Superintendencia de Sociedades

RECOMENDACIONES DE SEGURIDAD INFRAESTRUCTURA TECNOLÓGICA

1. OBJETIVO: Esta Guía tiene como fin dar recomendaciones sobre algunos parámetros de seguridad que se pueden tomar frente a la plataforma tecnológica garantizando así su optimo funcionamiento.

2. ACTIVIDADES

2.1. BASES DE DATOS

Parámetro o Componente	Descripción
Puertos Bases de Datos	De ser posible, cambie los puertos predeterminados utilizados por el motor de Base de Datos. En caso de realizar este cambio, debería modificar la configuración de los aplicativos que tienen acceso a la base de datos para reflejar el ajuste de puerto.
Filtrado de puertos por un firewall	Todos los puertos TCP y UDP utilizados por el motor de Base de Datos deben ser filtrados por un firewall (de host y/o de red) para que únicamente permita el acceso a este recurso a los equipos autorizados.
Acceso vía Internet	Debería existir un Firewall entre los servidores de Base de Datos y el servicio de Internet. En un ambiente multi-tier, deben utilizarse múltiples Firewall en configuración doble bastión para crear subredes más seguras.

2.1.1. AUDITORÍA

Parámetro o Componente	Descripción
Política de Logs de Auditoría	Se debería definir un periodo de retención de logs (sugerido 3 meses) para asegurar la trazabilidad y evitar la repudiación de eventos. Los logs deben redireccionar preferentemente a un servidor de logs. Los Logs de auditoría generados por los equipos deben ser protegidos contra acceso no autorizado
Auditoria de eventos	Se deben registrar los eventos de ingresos exitosos y fallidos. Los logs de auditoría de las Bases de Datos deben estar habilitados y configurados de manera que registre eventos relevantes de seguridad, entre ellos la creación, modificación y eliminación de grupos, usuarios y/o permisos.

2.1.2. POLÍTICAS DE CUENTAS

Parámetro o Componente	Descripción
Cuentas	Renombre la cuenta de administrador local de Base de Datos (por ejemplo, 'sa', 'root') y eliminar las cuentas predeterminadas instaladas por el motor de Base de Datos
Tablas y vistas	Se debería prevenir el acceso no autorizado a tablas, cluster y vistas que contengan información de la arquitectura y administración del motor de Base de Datos.

2.1.3. CONFIGURACIÓN

Parámetro o Componente	Descripción
Servidores de desarrollo	Los servidores de prueba y desarrollo pueden estar en un segmento de red diferente de los servidores de producción. Podrían estar definidos como instancias de pruebas o desarrollo, independiente de la instancia de producción.
Servidor Dedicado	Instale el servidor de Base de Datos en un Servidor donde no se proporcionen servicios adicionales como servicios Web o servicios de correo.
Parches y hotfixes	Se debería evaluar la aplicabilidad de instalar parches y hotfixes en el servidor Bases de Datos. En algunos casos la aplicación de tales parches no será posible debido a requerimientos específicos de funcionamiento de las aplicaciones instaladas. En estos casos, se deberán evaluar soluciones alternativas para mitigar los riesgos generados por la no instalación.
Particiones Separadas	Cree volúmenes o particiones de disco separando los archivos de programa del motor de Base de Datos y los datos.
Aplicativo de demostración o manuales del aplicativo	Elimine o cambie de ubicación los archivos predefinidos como archivos de demostración y manuales.
Herramientas de edición del registro del sistema.	Evalúe la aplicabilidad de eliminar o remover las herramientas y/o aplicaciones que permiten la edición de registro del sistema en el servidor de Base de Datos.

2.2. RECOMENDACIONES PARA SISTEMA OPERATIVO

Parámetro o Componente	Descripción
NetMeeting Remote Desktop Sharing	Esta vulnerabilidad permite a un usuario malicioso evitar el correcto funcionamiento de los servicios de Netmeeting y consumir el 100 % de los recursos de la CPU durante un ataque, por lo tanto, este servicio no debería operar en ninguno de los Servidores.
Network News Transport Protocol (NNTP)	El servicio del NNTP permite que un servidor de IIS reciba discusiones del grupo de noticias. Las discusiones se pueden recibir localmente, o se pueden remitir a los clientes de los servidores de noticias externos. La mayoría de los clientes populares del correo incluyen a lector de noticias. Este servicio debería estar deshabilitado en los servidores.
Configuración de servicios del sistema	Se debería tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema.
Servicios inseguros que debería ser deshabilitados	Los siguientes servicios deberían ser deshabilitados: Echo, Discard, Daytime, Qotd, Chargen, Telnet (usar SSH si es necesario), Alerter, Messenger. Se debería evaluar la necesidad de tener los siguientes servicios deshabilitados si no son absolutamente necesarios: IIS Admin Service, IIS Extensiones IDA y ISAPI, FTP (preferentemente usar SCP), POP, SNMP (si es necesario utilizar V3), SMTP. Finger, Sysstat, Daytime, Netstat, Who, Rbootd, Rstat, Rwall, Ruser, Bootps, Rexd, Pcnfs, Sprayd, Tftp.
Servicios de comandos remotos inseguros:	Se deberían deshabilitar los siguientes comandos: rexec, rshell, rlogin, rusers, rsh, rpc.

2.2.1. AUDITORÍA

Parámetro o Componente	Descripción
Auditoria de eventos de logueos de cuentas.	La auditoria de eventos debería habilitarse.
Auditoria de Policy Change.	La auditoria de Policy Change debería habilitarse.
Auditar el uso de Privilegios	La auditoria del uso de privilegios debería habilitarse
Auditoria de System Events.	La auditoria de System Events debería habilitarse.
Política de Logs de Auditoría	Se debería registrar los eventos que ofrecen información adicional a los administradores sobre sucesos exitosos y fallidos en el sistema.

Parámetro o Componente	Descripción
	Se debería definir un periodo de retención de logs (sugerido 3 meses) para asegurar la trazabilidad y evitar la repudiación de eventos. Los logs debería redireccionar preferentemente a un servidor de logs. Los Logs de auditoría generados por los equipos debería ser protegidos contra acceso no autorizado

2.2.2. POLÍTICAS DE CUENTAS

Parámetro o Componente	Descripción
Tiempo mínimo de validez del password	Esta característica evita el re-uso de passwords por parte de los usuarios, al obligarlos a utilizar un password por un determinado tiempo antes de poder cambiarlo, se recomienda 1 día.
Tiempo máximo de validez del password	El tiempo máximo de validez del password debería ser de 90 días.
Tamaño mínimo del pasword.	La longitud mínima de los passwords, debería ser al menos de 8 caracteres.
Complejidad de password	La complejidad de password debería habilitarse
Historial de las Contraseñas	El historial de contraseñas debería cambiarse al valor de 24.
Almacenar Contraseñas.	El almacenar Contraseñas debería estar habilitado.
Duración de bloqueo de cuenta	La duración de bloqueo de la cuenta en caso de errores sucesivos al intentar ingresar debería estar en 15 minutos.
Umbral de bloqueos de cuenta	El Umbral de errores sucesivos al intentar ingresar debería estar en 3 u 8 Intentos.

2.2.3. PARÁMETROS DE SEGURIDAD

Parámetro o Componente	Descripción
Cuenta "Administrador" e "Invitado"	La cuenta Administrador e Invitado deberían ser renombradas para dificultar la acción de un atacante que quiera realizar un ataque de fuerza bruta para encontrar las contraseñas.
Permisos de usuario conexiones anónimas	Identifique y configure los accesos permitidos mediante usuario anónimo, estos permisos debería revisarse muy cuidadosamente para verificar que cumplan con las necesidades de seguridad.
Recursos compartidos	Identifique y configure los accesos a recursos compartidos a través de autenticación, estos permisos debería revisarse muy cuidadosamente para verificar que cumplan con las necesidades de seguridad.
Permisos de archivos administrador del	Se debería identificar y definir los permisos únicamente a los usuarios administrador, SYSTEM, root, bin, sys, adm, sysadmin

Parámetro o Componente	Descripción
sistema	sobre los siguientes archivos: at.exe, attrib.exe, cacls.exe, debug.exe, drwatson.exe, sc.exe, drwtsn32.exe, edlin.exe, eventcreate.exe, net.exe, runas.exe, eventtriggers.exe, ftp.exe, net1.exe, netsh.exe, rcp.exe, reg.exe, regedit.exe, regedt32.exe, regsvr32.exe, rexec.exe, rsh.exe, subst.exe, telnet.exe, tftp.exe, tlntsvr.exe. etc, bin, usr/sbin, usr/bin, usr/etc.
Sistemas Operativos y aplicaciones sin contratos de soporte, desactualizados, no parchados, o sin respaldo por parte del fabricante	Realizar un monitoreo permanente y filtrar el trafico de acceso al equipo y/o aplicaciones con el objetivo de minimizar la materialización o explotación de vulnerabilidades y/o aislar el equipo en una zona de seguridad como una zona militarizada o una zona desmilitarizada previo estudio de necesidades

2.3. REDES Y COMUNICACIONES

Parámetro o Componente	Descripción
Servicios inseguros que deben ser deshabilitados	Eliminar, si no son necesarios: telnet (si es requerido el acceso remoto se sugiere usar ssh), Bootp, Finger, TFtp (a menos que sea estrictamente necesario para generar copias de seguridad)
Servicios del router y switch que deben ser protegidos de accesos no permitidos	SNMP, HTTP, FTP (si no son requeridos deben ser deshabilitados estos servicios. Si son requeridos, se deben configurar para ser habilitados solamente por IPs autorizados y/o autenticándose a través de nombre de usuario y contraseña)
Puertos predeterminados	Cambie los puertos predeterminados utilizados por los servicios como HTTP.
Encripción	El tráfico de administración remota de router/switch/firewall/access point debería ser intercambiado a través de cifrado (HTTPS, SSH) u otros métodos.
Servicio remoto	El acceso remoto a sistemas externos desde el router/switch/firewall/access point debería estar prohibido. De la misma forma el acceso remoto de estos equipos, desde redes diferentes a la LAN se debería desahabilitar.

2.3.1. AUDITORÍA

Parámetro o Componente	Descripción
Política de Logs de Auditoría	Se debería definir un periodo de retención de logs (sugerido 3 meses) para asegurar la trazabilidad y evitar la repudiación de eventos. Los logs deben redireccionar preferentemente a un servidor de logs. Los Logs de auditoría generados por los equipos deben ser protegidos contra acceso no autorizado
Auditoria de eventos	Se deben registrar los eventos de ingresos exitosos y fallidos. La auditoría de router/switch/firewall/access point debería estar habilitada y configurada de manera que registre eventos relevantes de seguridad al Cisco MARS.

2.3.2. POLÍTICAS DE CUENTAS

Parámetro o Componente	Descripción
Timeout	Se debería definir la duración de Timeout para conexiones con el router/switch/firewall/access point y appliance
Restringir el acceso al router/switch/firewall/ access point solo a IPs autorizadas	Se debería controlar el acceso mediante el uso de passwords fuertes (con adecuada complejidad y tamaño), para evitar ataques de fuerza bruta o de diccionario
Configuración predefinida de router/switch/firewall/ access point	Modifique las contraseñas predefinidas de router/switch/firewall/ access point
Passwords	Contraseñas y llaves secretas almacenadas en el router/switch/firewall/ access point deben estar encriptadas.

2.3.3. CONFIGURACIÓN

Parámetro o Componente	Descripción
Copias de respaldo	Se debería respaldar mensualmente la configuración de router/switch/firewall/ access point.
Control de acceso	Un ACL debería implementarse para impedir la acción de troyanos y filtrar servicios en la red interna (switch/router/firewall/access point), para evitar negación de servicios
Misión critica	El desempeño de router/switch/firewall/access point. debería ser monitoreado periódicamente, para garantizar la comunicación en la red y evitar la perdida de disponibilidad. Se sugiere realizar este monitoreo usando SNMPV3, configurado ro (Read-Only).
Paquetes ICMP	La redirección de paquetes ICMP debería estar bloqueada en router/switch/firewall/access point.
Fecha y hora	El reloj interno y fecha de router/switch/firewall/access point, debería estar configurada apropiadamente (según la hora oficial colombiana – Superintencia de Industria y Comercio) para ser utilizada en los registros de auditoria.
Actualizaciones y parches	Se deben mantener al día las actualizaciones y parches en router/switch/firewall/access point.

3. BIBLIOGRAFÍA

- The Center for Internet Security – http://www.cisecurity.org/
- The SANS Institute – http://www.sans.org/
- National Security Agency (NSA) Security Configuration Guidelines - http://www.nsa.gov/SNAC/