de intercambio.
A.10.8.4 Mensajes electrónicos.
A.11.2.2 Gestión de privilegios
A.11.2.3 Gestión de la clave del usuario
A.11.2.4 Revisión de los derechos de acceso del usuario.
A.11.3.1 Uso de clave.
A.11.5.3 Sistema de gestión de claves.
A.11.6.2 Aislamiento del sistema sensible.
A.11.7.2 Tele-trabajo

En el **ANEXO I – ISO 27001**, se menciona una breve descripción de la clasificación de los controles de seguridad sugeridos.

3.2. Análisis del año 2010-2

En la **Tabla 3.7** se muestra las vulnerabilidades detectadas en el segundo análisis que se realizó a mediados del año 2010.

Nombre de la Vulnerabilidad	DA	Descripción de la Vulnerabilidad	C	P	I
Acceso a información por archivos compartidos	19	Debido al acceso total que se tiene en algunos equipos, se puede obtener información personal/confidencial.	3	5	8
Contraseñas débiles	1	Es posible obtener la contraseña de algunos usuarios locales y de dominio ya que éstas no cuentan con un esquema de contraseñas fuertes. Tampoco existe la educación al usuario final de seguir con los lineamientos y políticas de seguridad que establece el Hospital. No hay una configuración en el servidor de Dominio para que defina el tiempo de caducidad de las contraseñas, ni que puedan ser reutilizadas.	4	5	9
Acceso no Autorizado a Redes Inalámbricas del Hospital	6	Es posible que cualquier persona externa al Hospital, obtenga la contraseña de acceso a la red inalámbrica debido a que los Access Point están configurados con un cifrado de clave muy débil (WEP).	5	5	10
Conexión directa y sin Restricción desde INTERNET a la red Corporativa del Hospital	2	Como consecuencia de la mala configuración de los Access Point de las redes inalámbricas es posible conectarse y tener acceso a la red interna del Hospital. Una vez conectado a la red inalámbrica, un atacante, podría robar información sensible o considerada como confidencial contenida en carpetas compartidas que carecen de la configuración de usuario y contraseña.	5	5	10
Sesiones Nulas	5	Es posible enumerar las cuentas de usuario de un equipo remoto sin conocer una cuenta válida en el mismo. Esto es debido a que tiene habilitada las sesiones nulas.	5	5	10
Protocolos inseguros	9	El uso de protocolos como FTP, Telnet o POP representa un riesgo ya que la información se transmite en texto claro, la cual puede ser interceptada por un atacante para obtener cuentas de usuarios.	4	5	9
Equipos no actualizados vulnerables a explotación y acceso remoto.	6	Es posible ingresar a equipos desactualizados de forma remota por medio de la explotación de vulnerabilidades conocidas. Una vez dentro es posible ejecutar comandos a discreción. Incluso es posible obtener el archivo SAM donde se encuentran los usuarios y hashes de contraseñas.	5	5	10
Contraseñas por defecto	9	Este tipo de contraseña permite el acceso como administrador al equipo o dispositivo.	5	5	10

Acceso remoto al sistema con cuenta de Administrador	2	Debido a que se carece de un esquema de contraseñas fuertes y controles de acceso es posible obtener la contraseña de usuarios de Administrador de dominio y locales, lo cual permite iniciar sesión por Remote Desktop en cualquier equipo y con cualquier usuario en la red.	5	5	10
Captura de contraseñas en la red	1	El servicio Ethernet proporcionado por los switches permite que cualquier persona dentro de la red del Hospital ejecute un envenenamiento a todos los hosts incluidos en la máscara de red 255.255.0.0, con ello el atacante puede interceptar la información de las comunicaciones sin cifrado, como son usuarios y contraseñas.	5	5	10
Acceso con cuentas de correo	26	Es posible que un atacante obtenga usuarios y contraseñas de los usuarios de correo que viajan por la red local del Hospital. Así como los mensajes de correo electrónico que viajen sin cifrado.	5	5	10
Impresoras sin control de acceso	8	Debido a la falta de control de acceso a las impresoras, es posible realizar modificaciones en la configuración, alterando su funcionamiento o causando Negación de Servicio.	2	2	4
			8.5		

Tabla 3.7. Análisis de Vulnerabilidades del año 2010-2

VALOR DEL IMPACTO: 8.5

MÉTRICA: Es factible que la pérdida de confidencialidad, integridad y disponibilidad muestre un efecto serio y adverso en la organización o las personas vinculadas con ella.

3.2.1. IMPACTO

- Se sigue presentando el robo de información extremadamente confidencial, como expedientes médicos, análisis clínicos, archivos de guardias del personal que labora en el Hospital, lo cual impacta directamente el prestigio del mismo.
- Entre los archivos compartidos sin control de acceso se encuentran blocks de notas con contraseñas de servidores lo cual los vulnera por completo. Cabe destacar que aunque, dichos equipos, cuenten con los controles de seguridad no sirve de nada si una cuenta de acceso está contenida en un archivo sin cifrar.
- Obtención de algunas cuentas de usuario del dominio ya que no fueron modificadas desde el análisis anterior y algunas de ellas pertenecen al grupo de administradores. Algunos equipos aun son vulnerables a sesiones nulas lo cual permite obtener cuentas de usuarios locales y de dominio.
- La cantidad de Access Point con cifrado WEP disminuyó considerablemente, sin embargo aun es posible acceder a la red del Hospital.
- Se detectan Access Point con cifrado WPA2, sin embargo las contraseñas fueron encontradas en blocks de notas contenidos en carpetas compartidas sin control de acceso, lo cual no sirve de nada que los Access Point cumplan con un

protocolo más fuerte si aún se sigue guardando la información en archivos sin cifrar.

- Disminuyeron la cantidad de Access Point colocados en algunas oficinas, sin embargo se sigue teniendo acceso a la red del Hospital debido a la carencia de segmentación en VLANS y controles de acceso.
- A pesar de que se usan protocolos inseguros por parte de un proveedor la información que se obtiene no afecta de forma crítica a la Organización.
- Es posible ingresar remotamente a equipos no actualizados y vulnerables a ejecución de exploits. Una vez dentro es posible ejecutar comandos para obtener los hash de cuentas de usuarios local.
- Las contraseñas por defecto permiten acceso como administrador a dispositivos de red. Los cuales pueden ser modificados en su configuración o peor aun borrarla y provocar daños graves y denegación de servicios.
- El poder llevar a cabo el ataque de Man in the middle con éxito ya representa un riesgo potencial en sí mismo porque un atacante puede provocar una Denegación de Servicios, sin embargo para fines de este análisis sólo es pasivo. Aun así, fue posible interceptar cuentas de usuario del servidor de correo ya que se transfieren sin ser cifradas. Con estas cuentas es posible disponer libremente del servicio de correo electrónico.
- La página de administración de impresoras es totalmente visible y manipulable debido a que no está configurada la cuenta de administrador. Aunque no es crítico, esto podría provocar que cualquier persona pueda modificar la configuración de dichos dispositivos e incluso hacer una denegación del servicio de impresión.

3.2.2. RECOMENDACIONES

Acceso a información por archivos compartidos: Se recomienda usar cifrado de información, creación de particiones cifradas para almacenamiento de información sensible.

Contraseñas por defecto, débiles y Acceso remoto al sistema con cuenta de Administrador: Se recomienda la creación de un esquema de contraseñas fuertes, con más de 14 caracteres y haciendo uso de caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales. En el caso de contraseñas por defecto, después de la instalación de los aplicativos, es forzoso realizar la configuración correspondiente siguiendo con los lineamientos de seguridad y requerimientos del Hospital. En caso de no tenerlos definidos se debe considerar al menos el cambio de la contraseña.

Acceso no Autorizado a Redes Inalámbricas del Hospital y Conexión directa y sin Restricción desde INTERNET a la red Corporativa del Hospital: Se recomienda definir, establecer, implementar y divulgar una política de seguridad que garantice que:

a) El acceso a las redes inalámbricas de la Organización son controladas y accedidas por personal autorizado.
b) Las redes inalámbricas con acceso público no tengan comunicación con la red local de la Organización.

Sesiones Nulas: Un administrador puede configurar un equipo basado en Windows 2000 para evitar que un registro anónimo tenga acceso a todos los recursos, con la excepción de aquellos a los que se haya dado explícitamente acceso al usuario anónimo.

Se debe tener en cuenta que si se están ejecutando Licencias de Terminal Server en el equipo basado en Windows 2000, otros servidores que tienen Terminal Services habilitado no podrán pedirle licencias. Es por ello que se recomienda hacer una evaluación del impacto que causaría deshabilitar dicho acceso anónimo en el Registro de Windows. http://support.microsoft.com/kb/246261

Protocolos inseguros Se recomienda erradicar el servicio FTP ya que no maneja cifrado de tráfico y puede comprometer las credenciales de acceso. Se recomienda utilizar servicios seguros como Secure Shell.

Equipos no actualizados vulnerables a explotación y acceso remoto: Se recomienda aplicar la actualización para las vulnerabilidades MS08-067 y MS12-020 tal como lo menciona Microsoft Windows en su boletín de seguridad. Con esto se evita que alguna persona no autorizada pueda ejecutar código malicioso de forma remota utilizando solicitudes RPC (Remote Procedure Call o Llamada a Procedimiento Remoto). Dichas actualizaciones se consideran críticas para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003; y se consideran importantes para todas las ediciones compatibles de Windows Vista y Windows Server 2008. Se pueden descargar de las siguientes ligas:
http://technet.microsoft.com/es-mx/security/bulletin/ms08-067
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Captura de contraseñas en la red: Se recomienda definir, establecer, implementar y divulgar políticas de seguridad que contemplen:

- Revisión periódica de procesos críticos y tecnología soportada garantizando la encripción de la información transmitida.
- Activar en los switches Port Security o DHCP Snooping

Acceso con cuentas de correo: Se recomienda el fortalecimiento de contraseñas, así como realizar la clasificación de la información confidencial y adecuar los controles necesarios a cada tipo. Utilizar un protocolo seguro para la conexión con el servidor ya que el protocolo POP es visible por tanto es susceptible a captura de cuentas de usuarios.

Impresoras sin control de acceso: Se recomienda definir una contraseña fuerte a cada dispositivo de impresión para proteger el acceso a la página web de administración.

3.2.3. CONTROLES ISO17799-2005

11.4-Control de Acceso a la Red

h) Prevenir el acceso no autorizado a la red
a) Cambiar el cifrado WEP por uno más robusto (ejemplo: WPA2).
b) Cambiar el nombre de los SSID por nombres no relacionados a los departamentos de la organización.
c) Deshabilitar la difusión del SSID
d) Habilitar el filtrado por direcciones MAC
e) Realizar un inventario completo de todos los dispositivos inalámbricos de la red.
f) Deshabilitar las conexiones inalámbricas a los Access Points y solo permitir Ethernet en medida de lo posible.

3.2.4. CONTROLES ISO 27001

A.7.2.1 Lineamientos de clasificación
A.7.2.2 Etiquetado y manejo de información.
A.8.2.2 Capacitación y educación en seguridad de la información.
A.8.2.3 Proceso disciplinario.
A.10.4.1 Controles contra software malicioso.
A.10.6.1 Controles de redes.
A.10.6.2 Seguridad de los servicios de la red.
A.10.7.3 Procedimientos de manejo de la información.
A.10.8.1 Procedimientos y políticas de información y software.
A.10.8.2 Acuerdos de intercambio.
A.10.8.4 Mensajes electrónicos.
A.11.2.3 Gestión de la clave del usuario
A.11.2.4 Revisión de los derechos de acceso del usuario.
A.11.3.1 Uso de clave.
A.11.5.3 Sistema de gestión de claves.
A.11.6.2 Aislamiento del sistema sensible.

En el **ANEXO I – ISO 27001**, se menciona una breve descripción de la clasificación de los controles de seguridad sugeridos.

3.3. Análisis del año 2011-1

En la **Tabla 3.8** se muestra las vulnerabilidades detectadas en el tercer análisis que se realizó a inicios del año 2011.

Nombre de la Vulnerabilidad	DA	Descripción de la Vulnerabilidad	C	P	I
Acceso a información por archivos compartidos	5	A través de archivos compartidos o en algunos casos discos duros compartidos, es posible robar información extremadamente confidencial para el Hospital que pone en riesgo la imagen y el prestigio de la misma.	3	5	8
Contraseñas débiles	8	Es posible obtener la contraseña de algunos usuarios locales y de dominio ya que éstas no cuentan con un esquema de contraseñas fuertes. Tampoco existe la educación al usuario final de seguir con los lineamientos y políticas de seguridad que establece el Hospital. No hay una configuración en el servidor de Dominio para que defina el tiempo de caducidad de las contraseñas, ni que puedan ser reutilizadas.	4	4	8
Acceso no Autorizado a Redes Inalámbricas del Hospital	10	Es posible que cualquier persona externa al Hospital, obtenga la contraseña de acceso a la red inalámbrica debido a que los Access Point están configurados con un cifrado de clave muy débil (WEP). Aunado a la falta de segmentación de la red interna es visible toda la red.	5	5	10
Sesiones Nulas	3	Es posible enumerar las cuentas de usuario de un	5	5	10

		equipo remoto sin conocer una cuenta válida en el mismo. Esto es debido a que tiene habilitada las sesiones nulas.			
Protocolos inseguros	5	El uso de protocolos como FTP, Telnet o POP representa un riesgo ya que la información se transmite en texto claro, la cual puede ser interceptada por un atacante para obtener cuentas de usuarios.	4	5	9
Equipos no actualizados vulnerables a explotación y acceso remoto.	1	Es posible ingresar a equipos desactualizados de forma remota por medio de la explotación de vulnerabilidades conocidas. Una vez dentro es posible ejecutar comandos a discreción. Incluso es posible obtener el archivo SAM donde se encuentran los usuarios y hashes de contraseñas.	5	5	10
Contraseñas por defecto	2	Este tipo de contraseña permite el acceso como administrador al equipo o dispositivo.	5	5	10
VNC vulnerable	6	Es posible el acceso remoto al sistema sin autenticación por el uso de VNC vulnerable.	5	5	10
Acceso remoto al sistema con cuenta de Administrador	2	Debido a que se carece de un esquema de contraseñas fuertes y controles de acceso es posible obtener la contraseña de usuarios de Administrador de dominio y locales, lo cual permite iniciar sesión por Remote Desktop en cualquier equipo y con cualquier usuario en la red.	5	5	10
Captura de contraseñas en la red	6	El servicio Ethernet proporcionado por los switches permite que cualquier persona dentro de la red del Hospital ejecute un envenenamiento a todos los hosts incluidos en la máscara de red 255.255.0.0, con ello el atacante puede interceptar la información de las comunicaciones sin cifrado, como son usuarios y contraseñas.	5	5	10
Acceso con cuentas de correo	6	Es posible que un atacante obtenga usuarios y contraseñas de los usuarios de correo que viajan por la red local del Hospital. Así como los mensajes de correo electrónico que viajen sin cifrado.	5	5	10
				8.2	

Tabla 3.8. Análisis de Vulnerabilidades del año 2011-1

VALOR DEL IMPACTO: 8.2

MÉTRICA: Es factible que la pérdida de confidencialidad, integridad y disponibilidad muestre un efecto serio y adverso en la organización o las personas vinculadas con ella.

3.3.1. IMPACTO

- Todavía es posible obtener información extremadamente Confidencial del Hospital tal como informes médicos, historiales de pacientes, análisis clínicos, etc. que definitivamente pone en Riesgo la imagen, el prestigio y la operación de la misma.

- Las contraseñas de usuarios de dominio detectadas en servicios anteriores, no son modificadas y con ello se tiene acceso a servidores por medio del servicio VNC.
- Algunos usuario reutilizan contraseñas por tanto es posible tener acceso a sus equipos sólo con hacer una comprobación de cuentas de análisis anteriores. O haciendo un ataque de diccionario o fuerza bruta utilizando las contraseñas encontradas anteriormente.
- A pesar de que disminuye la cantidad de redes inalámbricas con cifrado WEP es posible tener acceso a gran parte de la red interna debido a la carencia de segmentación en la red del Hospital.
- Aun hay equipos con sesiones nulas activadas lo cual tiene un impacto considerable ay que permite enumerar cuentas de usuarios locales sin necesidad de conocer una cuenta válida en el sistema.
- El uso de protocolos inseguros por parte de los proveedores del Hospital representa un riesgo ya que las conexiones y transferencia de la información es en texto claro por tanto es fácilmente interceptada. Es importante que el Hospital solicite a los proveedores que cumplan con los lineamientos y políticas de seguridad para hacer uso de los recursos de la red.
- Los equipos no actualizados tienen un riesgo potencial porque es posible explotar vulnerabilidades conocidas para obtener las cuentas de usuario local.
- Las contraseñas por defecto permiten acceso como administrador a dispositivos de red. Los cuales pueden ser modificados en su configuración o peor aun borrarla y provocar daños graves y denegación de servicios.
- El poder llevar a cabo el ataque de Man in the middle con éxito ya representa un riesgo potencial en sí mismo porque un atacante puede provocar una Denegación de Servicios, sin embargo para fines de este análisis sólo es pasivo. Aun así, fue posible interceptar cuentas de usuario del servidor de correo ya que se transfieren sin ser cifradas. Con estas cuentas es posible disponer libremente del servicio de correo electrónico.

3.3.2. RECOMENDACIONES

Acceso a información por archivos compartidos: Se recomienda usar cifrado de información, creación de particiones cifradas para almacenamiento de información sensible.

Contraseñas por defecto, débiles y Acceso remoto al sistema con cuenta de Administrador: Se recomienda la creación de un esquema de contraseñas fuertes, con más de 14 caracteres y haciendo uso de caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales. En el caso de contraseñas por defecto, después de la instalación de los aplicativos, es forzoso realizar la configuración correspondiente siguiendo con los lineamientos de seguridad y requerimientos del Hospital. En caso de no tenerlos definidos se debe considerar al menos el cambio de la contraseña.

Sesiones Nulas: Un administrador puede configurar un equipo basado en Windows 2000 para evitar que un registro anónimo tenga acceso a todos los recursos, con la excepción de aquellos a los que se haya dado explícitamente acceso al usuario anónimo. Se debe tener en cuenta que si se están ejecutando Licencias de Terminal Server en el equipo basado en Windows 2000, otros servidores que tienen Terminal Services habilitado no podrán pedirle licencias. Es por ello que se recomienda hacer una

evaluación del impacto que causaría deshabilitar dicho acceso anónimo en el Registro de Windows. http://support.microsoft.com/kb/246261

Protocolos inseguros: Se recomienda erradicar el servicio FTP ya que no maneja cifrado de tráfico y puede comprometer las credenciales de acceso. Se recomienda utilizar servicios seguros como Secure Shell.

Equipos no actualizados vulnerables a explotación y acceso remoto: Se recomienda aplicar la actualización para las vulnerabilidades MS08-067 y MS12-020 tal como lo menciona Microsoft Windows en su boletín de seguridad. Con esto se evita que alguna persona no autorizada pueda ejecutar código malicioso de forma remota utilizando solicitudes RPC (Remote Procedure Call o Llamada a Procedimiento Remoto). Dichas actualizaciones se consideran críticas para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003; y se consideran importantes para todas las ediciones compatibles de Windows Vista y Windows Server 2008. Se pueden descargar de las siguientes ligas:
http://technet.microsoft.com/es-mx/security/bulletin/ms08-067
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

VNC vulnerable: Se recomienda aplicar políticas de uso de software permitido en el Hospital y limitar el uso de software que permita la conectividad remota a equipos internos sino es sumamente necesario, de requerirse aplicar estrictos controles de seguridad lógica. Utilizar conexiones por servicio de VPN.

Captura de contraseñas en la red: Se recomienda definir, establecer, implementar y divulgar políticas de seguridad que contemplen:

- Revisión periódica de procesos críticos y tecnología soportada garantizando la encripción de la información transmitida.
- Activar en los switches Port Security o DHCP Snooping

Acceso con cuentas de correo: Se recomienda el fortalecimiento de contraseñas, así como realizar la clasificación de la información confidencial y adecuar los controles necesarios a cada tipo. Utilizar un protocolo seguro para la conexión con el servidor ya que el protocolo POP es visible por tanto es susceptible a captura de cuentas de usuarios.

3.3.3. CONTROLES ISO 27001

A.7.2.1 Lineamientos de clasificación
A.7.2.2 Etiquetado y manejo de información.
A.8.2.2 Capacitación y educación en seguridad de la información.
A.8.2.3 Proceso disciplinario.
A.10.4.1 Controles contra software malicioso.
A.10.7.3 Procedimientos de manejo de la información.
A.10.8.1 Procedimientos y políticas de información y software.
A.10.8.2 Acuerdos de intercambio.
A.10.8.4 Mensajes electrónicos.
A.11.2.2 Gestión de privilegios
A.11.2.3 Gestión de la clave del usuario
A.11.2.4 Revisión de los derechos de acceso del usuario.

A.11.5.3 Sistema de gestión de claves.
A.11.6.2 Aislamiento del sistema sensible.
A.11.7.2 Tele-trabajo

En el **ANEXO I – ISO 27001**, se menciona una breve descripción de la clasificación de los controles de seguridad sugeridos.

3.4. Análisis del año 2011-2

En la **Tabla 3.9** se muestra las vulnerabilidades detectadas en el cuarto análisis que se realizó a mediados del año 2011.

Nombre de la Vulnerabilidad	DA	Descripción de la Vulnerabilidad	C	P	I
Acceso a información por archivos compartidos	1	A través de archivos compartidos o en algunos casos discos duros compartidos, es posible robar información extremadamente confidencial para el Hospital que pone en riesgo la imagen y el prestigio de la misma.	3	5	8
Contraseñas débiles	7	Es posible obtener la contraseña de algunos usuarios locales y de dominio ya que éstas no cuentan con un esquema de contraseñas fuertes. Tampoco existe la educación al usuario final de seguir con los lineamientos y políticas de seguridad que establece el Hospital. No hay una configuración en el servidor de Dominio para que defina el tiempo de caducidad de las contraseñas, ni que puedan ser reutilizadas.	4	5	9
Acceso no Autorizado a Redes Inalámbricas del Hospital	2	Es posible que cualquier persona externa a el Hospital, obtenga la contraseña de acceso a la red inalámbrica debido a que los Access Point están configurados con un cifrado de clave muy débil (WEP). Aunado a la falta de segmentación de la red interna es visible toda la red.	5	5	10
Protocolos inseguros	1	El uso de protocolos como FTP, Telnet o POP representa un riesgo ya que la información se transmite en texto claro, la cual puede ser interceptada por un atacante para obtener cuentas de usuarios.	4	3	7
Equipos no actualizados vulnerables a explotación y acceso remoto.	8	Es posible ingresar a equipos desactualizados de forma remota por medio de la explotación de vulnerabilidades conocidas. Una vez dentro es posible ejecutar comandos a discreción. Incluso es posible obtener el archivo SAM donde se encuentran los usuarios y hashes de contraseñas.	5	5	10
VNC vulnerable	5	Es posible el acceso remoto al sistema sin autenticación por el uso de VNC vulnerable	5	5	10
Acceso remoto al sistema con cuenta de Administrador	13	Debido a que se carece de un esquema de contraseñas fuertes y controles de acceso es posible obtener la contraseña de usuarios de Administrador de dominio y locales, lo cual permite iniciar sesión por Remote Desktop en	5	5	10

		cualquier equipo y con cualquier usuario en la red.			
Captura de contraseñas en la red	1	El servicio Ethernet proporcionado por los switches permite que cualquier persona dentro de la red del Hospital ejecute un envenenamiento a todos los hosts incluidos en la máscara de red 255.255.0.0, con ello el atacante puede interceptar la información de las comunicaciones sin cifrado, como son usuarios y contraseñas.	5	5	10
Acceso con cuentas de correo	8	Es posible que un atacante obtenga usuarios y contraseñas de los usuarios de correo que viajan por la red local del Hospital. Así como los mensajes de correo electrónico que viajen sin cifrado.	5	5	10
Impresoras sin control de acceso	2	Debido a la falta de control de acceso a las impresoras, es posible realizar modificaciones en la configuración, alterando su funcionamiento o causando Negación de Servicio.	2	2	4
			6.8		

Tabla 3.9. Análisis de Vulnerabilidades del año 2011-2

VALOR DEL IMPACTO: 6.8

MÉTRICA: Es posible que la pérdida de confidencialidad, integridad y disponibilidad sólo tenga un efecto limitado y adverso en la organización o las personas relacionadas a ella.

3.4.1. IMPACTO

- Tener información sensible en carpetas compartidas sin control de acceso impacta gravemente al Hospital ya que está al alcance de cualquier persona que tiene acceso a la red.
- Se siguen utilizando contraseñas débiles que son vulnerables a ataques de diccionario y fuerza bruta. Estas cuentas dan acceso a equipos con información confidencial, así como a cuentas de correo.
- Disminuyó considerablemente el número de redes inalámbricas con cifrado WEP, sin embargo con las 2 que se vulneraron fue posible llegar al segmento de los servidores y equipos con archivos compartidos sin control de acceso y tener información confidencial. Cabe mencionar que la red ya está segmentada, sin embargo el impacto sigue siendo alto porque el segmento al que se tiene acceso conectándose a las redes inalámbricas es el de servidores.
- Al utilizar protocolos inseguros como telnet y ftp para la administración de dispositivos de red se intercepta la cuenta de administrador y se tiene acceso privilegiado a dichos dispositivos. Esto puede provocar daños considerables en el trabajo operativo del Hospital.
- El uso del protocolo POP para el correo electrónico permite la intercepción de cuentas de correo ya que se transmiten en texto claro. Con ello es posible disponer del servicio de correo electrónico en su totalidad.
- Los equipos no actualizados son vulnerables a ejecución de comandos remotos para obtener las cuentas de usuarios locales incluyendo la de Administrador.

Esto implica que alguna persona no autorizada puede tener acceso al equipo vulnerable y revisar que tipo de información se aloja en él y obtenerla fácilmente.

- La intercepción de información en texto claro que se transmite a través de la red tiene un impacto Muy Alto ya que es posible tener acceso a cuentas de correo y dispositivos de red.
- Nuevamente se detectan equipos con el servicio de VNC versión 4.1 la cual es vulnerable. Un atacante puede tomar control del equipo por medio de dicho servicio sin conocer alguna contraseña válida en el sistema.

3.4.2. RECOMENDACIONES

Acceso a información por archivos compartidos: Se recomienda usar cifrado de información, creación de particiones cifradas para almacenamiento de información sensible.

Contraseñas débiles y Acceso remoto al sistema con cuenta de Administrador: Se recomienda la creación de un esquema de contraseñas fuertes, con más de 14 caracteres y haciendo uso de caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales. En el caso de contraseñas por defecto, después de la instalación de los aplicativos, es forzoso realizar la configuración correspondiente siguiendo con los lineamientos de seguridad y requerimientos del Hospital. En caso de no tenerlos definidos se debe considerar al menos el cambio de la contraseña.

Protocolos inseguros: Se recomienda erradicar el servicio FTP ya que no maneja cifrado de tráfico y puede comprometer las credenciales de acceso. Se recomienda utilizar servicios seguros como Secure Shell.

Equipos no actualizados vulnerables a explotación y acceso remoto: Se recomienda aplicar la actualización para las vulnerabilidades MS08-067 y MS12-020 tal como lo menciona Microsoft Windows en su boletín de seguridad. Con esto se evita que alguna persona no autorizada pueda ejecutar código malicioso de forma remota utilizando solicitudes RPC (Remote Procedure Call o Llamada a Procedimiento Remoto). Dichas actualizaciones se consideran críticas para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003; y se consideran importantes para todas las ediciones compatibles de Windows Vista y Windows Server 2008. Se pueden descargar de las siguientes ligas:
http://technet.microsoft.com/es-mx/security/bulletin/ms08-067
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

VNC vulnerable: Se recomienda aplicar políticas de uso de software permitido en el Hospital y limitar el uso de software que permita la conectividad remota a equipos internos sino es sumamente necesario, de requerirse aplicar estrictos controles de seguridad lógica. Utilizar conexiones por servicio de VPN.

Captura de contraseñas en la red: Se recomienda definir, establecer, implementar y divulgar políticas de seguridad que contemplen:

- Revisión periódica de procesos críticos y tecnología soportada garantizando la encripción de la información transmitida.

- Activar en los switches Port Security o DHCP Snooping

Acceso con cuentas de correo: Se recomienda el fortalecimiento de contraseñas, así como realizar la clasificación de la información confidencial y adecuar los controles necesarios a cada tipo. Utilizar un protocolo seguro para la conexión con el servidor ya que el protocolo POP es visible por tanto es susceptible a captura de cuentas de usuarios.

Impresoras sin control de acceso: Se recomienda definir una contraseña fuerte a cada dispositivo de impresión para proteger el acceso a la página web de administración.

3.4.3. CONTROLES ISO 27001

A.7.2.1 Lineamientos de clasificación
A.7.2.2 Etiquetado y manejo de información.
A.8.2.2 Capacitación y educación en seguridad de la información.
A.8.2.3 Proceso disciplinario.
A.10.4.1 Controles contra software malicioso.
A.10.7.3 Procedimientos de manejo de la información.
A.10.8.1 Procedimientos y políticas de información y software.
A.10.8.2 Acuerdos de intercambio.
A.10.8.4 Mensajes electrónicos.
A.11.2.2 Gestión de privilegios
A.11.2.3 Gestión de la clave del usuario
A.11.2.4 Revisión de los derechos de acceso del usuario.
A.11.3.1 Uso de clave.
A.11.5.3 Sistema de gestión de claves.
A.11.6.2 Aislamiento del sistema sensible.
A.11.7.2 Tele-trabajo

En el **ANEXO I – ISO 27001**, se menciona una breve descripción de la clasificación de los controles de seguridad sugeridos.

3.5. Análisis del año 2012-1

En la **Tabla 3.10** se muestra las vulnerabilidades detectadas en el quinto análisis que se realizó a inicios del año 2012.

Nombre de la Vulnerabilidad	DA	Descripción de la Vulnerabilidad	C	P	I
Acceso a información por archivos compartidos	3	A través de archivos compartidos o en algunos casos discos duros compartidos, es posible robar información extremadamente confidencial para el Hospital que pone en riesgo la imagen y el prestigio de la misma.	3	4	7
Contraseñas débiles	3	Es posible obtener la contraseña de algunos usuarios locales y de dominio ya que éstas no cuentan con un esquema de contraseñas fuertes. Tampoco existe la educación al usuario final de seguir con los lineamientos y políticas de seguridad	4	5	9

		que establece el Hospital. No hay una configuración en el servidor de Dominio para que defina el tiempo de caducidad de las contraseñas, ni que puedan ser reutilizadas.			
Acceso no Autorizado a Redes Inalámbricas del Hospital	2	Es posible que cualquier persona externa al Hospital, obtenga la contraseña de acceso a la red inalámbrica debido a que los Access Point están configurados con un cifrado de clave muy débil (WEP). Aunado a la falta de segmentación de la red interna es visible toda la red.	5	4	9
Protocolos inseguros	1	El uso de protocolos como FTP, Telnet o POP representa un riesgo ya que la información se transmite en texto claro, la cual puede ser interceptada por un atacante para obtener cuentas de usuarios.	4	5	9
Equipos no actualizados vulnerables a explotación y acceso remoto.	7	Es posible ingresar a equipos desactualizados de forma remota por medio de la explotación de vulnerabilidades conocidas. Una vez dentro es posible ejecutar comandos a discreción. Incluso es posible obtener el archivo SAM donde se encuentran los usuarios y hashes de contraseñas.	5	5	10
Contraseñas por defecto	1	Este tipo de contraseña permite el acceso como administrador al equipo o dispositivo.	5	3	8
VNC vulnerable	6	Es posible el acceso remoto al sistema sin autenticación por el uso de VNC vulnerable	5	5	10
Acceso remoto al sistema con cuenta de Administrador	**6**	Debido a que se carece de un esquema de contraseñas fuertes y controles de acceso es posible obtener la contraseña de usuarios de Administrador de dominio y locales, lo cual permite iniciar sesión por Remote Desktop en cualquier equipo y con cualquier usuario en la red.	5	5	10
Captura de contraseñas en la red	6	El servicio Ethernet proporcionado por los switches permite que cualquier persona dentro de la red del Hospital ejecute un envenenamiento a todos los hosts incluidos en la máscara de red 255.255.0.0, con ello el atacante puede interceptar la información de las comunicaciones sin cifrado, como son usuarios y contraseñas.	5	5	10
Acceso con cuentas de correo	6	Es posible que un atacante obtenga usuarios y contraseñas de los usuarios de correo que viajan por la red local del Hospital. Así como los mensajes de correo electrónico que viajen sin cifrado.	5	5	10
Impresoras sin control de acceso	1	Debido a la falta de control de acceso a las impresoras, es posible realizar modificaciones en la configuración, alterando su funcionamiento o causando Negación de Servicio.	2	2	4
				7.3	

Tabla 3.10. Análisis de Vulnerabilidades del año 2012-1

VALOR DEL IMPACTO: 7.3

MÉTRICA: Es factible que la pérdida de confidencialidad, integridad y disponibilidad muestre un efecto serio y adverso en la organización o las personas vinculadas con ella.

3.5.1. IMPACTO

- Las carpetas compartidas han sido protegidas por una contraseña, sin embargo aun es posible obtener información confidencial debido a que es una contraseña débil que no cumple con los requerimientos mínimos sugeridos anteriormente, aunado a que la información contenida en dichas carpetas no está cifrada. Cabe mencionar que las contraseñas débiles también son utilizadas para acceso a equipos de usuarios, las cuales son fácil de obtener y descifrar.
- Aunque es posible vulnerar la red inalámbrica sólo es visible una parte del segmento en lugar de toda la red como al inicio. Los equipos que son visibles tiene archivos compartidos con información que no es considerada confidencial.
- El uso de protocolos inseguros como FTP tiene un impacto alto cuando se tiene acceso a un servidor para listar la información contenida en él y disponer de ella, así como la creación de cuentas de usuarios para asegurar el acceso.
- Los equipos no actualizados son vulnerables a ejecución de comandos remotos para obtener las cuentas de usuarios locales incluyendo la de Administrador. Lo cual impacta gravemente en caso de que haya información confidencial en dichos equipos que pueda ser extraída y usada con fines de lucro.
- Las contraseñas por default en dispositivos de red, en este caso, tiene un impacto Medio debido a que no se tiene la contraseña del usuario con privilegios para modificar la configuración.
- El servicio de VNC versión 4.1 es vulnerable y permite a un atacante conectarse sin conocer la contraseña. Lo cual proporciona control total del equipo al intruso. Esta vulnerabilidad tiene un impacto Muy Alto ya que afecta a un servidor que es fundamental para el trabajo operativo del Hospital. Dicho servidor aloja una aplicación utilizada para programar cirugías y es posible modificar medicamentos, instrumentos, horarios, etc. Si alguna persona con fines maliciosos llegará a toma control de este equipo podría provocar demandas legales por negligencia médica o algo aun más grave como la muerte de los pacientes dañando irremediablemente el prestigio del Hospital.
- El poder llevar a cabo el ataque de Man in the middle con éxito ya representa un riesgo potencial en sí mismo porque un atacante puede provocar una Denegación de Servicios, sin embargo para fines de este análisis sólo es pasivo. Aun así, fue posible interceptar cuentas de usuario del servidor de correo ya que se transfieren sin ser cifradas. Con estas cuentas es posible disponer libremente del servicio de correo electrónico.

3.5.2. RECOMENDACIONES

Acceso a información por archivos compartidos: Se recomienda usar cifrado de información, creación de particiones cifradas para almacenamiento de información sensible.

Contraseñas por defecto, débiles y Acceso remoto al sistema con cuenta de Administrador: Se recomienda la creación de un esquema de contraseñas fuertes, con más de 14 caracteres y haciendo uso de caracteres alfanuméricos, mayúsculas y

minúsculas y caracteres especiales. En el caso de contraseñas por defecto, después de la instalación de los aplicativos, es forzoso realizar la configuración correspondiente siguiendo con los lineamientos de seguridad y requerimientos del Hospital. En caso de no tenerlos definidos se debe considerar al menos el cambio de la contraseña.

Protocolos inseguros: Se recomienda erradicar el servicio FTP ya que no maneja cifrado de tráfico y puede comprometer las credenciales de acceso. Se recomienda utilizar servicios seguros como Secure Shell.

Equipos no actualizados vulnerables a explotación y acceso remoto: Se recomienda aplicar la actualización para las vulnerabilidades MS08-067 y MS12-020 tal como lo menciona Microsoft Windows en su boletín de seguridad. Con esto se evita que alguna persona no autorizada pueda ejecutar código malicioso de forma remota utilizando solicitudes RPC (Remote Procedure Call o Llamada a Procedimiento Remoto). Dichas actualizaciones se consideran críticas para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003; y se consideran importantes para todas las ediciones compatibles de Windows Vista y Windows Server 2008. Se pueden descargar de las siguientes ligas:
http://technet.microsoft.com/es-mx/security/bulletin/ms08-067
http://technet.microsoft.com/en-us/security/bulletin/ms12-020

VNC vulnerable: Se recomienda aplicar políticas de uso de software permitido en el Hospital y limitar el uso de software que permita la conectividad remota a equipos internos sino es sumamente necesario, de requerirse aplicar estrictos controles de seguridad lógica. Utilizar conexiones por servicio de VPN.

Captura de contraseñas en la red: Se recomienda definir, establecer, implementar y divulgar políticas de seguridad que contemplen:

- Revisión periódica de procesos críticos y tecnología soportada garantizando la encripción de la información transmitida.
- Activar en los switches Port Security o DHCP Snooping

Acceso con cuentas de correo: Se recomienda el fortalecimiento de contraseñas, así como realizar la clasificación de la información confidencial y adecuar los controles necesarios a cada tipo. Utilizar un protocolo seguro para la conexión con el servidor ya que el protocolo POP es visible por tanto es susceptible a captura de cuentas de usuarios.

Impresoras sin control de acceso: Se recomienda definir una contraseña fuerte a cada dispositivo de impresión para proteger el acceso a la página web de administración.

3.5.3. CONTROLES ISO 27001

A.7.2.1 Lineamientos de clasificación
A.7.2.2 Etiquetado y manejo de información.
A.8.2.2 Capacitación y educación en seguridad de la información.
A.8.2.3 Proceso disciplinario.
A.10.4.1 Controles contra software malicioso.
A.10.7.3 Procedimientos de manejo de la información.
A.10.8.1 Procedimientos y políticas de información y software.

A.10.8.2 Acuerdos de intercambio.
A.10.8.4 Mensajes electrónicos.
A.11.2.2 Gestión de privilegios
A.11.2.3 Gestión de la clave del usuario
A.11.2.4 Revisión de los derechos de acceso del usuario.
A.11.3.1 Uso de clave.
A.11.5.3 Sistema de gestión de claves.
A.11.6.2 Aislamiento del sistema sensible.
A.11.7.2 Tele-trabajo

En el **ANEXO I – ISO 27001**, se menciona una breve descripción de la clasificación de los controles de seguridad sugeridos.

3.6. Análisis del año 2012-2

En la **Tabla 3.11** se muestra las vulnerabilidades detectadas en el sexto y último análisis que se realizó a mediados del año 2012.

Nombre de la Vulnerabilidad	DA	Descripción de la Vulnerabilidad	C	P	I
Contraseñas débiles	7	Es posible obtener la contraseña de algunos usuarios locales y de dominio ya que éstas no cuentan con un esquema de contraseñas fuertes. Tampoco existe la educación al usuario final de seguir con los lineamientos y políticas de seguridad que establece el Hospital. No hay una configuración en el servidor de Dominio para que defina el tiempo de caducidad de las contraseñas, ni que puedan ser reutilizadas.	4	5	9
Protocolos inseguros	1	El uso de protocolos como FTP, Telnet o POP representa un riesgo ya que la información se transmite en texto claro, la cual puede ser interceptada por un atacante para obtener cuentas de usuarios.	4	3	7
Equipos no actualizados vulnerables a explotación y acceso remoto.	5	Es posible ingresar a equipos desactualizados de forma remota por medio de la explotación de vulnerabilidades conocidas. Una vez dentro es posible ejecutar comandos a discreción. Incluso es posible obtener el archivo SAM donde se encuentran los usuarios y hashes de contraseñas.	5	5	10
Contraseñas por defecto	2	Este tipo de contraseña permite el acceso como administrador al equipo o dispositivo.	5	5	10
VNC vulnerable	5	Es posible el acceso remoto al sistema sin autenticación por el uso de VNC vulnerable	5	5	10
Acceso remoto al sistema con cuenta de Administrador	3	Debido a que se carece de un esquema de contraseñas fuertes y controles de acceso es posible obtener la contraseña de usuarios de Administrador de dominio y locales, lo cual permite iniciar sesión por Remote Desktop en cualquier equipo y con cualquier usuario en la red.	5	5	10
Captura de contraseñas en la red	1	El servicio Ethernet proporcionado por los switches permite que cualquier persona dentro de la red del Hospital ejecute un envenenamiento a todos los hosts incluidos en la máscara de red 255.255.0.0, con ello el	5	5	10

		atacante puede interceptar la información de las comunicaciones sin cifrado, como son usuarios y contraseñas.			
Acceso con cuentas de correo	12	Es posible que un atacante obtenga usuarios y contraseñas de los usuarios de correo que viajan por la red local del Hospital. Así como los mensajes de correo electrónico que viajen sin cifrado.	5	5	10
				5.8	

Tabla 3.11. Análisis de Vulnerabilidades del año 2012-2

VALOR DEL IMPACTO: 5.8

MÉTRICA: Es posible que la pérdida de confidencialidad, integridad y disponibilidad sólo tenga un efecto limitado y adverso en la organización o las personas relacionadas a ella.

3.6.1. IMPACTO

- En cuentas de correo se sigue detectando el uso de contraseñas débiles, incluso contraseñas que ha sido usadas durante los 3 años que lleva el servicio de análisis de vulnerabilidades, es posible que lleven más tiempo, lo cual tiene un impacto Muy Alto debido a que cualquier persona con acceso a la red puede conservarla incluso cuando los controles de seguridad sugeridos se hayan implementado.
- Un dispositivo de red tiene telnet configurado lo cual permite capturar la contraseña de acceso, sin embargo no es posible realizar modificaciones al equipo ya que no se tiene una cuenta privilegiada. Cabe mencionar que ese dispositivo de red fue implementado un par de semanas antes del análisis y el administrador olvido desactivar el servicio de Telnet. Es importante destacar que cualquier descuido de los administradores son puntos vulnerables que pueden ser aprovechados por cualquier atacante.
- Se detectan equipos desactualizados y vulnerables a ejecución remota de código tal como sucedió con la vulnerabilidad reportada y corregida por Microsoft en 2008 (MS08-067 NetAPI). Ahora se conoce como MS12-020 y su explotación permite obtener los hash de cuentas de usuario locales incluyendo la de Administrador. Con ello es posible conectarse por Remote Desktop y obtener información confidencial/personal o conexiones con otros equipos.
- De los 2 servidores detectados con contraseñas por default, uno impacta a la base de datos en MySQL Server que sincroniza los dispositivos Black Berry, con ello es posible tener información personal de los empleados del Hospital.
- El otro servidor pertenece a un proveedor de Sistemas y la contraseña por default es de la aplicación web llamada Tomcat, explotando esta vulnerabilidad es posible tener acceso remoto al equipo, pero el impacto se ve reflejado al encontrar una contraseña de administrador en un block de notas en el escritorio, la cual pertenece a una aplicación que controla todos los dispositivos de red en los 2 campus del Hospital, el impacto es aún mayor ya que es posible modificar la configuración actual incluso provocar una denegación de servicios y afectar el trabajo operativo del Hospital dañando el prestigio de la misma.
- La versión de VNC usada por los 2 equipos es vulnerable a tener acceso al servidor sin conocer una cuenta de usuario válida en el sistema. Uno de los

servidores es crucial para el funcionamiento del Hospital, por tanto el impacto es muy alto.

- Los equipos no actualizados permiten la ejecución de comandos remotos para obtener las cuentas de usuarios locales incluyendo la de administrador. Esto implica que es posible tener control total de los equipos, realizar modificaciones y obtener información confidencial o personal.
- La captura de contraseñas afecta directamente al servidor de correo electrónico del Hospital por tener configurado un Protocolo inseguro como lo es POP, en el que la información se transmite en texto claro. Un atacante puede capturar cuentas de correo, tener acceso y hacer uso de la información o del servicio. Por este medio sería posible también, aplicar ingeniería social a los usuarios para obtener contraseñas de otras aplicaciones, simulando que escribe el administrador del sistema usando cualquier pretexto.

3.6.2. RECOMENDACIONES

Contraseñas por defecto, débiles y Acceso remoto al sistema con cuenta de Administrador: Se recomienda la creación de un esquema de contraseñas fuertes, con más de 14 caracteres y haciendo uso de caracteres alfanuméricos, mayúsculas y minúsculas y caracteres especiales. En el caso de contraseñas por defecto, después de la instalación de los aplicativos, es forzoso realizar la configuración correspondiente siguiendo con los lineamientos de seguridad y requerimientos del Hospital. En caso de no tenerlos definidos se debe considerar al menos el cambio de la contraseña.

Protocolos inseguros: Se recomienda erradicar el servicio FTP ya que no maneja cifrado de tráfico y puede comprometer las credenciales de acceso. Se recomienda utilizar servicios seguros como Secure Shell.

Equipos no actualizados vulnerables a explotación y acceso remoto: Se recomienda aplicar la actualización para las vulnerabilidades MS08-067 y MS12-020 tal como lo menciona Microsoft Windows en su boletín de seguridad. Con esto se evita que alguna persona no autorizada pueda ejecutar código malicioso de forma remota utilizando solicitudes RPC (Remote Procedure Call o Llamada a Procedimiento Remoto). Dichas actualizaciones se consideran críticas para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003; y se consideran importantes para todas las ediciones compatibles de Windows Vista y Windows Server 2008. Se pueden descargar de las siguientes ligas:
http://technet.microsoft.com/es-mx/security/bulletin/ms08-067
http://technet.microsoft.com/en-us/security/bulletin/ms12-020
VNC vulnerable: Se recomienda aplicar políticas de uso de software permitido en el Hospital y limitar el uso de software que permita la conectividad remota a equipos internos sino es sumamente necesario, de requerirse aplicar estrictos controles de seguridad lógica. Utilizar conexiones por servicio de VPN.

Captura de contraseñas en la red: Se recomienda definir, establecer, implementar y divulgar políticas de seguridad que contemplen:

- Revisión periódica de procesos críticos y tecnología soportada garantizando la encripción de la información transmitida.
- Activar en los switches Port Security o DHCP Snooping

Acceso con cuentas de correo: Se recomienda el fortalecimiento de contraseñas, así como realizar la clasificación de la información confidencial y adecuar los controles necesarios a cada tipo. Utilizar un protocolo seguro para la conexión con el servidor ya que el protocolo POP es visible por tanto es susceptible a captura de cuentas de usuarios.

3.6.3. CONTROLES ISO 27001

A.7.2.1 Lineamientos de clasificación
A.7.2.2 Etiquetado y manejo de información.
A.8.2.2 Capacitación y educación en seguridad de la información.
A.8.2.3 Proceso disciplinario.
A.10.4.1 Controles contra software malicioso.
A.10.7.3 Procedimientos de manejo de la información.
A.10.8.1 Procedimientos y políticas de información y software.
A.10.8.2 Acuerdos de intercambio.
A.10.8.4 Mensajes electrónicos.
A.11.2.2 Gestión de privilegios
A.11.2.3 Gestión de la clave del usuario
A.11.2.4 Revisión de los derechos de acceso del usuario.
A.11.3.1 Uso de clave.
A.11.5.3 Sistema de gestión de claves.
A.11.6.2 Aislamiento del sistema sensible.
A.11.7.2 Tele-trabajo

En el **ANEXO I – ISO 27001**, se menciona una breve descripción de la clasificación de los controles de seguridad sugeridos.

3.7. Gráficas comparativas por año

En este apartado se puede visualizar de forma gráfica la disminución del impacto de las vulnerabilidades detectadas en el Hospital por un periodo de 3 años. A pesar de que se ha trabajado constantemente junto con el personal de Sistemas encargado de corregir las vulnerabilidades se puede observar que hay problemas recurrentes en los que se requiere forzosamente otro tipo de mecanismos de seguridad como procesos disciplinarios y/o campañas de educación de seguridad de la información para el usuario final y así disminuir aún más el impacto hasta que sea muy bajo.

3.7.1. Total de Vulnerabilidades según la Prioridad

En la gráfica de la **Imagen 3.1**¡Error! No se encuentra el origen de la referencia. se observa que las vulnerabilidades detectadas en cada análisis por un periodo de 3 años, han disminuido. En esta gráfica se clasifican según la prioridad de atención. En el primer semestre del año 2012 se observa un incremento en las vulnerabilidades detectadas esto se debió a un cambio en la administración del Hospital, así como al cambio de proveedores de Sistemas. Sin embargo, para el segundo semestre del año 2012 se retomó el trabajo que se había realizado y se logró disminuir la cantidad de vulnerabilidades consideradas con una prioridad de atención **Muy alta**.

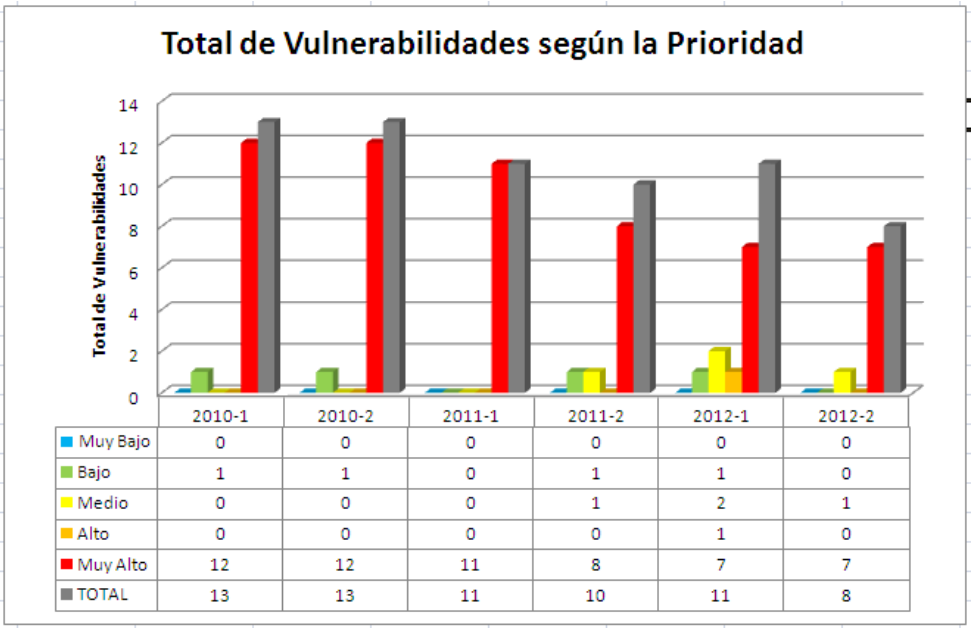


Imagen 3.1. Total de vulnerabilidades clasificadas por Prioridad

3.7.2. Total de equipos afectados

La cantidad de equipos afectados ha disminuido en cada análisis tal como lo muestra la gráfica de la **Imagen 3.2**. Cabe mencionar que la cantidad de equipos vulnerables no siempre es un buen indicador ya que basta con uno para obtener información confidencial. En este caso la cantidad de equipos afectados indica que se han aplicado algunos controles de seguridad sugeridos, aún falta aplicar algunos otros para poder mitigar el riesgo lo más que sea posible.

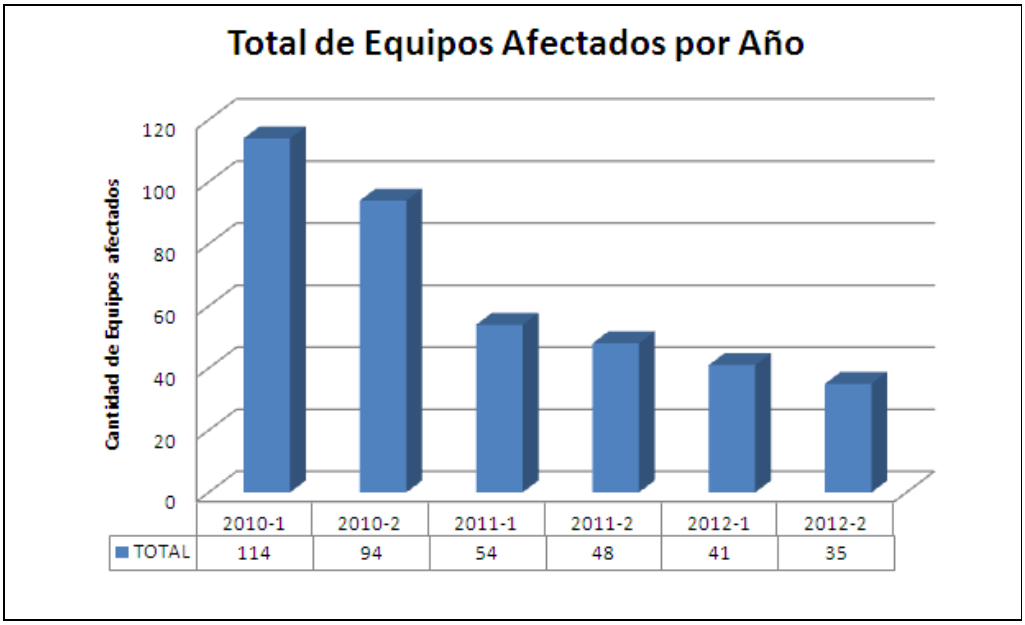


Imagen 3.2. Total de Equipos Afectados por Análisis

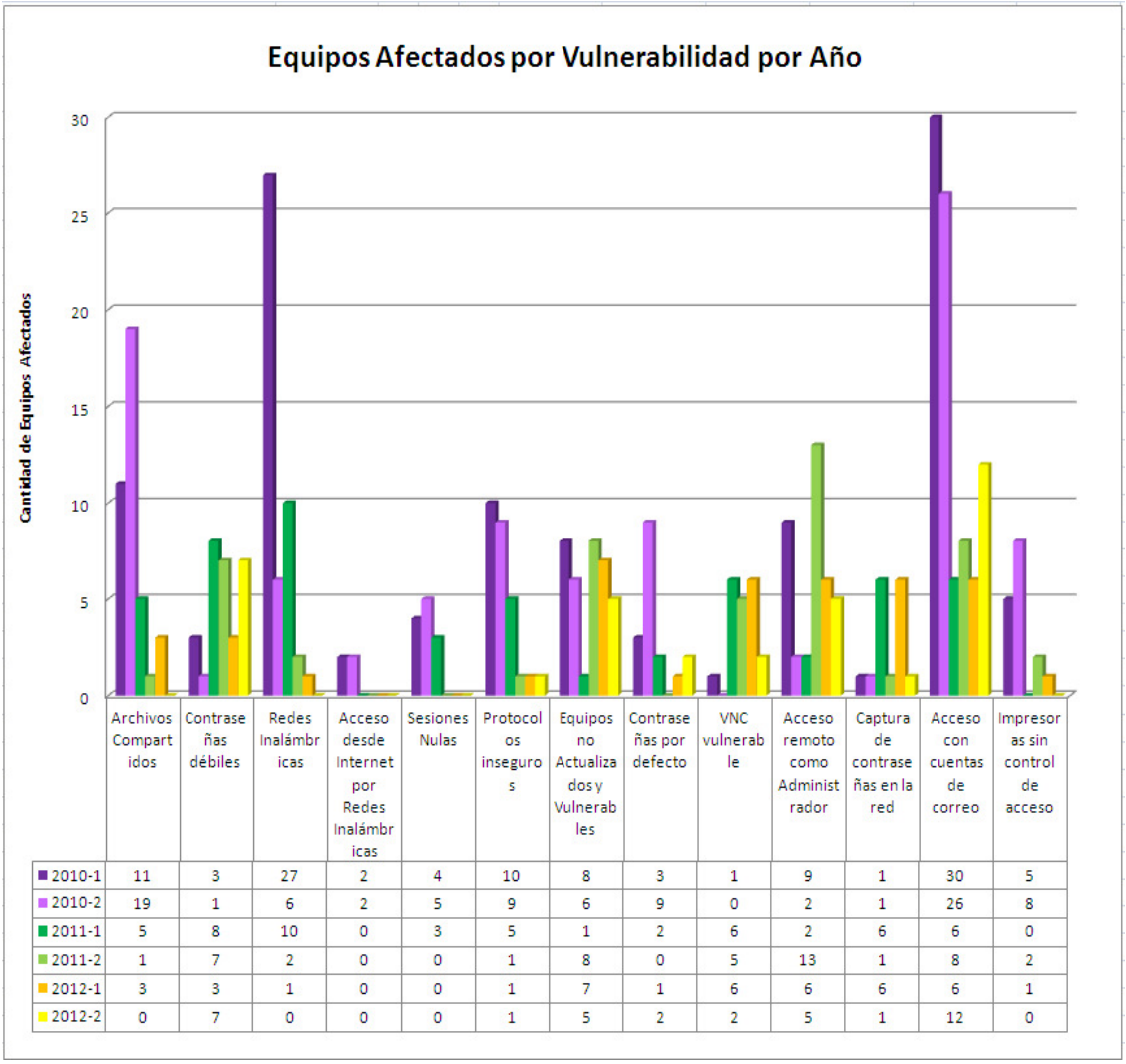
La **Tabla 3.12** muestra a detalle la cantidad de equipos afectados por cada vulnerabilidad en un periodo de 3 años. Las vulnerabilidades que al paso de los años han sido recurrentes son:

- Contraseñas débiles
- Equipos no actualizados vulnerables a explotación y acceso remoto.
- Acceso remoto al sistema con cuenta de administrador.
- Acceso con cuentas de correo.

Vulnerabilidad	2010-1	2010-2	2011-1	2011-2	2012-1	2012-2
Acceso a información por archivos compartidos	11	19	5	1	3	0
Contraseñas débiles	3	1	8	7	3	7
Acceso no Autorizado a Redes Inalámbricas del Hospital	27	6	10	2	1	0
Conexión directa y sin Restricción desde INTERNET a la red Corporativa del Hospital	2	2	0	0	0	0
Sesiones Nulas	4	5	3	0	0	0
Protocolos inseguros	10	9	5	1	1	1
Equipos no actualizados vulnerables a explotación y acceso remoto.	8	6	1	8	7	5
Contraseñas por defecto	3	9	2	0	1	2
VNC vulnerable	1	0	6	5	6	2
Acceso remoto al sistema con cuenta de Administrador	9	2	2	13	6	5
Captura de contraseñas en la red	1	1	6	1	6	1
Acceso con cuentas de correo	30	26	6	8	6	12
Impresoras sin control de acceso	5	8	0	2	1	0
	114	**94**	**54**	**48**	**41**	**35**

Tabla 3.12. Cantidad de equipos afectados por Vulnerabilidad por cada Análisis

En la gráfica de la **Imagen 3.3** se representa lo descrito en la **Tabla 3.12**.



	Archivos Compartidos	Contraseñas débiles	Redes Inalámbricas	Acceso desde Internet por Redes Inalámbricas	Sesiones Nulas	Protocolos inseguros	Equipos no Actualizados y Vulnerables	Contraseñas por defecto	VNC vulnerable	Acceso remoto como Administrador	Captura de contraseñas en la red	Acceso con cuentas de correo	Impresoras sin control de acceso
2010-1	11	3	27	2	4	10	8	3	1	9	1	30	5
2010-2	19	1	6	2	5	9	6	9	0	2	1	26	8
2011-1	5	8	10	0	3	5	1	2	6	2	6	6	0
2011-2	1	7	2	0	0	1	8	0	5	13	1	8	2
2012-1	3	3	1	0	0	1	7	1	6	6	6	6	1
2012-2	0	7	0	0	0	1	5	2	2	5	1	12	0

Imagen 3.3. Equipos afectados por Vulnerabilidad por Año

3.7.3. Disminución del Impacto por Año

En la gráfica de la **Imagen 3.4**, se muestra cada una de las vulnerabilidades detectadas por año, así como el valor del impacto en la infraestructura del Hospital. De lado derecho se obtuvo el promedio para dar el valor final para cada Análisis de Vulnerabilidades.

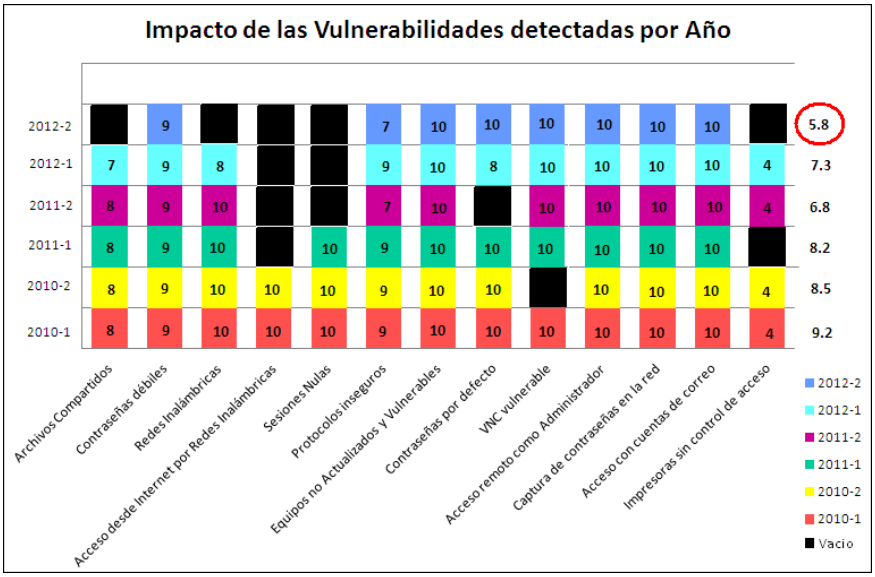


Imagen 3.4. Impacto de las Vulnerabilidades detectadas por Año

En la gráfica de la **Imagen 3.5**, se muestra que en caso de migrar el servidor de correo del Hospital, el impacto se reduce bastante. Sin embargo habría vulnerabilidades importantes por erradicar para que disminuya aún más.

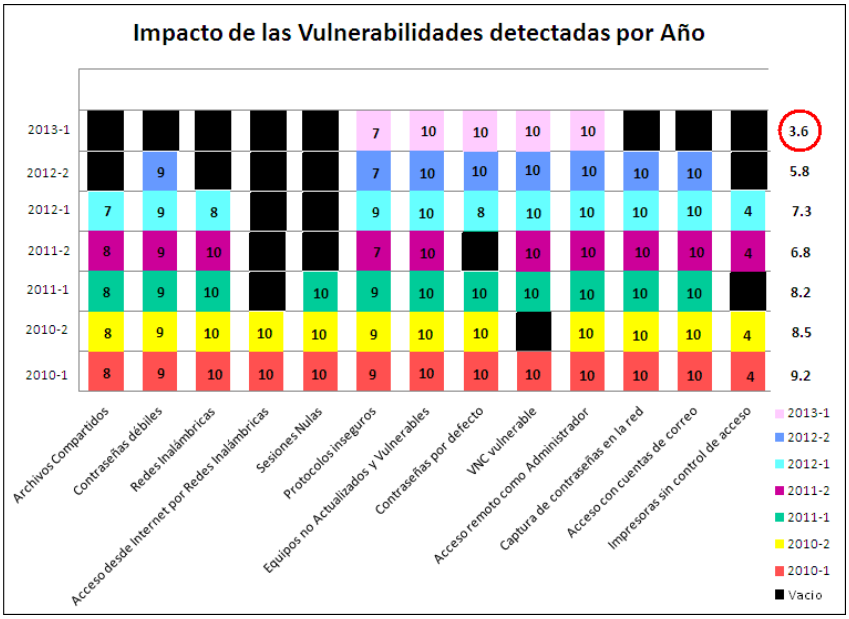


Imagen 3.5. Impacto de las Vulnerabilidades detectadas por Año incluyendo un supuesto para el año 2013

En la gráfica de la **Imagen 3.6** se puede observar claramente que el objetivo de este proyecto se está logrando. Se disminuyó el Impacto un 37% aproximadamente, respecto al inicio del proyecto. Cabe mencionar que a principios del año 2012 se detecta un aumento considerable esto fue porque en el Hospital hubo un cambio de administración la cual reflejó el impacto en la seguridad de los equipos que ya se habían trabajado. Sin embargo, a mediados del año 2012 fue posible recuperar el rumbo y se logró disminuir el impacto de las vulnerabilidades detectadas.

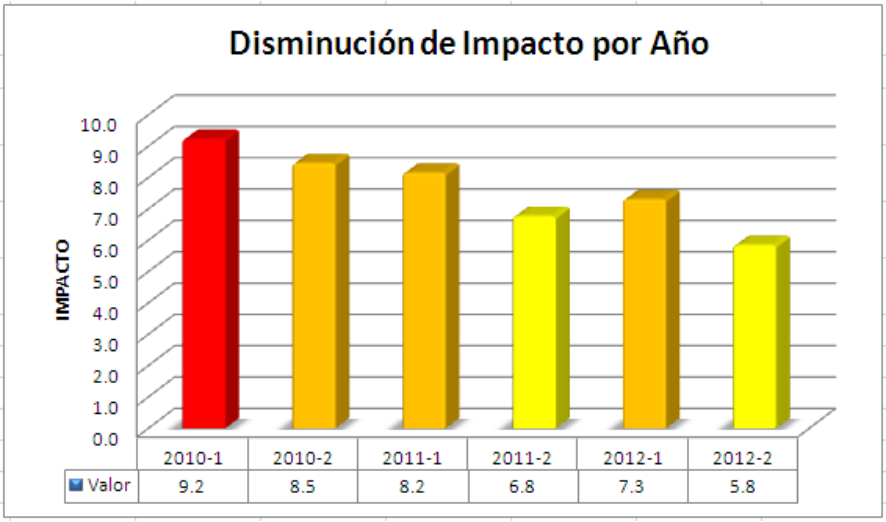


Imagen 3.6. Disminución de Impacto en un periodo de 3 años

El Hospital sigue teniendo una vulnerabilidad recurrente desde el inicio del proyecto la cual está considerada con un Impacto Muy Alto. Dicha vulnerabilidad es la **captura de contraseñas en la red**, la cual permite a un usuario no autorizado obtener contraseñas de cuentas de correo que viajan en texto claro. Una vez teniendo esas cuentas es posible acceder a información confidencial y personal como cuentas de otros dispositivos, expedientes, reportes del área de Sistemas solicitando cuentas de usuario de diversas aplicaciones, posibles contraseñas de usuarios SAP, etc. El Hospital migrará el servidor de correo a inicios del año 2013, de lo cual se podría deducir que el Impacto disminuirá hasta un 60% aproximadamente respecto al inicio del proyecto.

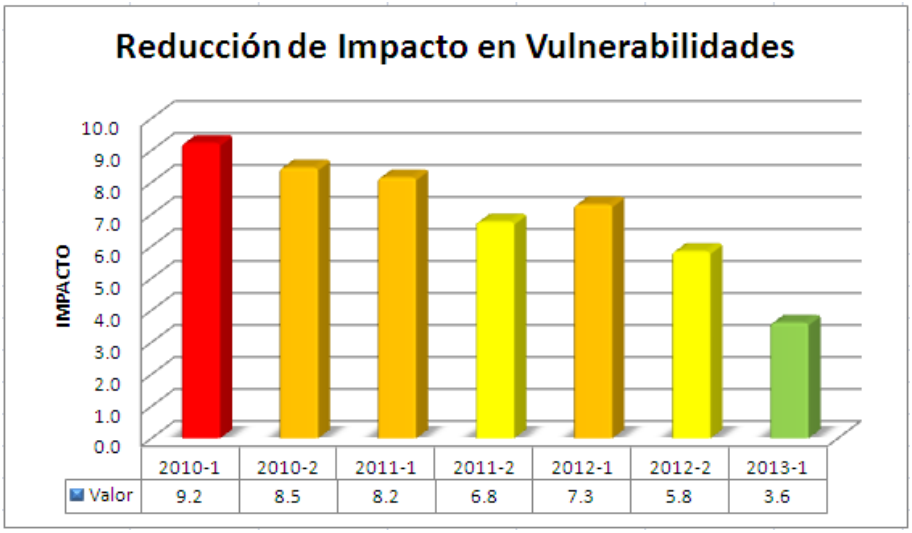


Imagen 3.7. Disminución de impacto corrigiendo la captura de contraseñas o migrando el Servidor de Correo

La gráfica de la **Imagen 3.7** muestra como disminuiría drásticamente el Impacto de las Vulnerabilidades migrando el servidor de correo y cifrando la comunicación, así en caso de ser interceptada no sería entendible.

CONCLUSIONES

Tomando en cuenta los resultados de los análisis de Vulnerabilidades y Pruebas de Penetración realizados en un lapso de 3 años, el Hospital decidió reducir gradualmente la cantidad de proveedores de Servicios de Cómputo ya que algunos de ellos no cumplían con lineamientos básicos en cuanto a seguridad de la información se refiere.

El área de Sistemas de Cómputo del Hospital ha adquirido los conocimientos necesarios para controlar las actividades de los proveedores y aplicar los controles de seguridad sugeridos.

Cabe mencionar que es muy importante aplicar las políticas de seguridad en general, pero primordialmente las relacionadas con CONFIDENCIALIDAD e INTEGRIDAD ya que la extracción y/o modificación de la información sensible puede perjudicar enormemente el prestigio y la reputación del Hospital dañando considerablemente su imagen ocasionando pérdidas incuantificables.

También, es importante recordar a los administradores y personal encargado del área de Sistemas que cualquier cambio efectuado en la red se debe realizar siguiendo los lineamientos, procedimientos, políticas y controles de seguridad del Hospital de lo contrario podrían dejar una entrada a un atacante, empleado molesto o cualquier persona que pretenda robar información indebidamente y usarla con fines de lucro.

Finalmente se puede concluir que con el trabajo conjunto del Hospital y la consultoría se logró reducir el nivel de impacto causado por las vulnerabilidades detectadas. Sin embargo, es indispensable un plan de concientización del personal del Hospital para que entiendan la importancia de la seguridad de la información y el impacto que puede causar la fuga de la misma, así como fomentar la cultura del buen uso de las contraseñas y los recursos dentro y fuera del Hospital. Así mismo es fundamental que la Alta Gerencia impulse la implementación de los controles de seguridad para mitigar los riesgos actuales y futuros.

ANEXO I – ISO27001

A continuación se mencionan de forma muy general algunos de los controles sugeridos en cada análisis de Vulnerabilidades y Pruebas de Penetración. Cabe mencionar que cada uno de estos controles se subdivide siendo más específicos y detallados pero para fines de este trabajo no es necesario mostrar tal detalle.

A.7 Administración de recursos

Este grupo cubre cinco controles y también se encuentra subdividido en:

- **Responsabilidad en los recursos:** Inventario y propietario de los recursos, empleo aceptable de los mismos.
- **Clasificación de la información:** Guías de clasificación y Denominación, identificación y tratamiento de la información.

A.8 Seguridad de los recursos humanos.

Este grupo cubre nueve controles y también se encuentra subdividido en:

- **Antes del empleo:** Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.
- **Durante el empleo:** Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias.
- **Finalización o cambio de empleo:** Finalización de responsabilidades, devolución de recursos, revocación de derechos.

Este grupo trata de un serio trabajo a realizar entre el departamento de Recursos Humanos y los responsables de Seguridad de la Información de la organización. Se debe partir por la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos, en la cual deberán quedar bien definidas las acciones a seguir para los diferentes perfiles de la organización, basados en la responsabilidad de manejo de información que tenga ese puesto. Tanto la contratación como el cese de un puesto, es una actividad conjunta de estas dos áreas, y cada paso deberá ser coordinado, según la documentación confeccionada, para que no se pueda pasar por alto ningún detalle, pues son justamente estas pequeñas omisiones de las que luego resulta el haber quedado con alta dependencia técnica de personas cuyo perfil es peligroso, o que al tiempo de haberse ido, mantiene accesos o permisos que no se debieran. En cuanto a formación, para dar cumplimiento al estándar, no solo es necesario dar cursos. Hace falta contar con un Plan de formación.

A.10 Administración de las comunicaciones y operaciones

Este grupo comprende treinta y dos controles, es el más extenso de todos y se divide en:

- **Procedimientos operacionales y responsabilidades:** Tiene como objetivo asegurar la correcta y segura operación de la información, comprende cuatro controles. Hace especial hincapié en documentar todos los procedimientos, manteniendo los mismos y disponibles a todos los

usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar uso inadecuado de los mismos. Esta tarea en todas las actividades de seguridad (no solo informática), se suele realizar por medio de lo que se denomina Procedimientos Operativos Normales (PON) o Procedimientos Operativos de Seguridad (POS), y en definitiva consiste en la realización de documentos breves y ágiles, que dejen por sentado la secuencia de pasos o tareas a llevar a cabo para una determinada función. La enorme ventaja que ofrecen los procedimientos es:

- Identificar con absoluta claridad los responsables y sus funciones.
- Evitar que ciertos administradores sean imprescindibles.
- Detectar ausencias de zonas sin procedimientos que a menudo se vuelven puntos vulnerables.

- **Administración de prestación de servicios de terceras partes:** Abarca tres controles, se refiere fundamentalmente, como su nombre lo indica, a los casos en los cuales se encuentran tercerizadas determinadas tareas o servicios del propio sistema informático. Los controles están centrados en tres aspectos fundamentales de esta actividad:
  - Documentar adecuadamente los servicios que se están prestando (obligaciones, responsabilidades, confidencialidad, operación, mantenimiento, etc.).
  - Medidas a adoptar para la revisión, monitorización y auditoría de los mismos.
  - Documentación adecuada que permita regularizar y mantener un eficiente control de cambios en estos servicios.

- **Planificación y aceptación de sistemas:** El objetivo es realizar una adecuada metodología para que al entrar en producción cualquier sistema, se pueda minimizar el riesgo de fallos. De acuerdo a la magnitud de la empresa y al impacto del sistema a considerar, siempre es una muy buena medida la realización de un ambiente de desarrollo y pruebas. Este ambiente deberá "acercarse" todo lo posible al entorno en producción. Los dos aspectos claves de este control son el diseño, planificación, prueba y adecuación de un sistema por un lado; y el segundo, es desarrollar detallados criterios de aceptación de nuevos sistemas, actualizaciones y versiones que deban ser implantados.

- **Protección contra código móvil y maligno:** el objetivo de este apartado es la protección de la integridad del software y la información almacenada en los sistemas. El código móvil es aquel que se transfiere de un equipo a otro para ser ejecutado en el destino final, este empleo es muy común en las arquitecturas cliente-servidor. En cuanto al código malicioso, el estándar hace referencia al conjunto de medidas comunes que ya suelen ser aplicadas en la mayoría de las empresas, es decir, detección, prevención y recuperación de la información ante cualquier tipo de virus. No es eficiente el mejor producto antivirus del mercado, sino se realizan dos tareas importantes: Preparación del personal e implementación de procedimientos.

- **Resguardo:** El objetivo de esta apartado conceptualmente es muy similar al anterior, comprende un solo control que remarca la necesidad de las copias de respaldo y recuperación.

- **Administración de la seguridad de redes:** Los dos controles que conforman este apartado hacen hincapié en la necesidad de administrar y controlar lo que sucede en la red, es decir, implementar todas las medidas posibles para evitar amenazas, manteniendo la seguridad de los sistemas y aplicaciones a través del conocimiento de la información que circula por ella. Se deben implementar controles técnicos, que evalúen permanentemente los servicios que la red ofrece, tanto propios como de terceros.

- **Manejo de medios:** Como "medio" debe entenderse todo elemento capaz de almacenar información (discos, cintas, papeles, etc. tanto fijos como removibles). Por lo tanto el objetivo de este grupo es, a través de sus cuatro controles, prevenir la difusión, modificación, borrado o destrucción de cualquiera de ellos ya sea física o lógicamente.

- **Intercambios de información:** Este grupo contempla el conjunto de medidas a considerar para cualquier tipo de intercambio de información, tanto en línea como fuera de ella, y para movimientos internos o externos de la organización. Los aspectos que no se deben descuidar son:
    - Políticas, procedimientos y controles para el intercambio de información para tipo y medio de comunicación a emplear.
    - Acuerdos, funciones, obligaciones, responsabilidades y sanciones de todas las partes intervinientes.
    - Medidas de protección física de la información en tránsito.
    - Consideraciones para los casos de mensajería electrónica
    - Medidas particulares a implementar para los intercambios de información de negocio, en especial con otras empresas.

- **Monitorización:** Este apartado tiene como objetivo la detección de actividades no autorizadas en la red y reúne seis controles. Los aspectos más importantes a destacar son:
    - Auditar Logs que registren actividad, excepciones y eventos de seguridad.
    - Realizar revisiones periódicas y procedimientos de monitorización del uso de los sistemas.
    - Implementación de robustas medidas de protección de los Logs de información de seguridad.
    - La actividad de los administradores y operadores de sistemas, también debe ser monitorizada, pues es una de las mejores formas de tomar conocimiento de actividad sospechosa, tanto si la hace un administrador propio de la empresa (con o sin mala intención) o si es uno que se hace pasar por uno de ellos.
    - Es necesario implementar un sistema de alarmas que monitorice el normal funcionamiento de los sistemas de generación de eventos de seguridad y/o Logs.

- Sincronización de tiempos. Una buena opción es el uso del protocolo NTP (Network Time Protocol). Ya que cuando llega la hora de investigar, monitorizar o seguir cualquier actividad sospechosa es fundamental tener una secuencia cronológica lógica que permita moverse por todos los sistemas de forma coherente.

A.11 Control de accesos

No se debe confundir la actividad de control de accesos con autenticación, esta última tiene por misión identificar que verdaderamente "sea, quien dice ser". El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro. Este apartado tiene veinticinco controles, que los agrupa de la siguiente forma:

- **Requerimientos de negocio para el control de accesos:** Debe existir una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.

- **Administración de accesos de usuarios:** Tiene como objetivo asegurar el correcto acceso y prevenir el no autorizado y, a través de cuatro controles, exige llevar un procedimiento de registro y revocación de usuarios, una adecuada administración de los privilegios y de las contraseñas de cada uno de ellos, realizando periódicas revisiones a intervalos regulares, empleando para todo ello procedimientos formalizados dentro de la organización.

- **Responsabilidades de usuarios:** Todo usuario dentro de la organización debe tener documentadas sus obligaciones dentro de la seguridad de la información de la empresa.
  Independientemente de su jerarquía, siempre tendrá alguna responsabilidad a partir del momento que tenga acceso a la información. Evidentemente existirán diferentes grados de responsabilidad, y proporcionalmente a ello, las obligaciones derivadas de estas funciones. Por lo tanto de este ítem se derivan tres actividades.
  - Identificar niveles y responsabilidades.
  - Documentarlas correctamente.
  - Difundirlas y verificar su adecuada comprensión.

  Para estas actividades propone tres controles, orientados a que los usuarios deberán aplicar un correcto uso de las contraseñas, ser conscientes del equipamiento desatendido (por lugar, horario, lapsos de tiempo, etc.) y de las medidas fundamentales de cuidado y protección de la información en sus escritorios, medios removibles y pantallas.

- **Control de acceso a redes:** Todos los servicios de red deben ser susceptibles de medidas de control de acceso; para ello a través de siete controles, en este grupo se busca prevenir cualquier acceso no autorizado a los mismos. Como primera medida establece que debe existir una política

de uso de los servicios de red para que los usuarios, solo puedan acceder a los servicios específicamente autorizados. Luego se centra en el control de los accesos remotos a la organización, sobre los cuales deben existir medidas apropiadas de autenticación. En los controles de este grupo menciona medidas automáticas, segmentación, diagnóstico y control equipamiento, direcciones y de puertos, control de conexiones y rutas de red. Para toda esta actividad se deben implementar: IDSs, IPSs, FWs con control de estados, honey pots, listas de control de acceso, certificados digitales, protocolos seguros, túneles, etc.

- **Control de acceso a sistemas operativos:** El acceso no autorizado a nivel sistema operativo presupone uno de los mejores puntos de escalada para una intrusión. Este grupo de controles proponen seguridad en la validación de usuarios del sistema operativo, empleo de identificadores únicos de usuarios, correcta administración de contraseñas, control y limitación de tiempos en las sesiones.

- **Control de acceso a información y aplicaciones:** Este grupo contiene dos controles y están dirigidos a prevenir el acceso no autorizado a la información mantenida en las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y a su vez el aislamiento de los sistemas sensibles del resto de la infraestructura como por ejemplo sistemas críticos, salas de terapia intensiva, centrales nucleares, servidores primarios de claves, sistemas de aeropuertos, militares, etc., los cuales no pueden ser accedidos de ninguna forma vía red, sino únicamente estando físicamente en ese lugar.

- **Movilidad y teletrabajo:** Esta nueva estructura laboral, se está haciendo cotidiana en las organizaciones y presenta una serie de problemas desde el punto de vista de la seguridad:
  - Accesos desde un ordenador de la empresa, personal o público.
  - Posibilidades de instalar o no, medidas de hardware/software seguro en el equipo remoto.
  - Canales de comunicaciones por los cuales se accede (red pública, privada, GPRS, UMTS, WiFi, Túnel, etc.).
  - Contratos que se posean sobre estos canales.
  - Personal que accede ya sea propio, de terceros o ajeno.
  - Lugar remoto: fijo o variable.
  - Aplicaciones e información a la que accede.
  - Nivel de profundidad en las zonas de red a los que debe acceder.
  - Volumen y tipo de información que envía y recibe.
  - Nivel de riesgo que se debe asumir en cada acceso.

La norma no entra en mayores detalles, pero de los dos controles que propone se puede identificar que la solución a esto es adoptar una serie de procedimientos que permitan evaluar, implementar y controlar adecuadamente estos aspectos en el caso de poseer accesos desde ordenadores móviles y/o teletrabajo.

GLOSARIO

ACCESS POINT: Es un dispositivo utilizado en redes inalámbricas de área local y se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

ARP: (Address Resolution Protocol o Protocolo de Resolución de Direcciones) como su nombre lo indica es un protocolo utilizado para la resolución de direcciones en informática, es el responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP.

CEH: (Certified Ethical Hacker) es una certificación que provee a un profesionista de habilidades para encontrar vulnerabilidades en los sistemas utilizando el mismo conocimiento y herramientas que un hacker malicioso con la diferencia de que no interfiere con el trabajo operativo y notifica los puntos vulnerables para que puedan ser corregidos.

DHCP: Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Host es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

DHCP SNOOPING: Es una funcionalidad de seguridad disponible en los switches. Su principal cometido es prevenir que un servidor DHCP no autorizado entre en la red. DCHP snooping permite además, en combinación con otras funcionalidades de seguridad evitar ARP spoofing, envenenamiento ARP e IP spoofing en la red.

EC-COUNCIL: Es una organización internacional con base en Malasia, dedicada al desarrollo de cursos y al otorgamiento de certificaciones en las áreas de Seguridad de la Información y Comercio Electrónico.

ENRUTAMIENTO: Es la función del Router para buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

EXPLOIT: Es una secuencia de comandos que tienen la finalidad de causar un error o un fallo en alguna aplicación provocando un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico. Con frecuencia, esto incluye cosas tales como la toma de control de un sistema de cómputo o permitir la escalada de privilegios o un ataque de denegación de servicio.

FTP: Siglas de File Transfer Protocol es un método muy común para transferir uno o más ficheros de un ordenador a otro. La principal desventaja de este protocolo es que la información es transferida en texto claro, por tanto es posible interceptarla.

HASH: Es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte en un rango de salida finito, normalmente cadenas de longitud fija. Por ejemplo si tenemos la palabra zorro y se le aplica la función hash, su hash seria DFCD3454.

IEEE: (Institute of Electrical and Electronics Engineers) en español Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización. Según el mismo IEEE, su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.

IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.

ISECOM: Es la autoridad oficial para las certificaciones OSSTMM Professional Security Tester (OPST) y OSSTMM Professional Security Analyst (OPSA).

ISO27001: Es un estándar diseñado para la gestión de la seguridad de la Información.

OSSTMM: (Open Source Security Testing Methodology Manual) es un manual de metodologías para pruebas y análisis de seguridad.

OUTSOURCING: Es el proceso económico en el cual una empresa mueve o destina los recursos orientados a cumplir ciertas tareas hacia una empresa externa por medio de un contrato. Esto se da especialmente en el caso de la subcontratación de empresas especializadas.

OSI: El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), también llamado OSI (en inglés open system interconnection) es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Consta de 7 niveles: Nivel Físico, Nivel de Enlace de Datos, Nivel de Red, Nivel de Transporte, Nivel de Sesión, Nivel de Presentación y Nivel de Aplicación.

POP: En informática se utiliza el Post Office Protocol (POP3, Protocolo de Oficina de Correo o "Protocolo de Oficina Postal") en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

PORT SECURITY: Es un feature (rasgo) de los switches Cisco que permite retener las direcciones MAC conectadas a cada puerto del dispositivo o switch y permitir solamente a esas direcciones MAC registradas comunicarse a través de ese puerto del switch. Esto permite: Restringir el acceso a los puertos del switch según la MAC; restringir el número de MACs por puerto en el switch; reaccionar de diferentes maneras a violaciones de las restricciones anteriores y establecer la duración de las asociaciones MAC-Puerto. Si un dispositivo con otra dirección MAC intenta comunicarse a través de un puerto de la LAN, port-security deshabilitará el puerto.

RDP: Remote Desktop Protocol es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón ó el teclado).

ROUTER: Es un dispositivo de red que se considera más " inteligente" que el switch, pues, además de cumplir la misma función, también tiene la capacidad de escoger la mejor ruta que un determinado paquete de datos debe seguir para llegar a su destino.

RPC: El Remote Procedure Call (RPC) (del inglés, Llamada a Procedimiento Remoto) es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos. El protocolo es un gran avance sobre los sockets usados hasta el momento. De esta manera el programador no tenía que estar pendiente de las comunicaciones, estando éstas encapsuladas dentro de las RPC.

SAM: Security Accounts Manager = Gestor de Seguridad de las Cuentas. Es una base de datos almacenada como un fichero del registro en Windows NT, Windows 2000, y versiones posteriores de Microsoft Windows. Almacena las contraseñas de los usuarios en un formato con hash (seguro, cifrado).

SAP: "SAP Systemanalyse, Anwendungen und Programmentwicklung". El nombre fue tomado de la división en la que trabajaban en IBM. El nombre SAP R/3 es al mismo tiempo el nombre de una empresa y el de un sistema informático. Este sistema comprende muchos módulos completamente integrados, que abarca prácticamente todos los aspectos de la administración empresarial. SAP proporciona la oportunidad de sustituir un gran número de sistemas independientes, que se han desarrollado e instalado en organizaciones ya establecidas, por un solo sistema modular.

SSID: El SSID (Service Set IDentifier) es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos (aunque el estándar no lo especifica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

SWITCH: es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

TELNET: (TELecommunication NETwork) es el nombre de un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23. Sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía.

TERMINAL SERVICES: Los Servicios de Escritorio Remoto (del inglés Remote Desktop Services), antiguamente conocido como Servicios de Terminal (o Terminal Services) son un componente de los sistemas operativos Windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red.

TEST: Test es una palabra inglesa aceptada por la Real Academia Española (RAE). Este concepto hace referencia a las pruebas destinadas a evaluar conocimientos, aptitudes o funciones.

TESTEO: Someter a una persona o una cosa a un test.

VLAN: Una VLAN (acrónimo de virtual LAN, «red de área local virtual») es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

VNC: Es un programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. También llamado software de escritorio remoto. VNC no impone restricciones en el sistema operativo del ordenador servidor con respecto al del cliente: es posible compartir la pantalla de una máquina con cualquier sistema operativo que soporte VNC conectándose desde otro ordenador o dispositivo que disponga de un cliente VNC portado.

VPN: Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada. Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

WEP: (Wired Equivalent Privacy) es un sistema de cifrado para el estándar IEEE 802.11 como protocolo para redes Wi-Fi.

WPA: (Wi-Fi Protected Access) es una clase de sistemas de seguridad para redes inalámbricas. Fue creado en respuesta a los serios problemas y debilidades encontrados en el sistema de seguridad anterior llamado WEP.

WPA2 : WPA2 o Wi-Fi Protected Access 2, también conocido como IEEE 802.11i. Se trata de una enmienda en la seguridad del estándar 802.11 (WPA). WPA2 establece medidas estándares de seguridad para redes inalámbricas. WPA2 utiliza CCMP [*Counter-mode/CBC-MAC Protocol*] basado en AES [*Advanced Encrytion System*]

REFERENCIA BIBLIOGRÁFICA

Ethical Hacking and Countermeasures v6.1 Copyright © by **EC-Council**
All Rights Reserved.

ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems ***– Requirements.***

Herzog, Peter. *OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad.* 2000-2003. [Documento en línea] Disponible en: http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

Herzog Peter. *OSSTMM 3 L I T E, Introduction and Sample to the Open Source Security Testing Methodology Manual.* Agosto 2008. [Documento en línea] Disponible en: http://www.idpnow.net/Documents/OSSTMM_3.0_LITE.pdf

Portal de actualizaciones de Microsoft [Página en línea] Disponible en: http://support.microsoft.com/kb/246261

Portal de boletines de Microsoft [Documentos en línea] Disponible en:
http://technet.microsoft.com/es-mx/security/bulletin/ms08-067
http://technet.microsoft.com/en-us/security/bulletin/ms12-020