ANEXO E. ENCUESTA

POLÍTICAS DE SEGURIDAD QUE SIGUEN LAS INSTITUCIONES QUE CONFORMAN LA RUP

Las siguientes preguntas fueron hechas a los encargados del área de sistemas en cada sede que conforma la RUP para tener una idea de las premisas de seguridad que cumplen en cada una de las instituciones, las cuales están establecidas en el estándar ISO/IEC 27001.

ENTIDADES EXTERNAS

1. Las cámaras de seguridad cubren las entradas a la institución y al área de servidores?
2. Los equipos de alarmas funcionan correctamente?
3. Tienen control sobre información que pueda ser sustraída de manera inadecuada de las cuentas de usuario ya sea en forma escrita o almacenada en medio magnético?
4. Están deshabilitados los puntos de red que no se encuentran en servicio y que están ubicados en áreas públicas?
5. Existen controles para las personas que deban utilizar la red ya sea como usuarios o administradores?
6. Protegen y aseguran adecuadamente los medios de copias de seguridad del sistema?

CONTROL DE ACCESO

CONTROL DE ACCESO AL SISTEMA DE OPERACIÓN

7. Actualizan constantemente los sistemas operativos basados en Windows que utiliza la red?
8. Tienen una clasificación de servicios necesarios y no necesarios los cuales son deshabilitados para los usuarios?
9. Utilizan filtros IPsec para bloquear puertos que estén a la escucha de servicios externos a la red?
10. Utilizan un firewall?
11. Limitan los privilegios interactivos de inicio de sesión para los usuarios que no sean administradores de la red?

12. Crean y distribuyen configuraciones seguras para usuarios de Windows 2000 y 2003 server?
13. Las instalaciones en las que están ubicados los servidores de la red son físicamente seguras, con contraseña a nivel de BIOS y sin unidades de arranque que puedan ser configuradas para iniciar un sistema operativo alternativo al instalado?
14. Utilizan contraseñas de mas de 8 caracteres combinando caracteres alfanuméricos?
15. Utilizan herramientas sw para cerrar la sesión de usuario inmediatamente éste termine la llamada al servidor?
16. Limitan el número de intentos de inicio de sesión antes de desconectar al usuario?
17. Bloquean a los usuarios fallidos en aplicaciones remotas?
18. Mantienen actualizado el kernel en los sistemas operativos basados en Linux que utiliza la red?
19. Eliminan frecuentemente los archivos que contengan el identificador de usuario SUID y el de grupo SGID de root?
20. Mantienen la información del archivo de registro en un medio difícil de modificar?

CONTROL DE ACCESO A REDES

21. Llevan un registro de las actividades que realizan todos los usuarios de la red?
22. Exigen el uso de contraseñas adecuadas para los usuarios remotos que utilizan los servicios de la red?
23. Las impresoras que están siendo utilizadas en la red están configuradas con los niveles de seguridad adecuados?
24. Tienen un registro de todos los equipos que hacen uso de la red, que sistemas operativos utilizan cada uno de ellos y sus respectivas direcciones MAC?
25. Utilizan tarjetas magnéticas o testigos de hw para identificación de personal?
26. Controlan el uso de sw de control remoto en la red?
27. Utilizan claves repetidas para diferentes puntos de la red?
28. Tienen un control sobre los puertos que no están siendo utilizados por servicios de la red?
29. Existe algún tipo de control entre los usuarios que utilizan la red Ethernet y los usuarios que utilizan los puntos de acceso inalámbricos dentro de las instalaciones?

30. Utilizan sw para detección de rastreadores de tráfico dentro de un segmento de la red?
31. Utilizan contramedidas electrónicas de utilización de espectro de radiofrecuencia como ECM?
32. Utilizan contramedidas electromagnéticas como ESM para interferir las fuentes de transmisión de estaciones base?
33. Utilizan antenas direccionales para sus enlaces de radio frecuencia?
34. Tienen algún plan de acción contra ataques del tipo DoS?
35. Los armarios en donde están ubicados los equipos de telecomunicaciones son físicamente seguros?
36. Cambiaron los valores por defecto de las contraseñas y opciones de seguridad de los equipos que vienen configurados de fábrica?
37. Tienen entradas estáticas entre el firewall y el router de frontera de la red?
38. Utilizan SSH o IPsec para enviar información relevante extremo a extremo?
39. Utilizan el AES como método de cifrado?
40. Utilizan el RSA como método de cifrado público?

GESTIÓN DE OPERACIONES Y CONTROL
PROTECCIÓN CONTRA SW MALICIOSO Y CÓDIGO MÓVIL

41. Utilizan sw de control remoto en sistemas de autenticación para la familia Windows 2000 y 2003 server?
42. Si utilizan este tipo de sw, mantienen las versiones del sistema operativo actualizadas con los parches de seguridad que ofrece el fabricante?
43. Comprueban que todo programa que se baja de internet sea seguro y confiable?
44. Comprueban el objetivo de cada programa que se ejecuta en Windows o en Linux?
45. Comprimen los datos cifrados mediante SSH antes de enviarlos por la red?
46. Controlan las claves públicas de cada computador que utiliza SSH?
47. Utilizan la última versión de SSH?
48. Mantienen un control sobre todas las aplicaciones que corren los servidores WEB, validación de las entradas efectuadas por los usuarios y lo mantienen actualizado mediante parches de actualización?
49. Utilizan un antivirus que se esté actualizando periódicamente y que a su vez estas actualizaciones lleguen a los equipos terminales de la red diariamente?

BILBIOGRAFÍA UTILIZADA EN LOS ANEXOS

[1] AHMED, M. Abdesalam. wimax security solutions for 802.16. 2007.

[2] AHSON, Syed y ILYAS, Mohammad. wimax standars and security. 2007.

[3] FÚSTER, Amparo; De la GUÍA, Dolores; HERNÁNDEZ, Luis; MONTOYA, Fausto; MUÑOZ, Jaime. Técnicas Criptográficas de Protección de Datos 3a Edición Actualizada. Ra-Ma Editores. España. 2004.

[4] LOW, Richard y STAMP, Mark. Applied Cryptanalysis. John Wiley & Sons Inc. USA. 2007.

[5] LUCENA, Manuel. Criptografía y Seguridad en Computadores 4ª Edición. Creative Commons. España. 2007. Disponible en: http://wwwdi.ujaen.es/_mlucena/lcripto.html.

[6] De BUSTOS, José Angel. Criptografía. HispaLinux. España. 2005.