CAPÍTULO 4
Buenas Prácticas de Seguridad

"El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en un caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy bien armados y pagados. Aun así, no apostaría mi vida por él". [Eugene Spafford].

4.1. Justificar por qué invertir en seguridad

Tal vez uno de los puntos más importantes al momento de tratar de implementar una solución de seguridad es demostrar la necesidad de invertir en este rubro, debido a que es complicado cuantificar el daño que representa la afectación de un principio de seguridad en un bien, algunos de los mecanismos para esto son los siguientes:

- Retorno de inversión, se logra demostrar en términos financieros que la inversión en seguridad será rentable para la compañía y que sus beneficios van más allá del ámbito de seguridad.

- Desarrollar una demostración presencial de qué tan sencillo resulta comprometer un sistema con la finalidad de mostrar la gravedad del problema.

- Regulaciones, las compañías invierten en seguridad para cumplir con alguna regulación a la cual están sujetas, dependiendo el tamaño de éstas.

- Clasificar la escala de gravedad de un incidente, para catalogar los hechos de seguridad en función del impacto sobre el sistema de información, se trata en algunos casos de medir una pérdida económica, y en otros, comparecer ante un tribunal. Por tal motivo es fundamental comprender que esta medición de la gravedad de un incidente debe realizarse tras una gestión de los riesgos (tabla 4.1).

Tabla 4. 1 Escala de gravedad de un incidente.

Categoría	Nivel	Gravedad	Criterio
Parada	5	Inaceptable	El hecho cuestiona la supervivencia de la empresa.
	4	Muy importante	El hecho presenta un riesgo muy importante y necesita medidas de urgencia inmediatas.
Degradación	3	Importante	El hecho no ocasiona riesgo importante alguno, pero se toca una parte significativa del sistema.
	2	Media	El hecho tiene una consecuencia sobre el funcionamiento normal y debe generar una reacción inmediata.
Perturbación	1	Leve	El hecho no tiene consecuencias notables pero debe tratarse para restablecer el funcionamiento normal
Funcionamiento normal	0	Ninguna importancia desde el punto de vista de la seguridad	Funcionamiento normal

- Apegarse a estándares internacionales con la finalidad de brindarle prestigio a la institución, requieren de mayores recursos económicos.
- Demostrar que lo que se ha gastado en seguridad es lo correcto con respecto, al valor de la información a proteger.
- Demostrar el impacto que se produce si se compromete cierta información, o se deja de brindar un servicio por algún tiempo.

4.2. Buenas prácticas en la administración de la seguridad con base en estándares

Los estándares internacionales son una muy buena guía que proporcionan un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización. [37]

Entre los puntos importantes a considerar con relación a los estándares internacionales, enfocándose en el ISO 27001 se encuentran:

1. Adoptan algún modelo para aplicarse a los procesos de SGSI, como lo es el modelo Planear-Hacer-Checar-Actuar (PDCA – Plan-Do-Check-Act), Figura 4.1. La adaptación del modelo PDCA también refleja los principios tal como se establecen en los lineamientos OECD (2002).[38]

    a) ***Planear (establecer el SGSI):*** Establecer políticas, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

    b) ***Hacer (implementar y operar el SGSI):*** Implementar y operar la política, controles, procesos y procedimientos SGSI.

    c) ***Checar (Monitorear y revisar el SGSI):*** Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.

    d) ***Actuar (mantener y mejorar el SGSI):*** Tomar acciones correctivas y preventivas, basados en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante para lograr el mejoramiento continuo SGSI.

[37] Estándar Internacional ISO/IEC 27001, Primera edición, Referencia ISO/IEC 27001:2005

[38] Guias de la OCDE para la seguridad de los sistemas de información y redes, http://www.anacom.pt/streaming/1946922.pdf?categoryId=45842&contentId=132698&field=ATTACHED_FILE

Figura 4. 1 modelo PDCA.

2. Un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de varios estándares.

La organización por su parte debe hacer lo siguiente:

1. Permiten definir el alcance y los limites de SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología, incluyendo los detalles de la justificación de cualquier exclusión del alcance.

2. La creación de una política de SGSI en términos de las características del negocio, la organización, activos y tecnología.

3. Permite definir las líneas a seguir para realizar el análisis de riesgo, que contempla:
    b) Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.
    c) Identificar las amenazas para aquellos activos.
    d) Identificar las vulnerabilidades que podrán ser aprovechadas por las amenazas.
    e) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.
    f) Calcular la probabilidad realista de que ocurra dicha falla.
    g) Determinar si el riesgo es aceptable o requiere tratamiento.
    h) Identificar y evaluar las opciones para el tratamiento de los riesgos, las acciones posibles incluyen:

        - Aplicar los controles apropiados.
        - Aceptar los riesgos conscientes y objetivamente siempre que se satisfagan claramente las políticas y el criterio de aceptación del riesgo de la organización.
        - Transferir los riesgos comerciales asociados a otras entidades, por ejemplo: aseguradores, proveedores.

4. Seleccionar objetivos de control y controles para el tratamiento de riesgo, esta selección debe tomar en cuenta el criterio para aceptar los riesgos, así como los requerimientos legales, reguladores y contractuales.

5. Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

6. Obtener la autorización de la gerencia para implementar y operar el SGSI.

7. Implementar los procedimientos y otros controles capaces de permitir una pronta detección y respuesta a incidentes de seguridad.

8. Implementar los programas de capacitación y conocimiento.

9. Ejecutar procedimientos de monitoreo y revisión y otros controles para :

    a) Identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos
    b) Permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante alguna tecnología se están realizado como se esperaba.
    c) Realizar revisiones regulares de la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
    d) Actualizar los planes de seguridad para tomar en cuenta las actividades de monitoreo y revisión.
    e) Registrar las acciones o eventos que podrían tener un impacto sobre la efectividad.

10. Realizar auditorías internas a intervalos planeados, contemplando:

    a) Que se cumplan los requerimientos del estándar.
    b) Cumple con los requerimientos de seguridad.
    c) Se implementa y mantiene de manera efectiva.
    d) La selección de los auditores y la realización de las auditorías debe asegurar la objetividad e imparcialidad del proceso de auditoría.
    e) Los auditores no pueden auditar su propio trabajo.
    f) Las responsabilidades y requerimientos para la planeación y realización de las auditorías y para el reporte de los resultados y mantenimiento de registros se debe definir en un proceso documentado.
    g) La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no conformidades detectadas.

11. Actualizar los planes de seguridad para tomar en cuenta las actividades de monitoreo y revisión.

12. Implementar las mejoras identificadas en el SGSI.

13. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones.

14. Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle de acuerdo con las circunstancias.

15. Asegurar que las mejoras logren su objetivo señalado.

La documentación del SGSI debe incluir lo siguiente:

1. Enunciados documentados de la política y los objetivos.
2. El alcance del SGSI.
3. Procedimientos y controles del SGSI.
4. Una descripción de la metodología de evaluación de riesgos.
5. Reporte de la evaluación de riesgos.
6. Plan de tratamiento del riesgo.
7. Los procedimientos necesarios por la organización se establecen, documentan, implementan y mantienen para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles.
8. Revisar y actualizar los documentos conforme sea necesario y re aprobar los documentos.
9. Asegurar que se identifiquen los cambios y el estado de la revisión actual de los documentos.
10. Los documentos pueden estar en cualquier forma o medio.
11. Se debe establecer un proceso documentado para definir las acciones gerenciales para:
    a) Aprobar la idoneidad de los documentos antes de su emisión.
    b) Revisar y actualizar los documentos conforme sea necesario.
    c) Asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso.
    d) Asegurar que los documentos se mantengan legibles y fácilmente identificables.
    e) Asegurar que se controle la distribución de los documentos.
    f) Evitar el uso indebido de documentos obsoletos.

12. Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva, deben protegerse y controlarse.

13. Se debe mantener registro del desempeño de los procesos y de todas las ocurrencias de incidentes de seguridad significativos.

14. La gerencia debe establecer compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora.

a) Establecer una política SGSI.
b) Asegurar que se establezcan objetivos y planes SGSI.
c) Establecer roles y responsabilidades para la seguridad de la información.
d) Comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de una mejora continua.

15. Propiciar la capacitación o realizar otras acciones (por ejemplo emplear al personal competente) para satisfacer estas necesidades.

De manera resumida éstos son algunos puntos principales en los cuales se puede apoyar para definir un esquema de seguridad de la información, ya que permite llevar el proceso de forma ordenada y efectiva.

4.3. Buenas prácticas de seguridad en redes

En la actualidad la aplicación de buenas prácticas en los esquemas de seguridad de las organizaciones, permite responder de una mejor manera frete a los incidentes, ya que se contemplan las mejores experiencias para cada caso. En el presente tema se pretende destacar la importancia de las buenas prácticas de seguridad en redes, a continuación se muestra una lista de las cuestiones que se deben tomar en cuenta para garantizar un nivel de seguridad adecuado en las redes de datos:

- Contar con políticas de seguridad basados en modelos como COBIT y estándares como ISO 27001.
- Realizar planes de contingencia en caso de incidentes BRP (Business Recovery Plan- Plan de recuperación del negocio), BCP (Business Continuity Plan – Plan de continuidad del negocio).
- Dar a conocer la importancia de la seguridad a todos los que trabajan en la institución o empresa a través de carteles, cursos, campañas u otros medios.
- Ejecutar frecuentes auto-evaluaciones de seguridad de la información.
- Consultar guías de configuración de sitios como NSA, NIST, SANS, ISO, security focus, insecure, entre otros.
- Contar con un equipo de personas dirigidos a la administración y seguridad de la organización.
- Manejar Canales seguros de comunicación.
- Cifrar comunicaciones y datos durante el transporte y almacenamiento.
- Hacer un uso adecuado de contraseñas.
- Realizar respaldos de información.

- Establecer planes de contingencia ante un incidente de seguridad.
- Contar con un inventario detallado de los equipos que integran la red incluyendo localización geográfica.
- Identificar los servicios que se ofrecen y eliminar aquellos que no son necesarios.
- Establecer esquemas de seguridad en profundidad.
- Proteger las redes a través de diferentes mecanismos.
- Delimitar tanto el acceso lógico como físico a los sistemas.
- Utilizar firewalls, sistemas detectores de intrusos, antivirus.
- Controlar y regular las cuentas de usuarios tanto de administradores como otros usuarios.
- Evitar utilizar la misma contraseña para todos los dispositivos o sistemas.
- Evaluar los impactos que se tendrían si se pierde algún activo.
- Asegurar física y lógicamente los equipos que integran la red.
- Evitar utilizar servicios como Telnet o donde la información viaje en claro.
- Instalar monitores de red que permitan analizar el comportamiento de la red.
- Auditar firewalls, sistemas y cualquier dispositivo que se considere necesario.
- Implementar controles de autenticación robusta para administradores o para el acceso a una intranet, se recomienda emplear mínimo dos controles.
- Minimizar el número de cuentas de usuarios que operen sistemas críticos.
- Utilizar contraseñas robustas para administradores y usuarios.
- Llevar un control de la asignación de direcciones IP.
- Contar con mapas de red.
- Establecer responsables por área.
- Identificar equipos críticos.
- Deberán implementarse políticas de uso de la red.
- Realizar pruebas de estrés a la red.
- Realizar pruebas de penetración.
- Realizar continuamente auditorías.

En el listado anterior se da un panorama general de las buenas prácticas que se deben seguir, sin embargo, será necesario tomar en cuenta otras recomendaciones que se crean necesarias con base en los objetivos y prioridades de cada organización.

4.4. Respaldo de información

Dentro de las políticas de seguridad o como parte de un plan de seguridad se debe contemplar y recalcar la importancia de realizar respaldos de la información, la razón es simple y sencilla, cualquier sistema puede incurrir en un fallo y con ello pérdida o daño de la información, lo que puede representar una pérdida económica, en tiempo o continuidad de operaciones.

Toda información por mínima que ésta sea, deberá respaldarse y clasificarse de acuerdo con la sensibilidad de la misma, a continuación se muestra un listado del tipo de información que debería considerarse para respaldar.

- En caso de maquinas virtuales, una copia idéntica de los archivos que la conforman
- Bases de datos.
  - Estructura e información.
- Documentos.
  - Texto.
  - Audio.
  - Video.
  - Archivos de configuración.
  - Bitácoras.
  - Políticas de seguridad.
  - Inventarios de equipos.
- Cuentas de usuarios.
  - Archivos.
- Cualquier otro tipo de información que se considere importante.
  - Guías de configuración.
  - Facturas.
  - Informes de trabajo.
  - Proyectos, por mencionar solo algunos.

Los respaldos deberán estar almacenados en distintos medios como cintas magnéticas, equipos alternos, dispositivos de almacenamientos masivos, además de que éstos deberán estar seguros de manera física y en caso extremo, cifrados.

El acceso a dicha información deberá estar restringido y sólo personal autorizado tendrá los privilegios para realizar dichos respaldos para evitar fuga de información, pérdida, o alteración de la misma.

Otros puntos importantes que se deberán considerar para un respaldo adecuado de la información son:

- Evitar contar con respaldos excesivos ya que esto puede complicar la administración de los mismos por lo que se deberán establecer fechas y tiempos de respaldo, esto dependerá de la importancia de la información.

- Los respaldos de la información no sólo son responsabilidad del administrador de un equipo, los usuarios deberán de contemplar que son responsables de su propia información y con ello implica que son responsables de lo que pueda acontecer con la misma. Esto deberá estar detallado en las políticas de seguridad.

- También deberán contar con una bitácora donde se contemple fecha, tamaño del archivo que se haya respaldado, responsable e incluso tipo de archivo y versión del software utilizado, en algunos casos requerirá mayor detalle.

4.5. Seguridad en aplicaciones

En la actualidad el desarrollo de aplicaciones seguras ha cobrado mayor importancia, esto debido a que los programas constituyen la mayor parte de los sistemas de cómputo como lo son los sistemas operativos, drivers, programas de infraestructura de red, administradores de bases de datos entre otras aplicaciones, debido a que los programas integran un gran porcentaje de los sistemas de cómputo, es importante tener especial cuidado con el manejo de ellos tanto en la implementación, como en el desarrollo de los mismos.

En el desarrollo de sistemas generalmente implica la integración de distintas tecnologías por lo que será necesario realizar un análisis profundo de las tecnologías a utilizar para determinar su factibilidad, éste debe incluir un análisis de seguridad, costo y beneficios que implica el uso de una u otra tecnología. La seguridad en aplicaciones deberá cubrir los aspectos tratados durante el desarrollo del presente trabajo: disponibilidad, confidencialidad e integridad.

Entre los puntos más importantes a considerar durante la implementación de aplicaciones se encuentran:

- Distribución libre o comercial.
- Tipo de tecnología utilizada.
- Compatibilidad.
- Soporte.

Durante el desarrollo de algún sistema se deberán tomar en cuenta los diferentes tipos de ataques en los que se podría verse implicado el software desarrollado, como por ejemplo el ataque buffer overflow y todas sus variantes que han sido muy aprovechadas por los intrusos atentando contra la disponibilidad, SQL injection, Cross-Site Scripting(XXS).

Algunos puntos importantes a considerar durante el desarrollo de software se encuentran:

- Basar los códigos de programación en estándares sobre todo si se maneja algún lenguaje de programación como C o C++.
- Verificar código haciendo uso de herramientas de auditoría.
- Evitar utilizar rutinas de C que impliquen el uso de rutinas que interactúen con la memoria.
- Utilizar herramientas de compilación que permitan detectar posibles vulnerabilidades.
- Tomar en cuenta la seguridad durante el desarrollo de aplicaciones.
- Tomar en cuenta estándares como ISO 2700x así como publicaciones de NIST 800-64 y 800-27.
- Establecer un modelo de desarrollo de código seguro.
- Utilizar herramientas que permitan detectar defectos de seguridad.
- Contar con un modelo de amenazas.
- Contar con una lista de verificación de implementación.
- Realizar pruebas de penetración.

En la tabla 4.2 se muestra una lista de herramientas útiles para el análisis de vulnerabilidades[39].

Tabla 4. 2 Herramientas de análisis de vulnerabilidades.

Nombre	Lenguaje
FXCop	.NET
SPLINT	C
Flawfinder	C/C++
ITS4	C/C++
Bugscan	C/C++ binaries
CodeAssure	C/C++, Java
Prexis	C/C++, Java
RATS	C/C++, Python, Perl, PHP

Otras herramientas para el análisis de vulnerabilidades

- NESUS
- NIKTO
- WebInspect
- GFILANguard

4.6. Seguridad en sistemas operativos

Entre las buenas prácticas de seguridad se recomienda asegurar los distintos sistemas operativos, así como los distintos elementos que lo integran, programas y servicios. Deberán existir políticas de configuración de los distintos equipos que integran una red, esto con la finalidad de disminuir el riesgo.

[39] Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001

A continuación se describen algunas características que deberán tomarse en cuenta para los sistemas operativos Linux, Windows y aunque no se consideren otros sistemas, de igual forma deberán tomarse en cuenta, desde luego esto dependerá de la infraestructura con la que cuente cada institución.

4.6.1. Hardening en plataformas Microsoft

Hardening es el proceso que se realiza para aumentar el grado de confianza de un sistema, acción compuesta por un conjunto de actividades para reforzar al máximo la seguridad. Al referirnos a Hardening en plataformas Microsoft se dan recomendaciones para aumentar el nivel de confianza de los sistemas operativos fabricados por Microsoft, tanto en sus versiones de estación de trabajo como de servidor.

El sistema operativo Windows es uno de los sistemas operativos más utilizados a nivel mundial, lo que implica un especial cuidado en el manejo del mismo, pues el hecho de que éste sea uno de los sistemas más populares también implica que éste sea un objetivo común de los atacantes.

A continuación se muestran algunas prácticas para asegurar la familia de los sistemas operativos Windows.

- La instalación deberá realizarse utilizando el sistema de archivos NTFS.
- Ubicar los equipos en algún lugar seguro físicamente.
- Colocar contraseña al BIOS.
- Las instalaciones eléctricas deberán ser las adecuadas, así como las condiciones físicas.
- Mantener un control adecuado de usuarios.
- Establecer contraseñas robustas para el administrador y usuarios limitados.
- Deshabilitar cuentas innecesarias como "invitado" y aquellas que no se utilicen.
- Renombrar la contraseña de administrador y no dejar la que el sistema operativo crea. por default, así como asignarle una contraseña robusta.
- Forzar a los usuarios para que cambien su contraseña periódicamente.
- Instalar antivirus y mantenerlo actualizado.
- Mantener actualizado el sistema operativo.
- Mantener activado el firewall local.
- Contar con la última actualización para cada sistema operativo.
- Evitar instalar programas innecesarios.
- Deshabilitar, en caso de que esté habilitado, el servicio de escritorio remoto.
- Algunos servicios deberán de activarse sólo cuando se requieran.
- Evitar instalar todos los servicios en un mismo equipo.
- Deshabilitar la reproducción automática de dispositivos como USB, disco o cualquier dispositivo extraíble.
- Establecer políticas locales o de grupo del sistema de acuerdo con las necesidades o actividades que desempeñan los usuarios.

- Restringir el uso de ciertos programas.
- Si el equipo se administra de manera remota, deberá realizarse a través de un canal seguro de comunicación.
- Analizar bitácoras del sistema operativo a través del visor de eventos de Windows u otras herramientas.
- Utilizar herramientas para el análisis de vulnerabilidades y actualizaciones de Microsoft como Microsoft Baseline Security Analyzer (MBSA).
- Utilizar herramientas para escanear puertos y ver qué servicios están haciendo uso de ellos.
- Utilizar herramientas que permitan escanear puertos para determinar las aplicaciones o servicios que los están utilizando.
- Deshabilitar NetBios, así como SMB si no es necesario que éste se encuentren habilitados.
- Activar el protector de pantallas después de cierto tiempo de inactividad.
- No permitir la enumeración de cuentas y recursos compartidos.
- Cifrar carpetas o archivos utilizando herramientas externas o las que ofrece el propio sistema operativo.

4.6.2. Hardening en Unix y Linux.

Los ataques no sólo van dirigidos hacia el sistema operativo Windows, en realidad no importa el tipo de sistema operativo, cualquiera que éste sea, es vulnerable, algunos con mayor frecuencia que otros pero todos están en riesgo, por ello sin importar el nombre del sistema o versión deberá de asegurarse.

El sistema operativo Linux que deriva directamente del sistema operativo UNIX ha ganado aceptación por los usuarios, además de que ha tenido un crecimiento muy rápido por toda la comunidad de desarrolladores que se encuentran detrás de éste.

Como se mencionó aunque es un sistema operativo menos utilizado, no está exento de incurrir en algún problema de seguridad, a continuación se describen algunos aspectos que se deben considerar para asegurar un sistema con ambiente Linux:

- Sin importar la distribución, ésta deberá personalizarse de acuerdo con las necesidades.
- Prevenir el cambio de configuración del BIOS.
- Analizar la posibilidad de no instalar el modo gráfico.
- Planear la instalación para asignar y crear las particiones necesarias.
- Determinar los servicios que se ofrecerán.
- Evitar instalar servicios innecesarios.
- Crear sólo las cuentas de usuario necesarias.
- Monitorear constantemente las cuentas de usuarios.
- Limitar el número de procesos que un usuario puede ejecutar.

- Verificar que los usuarios utilicen contraseñas robustas.
- Verificar integridad de archivos importantes como /etc/passwd y /etc/shadow y los binarios.
- Configurar los archivos de etc/group.
- Configurar el archivo que inicia servicios al arrancar el sistema etc/intetd.conf.
- Utilizar software que permita determinar vulnerabilidades.
- Mantener actualizado los programas que se instalen.
- Analizar constantemente bitácoras de los servicios instalados.
- Establecer cuotas a los usuarios.
- Cifrar archivos.
- Verificar integridad de archivos.
- Establecer permisos, lectura, ejecución, escritura y borrado.
- Si no es necesario ejecutar el modo gráfico, editar los niveles de ejecución.
- Asegurar cada uno de los servicios instalados como ssh, bases de datos, web, correo etcétera.
- Utilizar software que permita realizar auditorías para determinar fallas en la configuración.
- Escanear periódicamente los puertos abiertos TCP y UDP.
- Realizar pruebas de penetración.

4.7. Buenas prácticas de seguridad en servidores

En las infraestructuras de redes, los servidores juegan un papel muy importante, esto debido a que la información que manejan la mayoría de las veces es sensible, las recomendaciones que se hacen recaen en los siguientes puntos:

- Tratar de utilizar versiones de software lo más estable posible.
- Deshabilitar el booteo a partir de otros dispositivos diferentes al disco duro, como CD-ROM, USB, red, floppy, etcétera.
- Tener todo el sistema operativo dentro de una aplicación de cifrado.
- Saber reconocer los procesos que están corriendo en el equipo.
- Eliminar componentes de software extraños.
- Implementar un adecuado control de usuarios y privilegios.
- Forzar al uso de contraseñas robustas cuando se utilicen como métodos de autenticación.
- Habilitar la auditoría en el servidor.
- Verificar la aplicación de los parches de seguridad.
- Realizar auditorías de[40]:
    - Intentos de obtener acceso a través de cuentas existentes
    - Acceso y permiso a los archivos y directorios.
    - Cambios no autorizados a usuarios, grupos y servicios.
    - Sistemas más vulnerables a ataques.
    - Tráfico de red sospechoso o no autorizado.

[40] Chris Brenton,Top 5 Essential Log Reports version 1, SANS, http://www.sans.org/security-resources/top5_logreports.pdf

- Identificar los puertos válidos con base en los servicios que debe ofrecer cada equipo.
- Utilizar software de reconocimiento de rootkits.
- Renombrar las cuentas de administrador o root, según sea el caso.
- No tener habilitados en usuarios remotos root o administrador, utilizar un usuario sin privilegios para el logueo y elevar privilegios de ser necesario.
- Cambiar las contraseñas de root o administrador cada cierto tiempo, recomendación con cambio cada tres meses como mínimo y un registro de cada acceso de esta cuenta al servidor.
- Deshabilitar cuentas de usuarios invitados.
- Eliminar cuentas de usuario sin uso.
- En servidores Windows, uso de alguna herramienta que le permita utilizar un segundo factor, como método de autenticación, el cual debe ser introducido en el sistema cada vez que se desee iniciar sesión.
- Uso de particiones NTFS en el caso de servidores Windows por sus beneficios de cuotas, compresión y cifrado.

Es un hecho que no todos los puntos pueden ser cubiertos, aunque sería lo más recomendable, pero con base en las necesidades de cada caso particular, tener los elementos para dar la solución adecuada es una buena práctica.

4.8. Seguridad en dispositivos removibles y verificaciones regulares al sistema

Los dispositivos de almacenamiento removibles que se conectan a través del puerto USB (memorias, cámaras digitales, cámaras de video, teléfono celular, etcétera), constituyen otro de los mayores focos de infección y propagación de malware, el extravío de estos dispositivos permite filtrado de información, así como medio para la extracción de información debido al avance tecnológico que permite actualmente guardar grandes cantidades de información en espacios muy pequeños.

Por lo tanto, es necesario tener presente algunas de las siguientes medidas que ayudan a mantener el entorno de información con un nivel adecuado de seguridad, ya sea en entornos corporativos como en casa:

- Establecer políticas que definan el uso correcto de dispositivos de almacenamiento removibles, esto ayuda a tener claro las implicaciones de seguridad que conlleva el uso de estos dispositivos.
- Deshabilitar el autoarranque de estos dispositivos en los sistemas operativos de Microsoft Windows en los equipos de la institución.
- De ser necesario, registrar el uso de los mismos.
- Deshabilitar o bloquear dispositivos removibles en equipos sensibles de la institución con la finalidad de evitar sustracción de información.
- Si se transporta información confidencial en estos dispositivos, es recomendable cifrarla, de esta forma en caso de robo o extravío, la información no podrá ser vista por terceros.

- Es recomendable verificar con antivirus cualquier dispositivo que se conecte a la computadora para controlar cada posible infección.

Desde el punto de vista técnico, se podría contar con la más alta tecnología e infraestructura para garantizar un nivel de seguridad aceptable, sin embargo, si estos sistemas no son monitoreados de manera constante no será posible detectar fallas y mucho menos garantizar el servicio que se ofrece.

La verificación o revisión del sistema deberá de realizarse de manera periódica para tener la certeza de que todo funciona de manera adecuada o esperada para determinar anomalías y corregirlas.

La verificación del sistema implica análisis de bitácoras - logs de los distintos servicios que se ofrecen como web, correo, bases de datos IDS, RADIUS, switches, ruteadores, firewalls, e incluso cualquier sistema debería contar con una bitácora que permita analizar procesos, fallas, tiempo de activación del servicio, última actualización y todos los procesos que generen error.

Además del análisis de bitácoras, también es conveniente analizar procesos en tiempo real, lo cual permitirá medir el desempeño del equipo o sistema de cómputo.

Ventajas:

- Recuperación ante incidentes de seguridad.
- Detección ante un comportamiento inusual.
- Evidencia legal.
- Información para resolver problemas.
- Son de utilidad para un análisis forense.

4.9 Concientizar a los usuarios finales

El usuario final es uno de los pilares más débiles en la cadena de los controles empleados para la seguridad, tanto los usuarios como las organizaciones son cada vez más dependientes de Internet, por esta razón se dan recomendaciones que tiene que ser consideradas por el usuario final con el fin de que reduzca la posibilidad de caer en alguno engaño. En consecuencia, se presenta una serie de medidas preventivas:

- Dar curso de Ingeniería Social al personal con la finalidad de anular su impacto.
- No confiar en correos SPAM con archivos adjuntos y explorar el archivo antes de ejecutarlo, esto asegura que no se ejecutará malware.
- Cuando se reciben archivos adjuntos, prestar especial atención a las extensiones de los mismos.
- Evitar publicar la dirección de correo en sitios web de dudosa reputación como sitios de foros, chat, pornográficos, entre otros.

- Emplear filtros anti-spam.

- Evitar responder correo spam.
- Utilizar claves seguras y cambiar la contraseña con periodicidad.
- Eliminar o deshabilitar programas innecesarios.
- Proteger la dirección de correo utilizando una cuenta alternativa.
- Tener en cuenta que las entidades bancarias no solicitan información por correo electrónico.
- Tratar de no acceder a VPN, cuentas bancarias, cuentas de correo desde lugares públicos.
- Tratar de no publicar información sensible y confidencial, debido a que personas extrañas pueden aprovechar esa información con fines maliciosos.
- Evitar el almacenamiento de información confidencial y sensible en computadoras que comparten archivos.
- Es recomendado, dependiendo el grado de confidencialidad que se desea, cifrar todo el sistema operativo.
- Evitar aceptar contactos desconocidos en la mensajería instantánea.

4.10. Controles críticos de seguridad

El SANS (SysAdmin, Audit, Network, Security Institute – Administración de sistemas, auditoría, Red, Instituto de Seguridad) la fuente más confiable y más completa sobre información de seguridad informática, publicó una serie de controles que con base en estudios realizados, son los 20 controles de seguridad más críticos de seguridad de hoy en día:

- Inventario de los dispositivos autorizados y no autorizados.
- Inventario de software autorizado y no autorizado.
- Configuraciones seguras y que cumplan con políticas para servidores, estaciones de trabajo, laptops, etcétera.
- Configuraciones seguras de dispositivos de red.
- Defensa perimetral.
- Mantenimiento y análisis de log; mediante el análisis de las alertas emitidas en cada sistema se realiza una revisión las cuales permiten dar mantenimiento y mejorar el funcionamiento del mismo.
- Seguridad en el software de aplicación, el software que funcione en la red debe ser seguro.
- Uso controlado de los derechos de administrador.
- Acceso controlado de acuerdo con funciones, definir quiénes tienen derecho a qué.

- Mantenimiento y remedio continúo a las vulnerabilidades.
- Control y monitoreo de cuentas, políticas de contraseñas en general.
- Defensa contra malware.
- Limitación y control de puertos de red, protocolos y servicios.
- Control de dispositivos inalámbricos.
- Prevención de pérdida de datos, planes de contingencia, respaldos, control de salida de información.
- Ingeniería de seguridad en redes, es decir, planear una red con la seguridad en mente.
- Pruebas de penetración, tener un plan de evaluación de su red, saber dónde es vulnerable.
- Capacidad de respuesta a incidentes, hay que considerar factores internos como sabotaje o fallas de suministro y factores externos como ataques y fenómenos naturales.
- Capacidad de recuperación de datos, respaldos, una política correcta de respaldos e incluso contar con servidores espejo.
- Capacitación en seguridad, debe haber responsables de la seguridad y contar con capacitación constante.

Así mismo SANS publica una lista con las 20 vulnerabilidades mayormente comprometidas, el propósito de crear esta lista fue ayudar a los administradores a comenzar a asegurar sus equipos contra las más comunes amenazas.[41]

- Vulnerabilidades del lado del cliente.
  - Navegadores Web.
  - Software de oficina.
  - Clientes de correo.
  - Reproductores multimedia.

- Vulnerabilidades en servidores.
  - Aplicaciones web.
  - Servicios de Windows.
  - Servicios de Unix y Mac.
  - Software de respaldo.
  - Software antivirus.
  - Administración de servidores.
  - Software de bases de datos.

[41] The Top Cyber Security Risk, SANS, http://www.sans.org/top20/

- Políticas de seguridad y personal.
  - Derechos de usuario excesivos y dispositivos no autorizados.
  - Phishing.
  - Laptops sin cifrado y dispositivos removibles.

- Abuso de aplicaciones.
  - Mensajería instantánea.
  - Programas punto a punto (Peer-to-Peer).

- Dispositivos de red.
  - Servidores y teléfonos de VoIP.

- Ataques de día cero; todos aquellos nuevos ataques que explotan vulnerabilidades aun no detectadas, que por su característica no existe a la fecha procedimiento de solución.

Algunos años atrás la seguridad de los servidores y servicios fue la principal tarea para la seguridad de una organización, hoy es igual de importante, quizás inclusive más importante es prevenir a los usuarios finales para que no comprometan sus máquinas por medio de páginas web con código malicioso u otros objetivos en el cliente.

4.11. Pruebas de penetración

Una vez implementado todo un esquema de seguridad con todos los mecanismos necesarios para implementar la seguridad, éstos deberán ser sometidos a pruebas de intrusión o penetración haciendo uso de las mismas herramientas que cualquier intruso utilizaría para intentar burlar la seguridad con la finalidad de hallar vulnerabilidades o encontrar algunas cuestiones que no se hayan tomado en cuenta y poder corregirlas antes de que algún intruso lo haga.

No deberá confundirse una prueba de penetración con un ataque real, puesto que un ataque pone en riesgo información, mientras que una prueba será con la finalidad de reforzar, crear o modificar los mecanismos de seguridad.

Para realizar un proceso de penetración deberá especificarse el ámbito donde se aplicará la prueba y puede incluirse una lista específica de las pruebas a realizar o incluso se puede proporcionar una descripción amplia de los procedimientos a realizar.

También es importante establecer límites, ya que en algunas ocasiones existe información con un alto grado de sensibilidad la cual por ningún motivo deberá darse a conocer.

Se debe establecer un tiempo exacto para realizar la prueba, esto con la finalidad de evitar confusiones con las personas encargadas de la seguridad.

Una vez concluidas las pruebas se deberá realizar un reporte ejecutivo con los resultados de las pruebas realizadas, además de un reporte técnico donde se incluyan de manera detallada:

- Los resultados ordenados por prioridad.
- Riesgos a los que está expuesta la organización.
- Requerimientos para disminuir las amenazas.
- Recomendaciones y acciones a realizar.

Una vez generado el reporte, uno de los pasos finales es evaluar los resultados para mejorar las políticas de seguridad de la organización, lo ideal es realizar las pruebas de penetración antes de que las políticas estén completamente terminadas.

Algunas consideraciones importantes a tomar durante las pruebas de penetración, es comprender las razones o motivos por las que un atacante decidiría irrumpir la seguridad, actuar como si se tratase del propio atacante, pensar como un atacante.

Como se mencionó, la importancia de las pruebas de penetración permite revelar vulnerabilidades que pueden ser solucionadas de diferentes maneras:

- Actualizar el sistema afectado.
- Reconfigurar el firewall u otros dispositivos de seguridad.
- Modificar los controles de acceso de aplicaciones y sistemas operativos.

Aunque se realicen pruebas de penetración para determinar fallas técnicas, también es necesario verificar cuestiones de seguridad física, además de realizar un análisis de las políticas establecidas para determinar si éstas son suficientes para garantizar la seguridad.

4.12. Implementar un Plan de Continuidad y Recuperación de Desastres (DRP)

Desde hace tiempo muchas organizaciones, frente a un evento catastrófico, formulan un conjunto de procedimientos que detallen acciones para ser tomadas de manera anticipada frente a una catástrofe, este procedimiento deberá ser diseñado como si el evento catastrófico fuera inevitable, este tipo de planes se conoce como DRP. Es importante recordar que uno de los elementos claves de la seguridad de la información es la *disponibilidad*, la planeación correcta es necesaria para asegurar la disponibilidad de sistemas de misión crítica.

Los requerimientos para un plan de recuperación de desastres varía para cada organización, sin embargo, para la mayoría los objetivos mínimos de plan de recuperación de desastres es brindar la información y procedimientos necesarios para hacer lo siguiente[42]:

- Plan de respuesta a emergencias de cómputo.

[42] Robert Comella, Computer Disaster Recovery Plan Policity, SANS, http://www.sans.org/security-resources/policies/disaster_recovery2.pdf

    - Creación de equipo de recuperación de desastres.
  - Contar con un directorio de las personas que forman el equipo de respuesta.
  - Quién debe ser contactado, cuándo y cómo.
  - Qué acciones inmediatas deben tomarse cuando se presente un evento.

- Sucesión del plan.

  - Notificar al personal necesario para responder al evento.
  - Describe el flujo de responsabilidades cuando un staff normal no está disponible para ejecutar sus obligaciones.

- Estudio de datos.

  - Detalla los datos almacenados en los sistemas, críticos y confidenciales.

- Lista de servicios críticos.

  - Lista todos los servicios brindados y su orden de importancia.

- Plan de restauración y respaldo de datos.

  - Detalla qué datos son respaldados.
  - Los medios de almacenamiento.
  - Lugar de almacenamiento.
  - Tiempos de ejecución de los respaldos.
  - Qué datos deben ser almacenados.

- Plan de reemplazo de equipo.

  - Describe qué equipo es requerido para comenzar a brindar servicio.
  - Lista el orden en que esto es necesario.
  - Nota dónde comprar el equipo.

- El plan debe de ser puesto en acción.

  - Después de crear los planes, es importante practicarlo y extender sus alcances.
  - Durante las pruebas puede causar que el plan falle, lo que permite corregirlo en un entorno de pocas consecuencias.

- El plan debe ser actualizado.

  - Revisar los planes por lo menos una vez al año, que permitan incorporar los nuevos procesos en la organización.

- Tener en un lugar estratégico las guías de configuración y bitácoras que muestren el procedimiento a seguir en caso de un evento.

- Contar con sitios alternos que permitan brindar servicios desde sitios físicos diferentes.
- Respuesta a los procesos tan rápidamente como sea posible para asegurar la mínima ruptura en las operaciones de la organización.
- Cumplir con algunos requerimientos regulatorios que dicten la existencia de un plan de recuperación de desastres para la organización.
- Responder a la existencia de un desastre.

Uno de los factores clave en el éxito de un plan de recuperación de desastres, es la planificación apropiada de un grupo que administre las tecnologías de la información. La mayoría de las organizaciones en estos días tiene mucha confianza en el uso de equipos de cómputo, redes de datos, telecomunicaciones y tecnologías de la información en general, como resultado, las TI juegan un papel clave en el plan de recuperación de desastres de las organizaciones.

El plan de recuperación de desastres es una decisión que debe ser considerada como decisión del negocio, el costo de la recuperación debió haber sido comparado contra las pérdidas generadas como resultado de la intervención del servicio.