DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.1**	**Actividad**	Políticas de seguridad en redes y sus elementos				
Unidad:	2: Configuración de seguridad en firewall, Switches, Routers y Access						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**SEGURIDAD EN ITI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	Daniel Tejeda Saavedra					Registro:	17300288
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	12/03/2021
Compet. Genéricas	4.1, 4.5, 5.2,			Compet. Profesional		CP1-1	

1. Objetivo(s) de la actividad

- Identificar las políticas en el ámbito de seguridad informática.

2. Introducción

Conocer las políticas en el ámbito de seguridad informática, es prioritario para poder proteger correctamente un sistema.

3. Instrucciones (Descripción) de la actividad

1. Identificar y redactar el significado de política de seguridad en redes, sus elementos. Además, desarrollar las políticas de seguridad (alrededor de 10) considerando el producto integrador, especificando su alcance, objetivo general, objetivos específicos, definiendo:

- Las políticas y normas de seguridad personal (política, obligaciones de los usuarios y sanciones)
- Políticas y Normas de acceso y autenticación (política, controles de acceso, administración de privilegios, equipo desatendido y especificaciones para uso de contraseña).
- Políticas y normas de seguridad y Administración de Equipo de Cómputo. Etc.

Consultar: el PDF: CISCO security
Consultar: https://www.netacad.com/ Cybersecurity Essentials, los siguientes temas:

2.2.1.4 Leyes y responsabilidades
2.4.3.1 Políticas
7.2.2.3 Políticas de grupo

2. Usar el archivo de ejemplo de actividades, completar todos los datos del encabezado identificando si es Actividad, Investigación o Practica, así como las competencias a desarrollar para esta actividad.

3. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.

Desarrollo

Una política de seguridad es un conjunto de objetivos de seguridad para una empresa que incluye las reglas de comportamiento de usuarios y administradores y especificar los requisitos del sistema. Estos objetivos, estas reglas y estos requisitos en conjunto garantizan la seguridad de una red, de los datos y de los sistemas informáticos de una organización.

Una política de seguridad completa logra varias tareas:

- Demuestra el compromiso de una organización con la seguridad.
- Establece las reglas para el comportamiento esperado.
- Garantiza la uniformidad en las operaciones del sistema, el software y la adquisición y uso de hardware, y el mantenimiento.
- Define las consecuencias legales de violaciones.
- Brinda al personal de seguridad el respaldo de la administración.

Las políticas de seguridad informan a los usuarios, al personal y a los gerentes los requisitos de una organización para proteger la tecnología y los activos de información. Una política de seguridad también especifica los mecanismos necesarios para cumplir con los requisitos de seguridad.

Como se muestra en la figura, una política de seguridad generalmente incluye:

- **Políticas de autenticación e identificación:** determinan cuáles son las personas autorizadas que pueden acceder a los recursos de red y describen los procedimientos de verificación.

- **Políticas de contraseña:** garantizan que las contraseñas cumplan con requisitos mínimos y se cambien periódicamente.

- **Políticas de uso aceptable:** identifican los recursos y el uso de red que son aceptables para la organización. También puede identificar las consecuencias de las violaciones de la política.

- **Políticas de acceso remoto:** identifican cómo los usuarios remotos pueden obtener acceso a la red y cuál es accesible de manera remota.

- **Políticas de mantenimiento de red:** especifican los sistemas operativos de los dispositivos de la red y los procedimientos de actualización de las aplicaciones de los usuarios finales.

- **Políticas de manejo de incidentes:** describen cómo se manejan los incidentes de seguridad.

Uno de los componentes más comunes de la política de seguridad es una política de uso aceptable (AUP). Este componente define qué pueden y no pueden realizar los usuarios en los distintos componentes del sistema. El AUP debe ser lo más explícito posible para evitar la mala interpretación. Por ejemplo, un AUP enumera las páginas web, los grupos informativos o las aplicaciones de uso intensivo de ancho de banda específicos a las que los usuarios no pueden acceder utilizando las computadoras o la red de la empresa.

Políticas Producto integrador:

Política de Contraseña:

1. Deberán tener una longitud igual o superior a 8 caracteres.
2. Estar compuesta por uno o más caracteres de al menos 3 de estos grupos:
   - Letras mayúsculas (de la A a la Z)
   - Letras minúsculas (de la a a la z)
   - Números (del 0 al 9)
   - Símbolos (caracteres no alfanuméricos): ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
3. La contraseña no deberá ser igual a ninguna de las 6 últimas contraseñas usadas
4. No contendrá el nombre de cuenta del usuario o partes de su nombre completo.
5. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma.
6. La contraseña se deberá cambiar al menos una vez al año.
7. Pasado el tiempo de caducidad de la contraseña, la cuenta será bloqueada

Política de uso de contraseñas:

No utilizar la contraseña de acceso al equipo para otros servicios (ej. Cuenta de correo)

Si un usuario entiende que su contraseña ha quedado comprometida o la ha cedido a terceros autorizados por motivos de trabajo o mantenimiento, debe sustituirla por otra que no hubiera sido comprometida, de manera inmediata.

Las contraseñas no deben incluirse en ningún tipo de comunicación electrónica. En medios de comunicación internos o externos a la empresa.

En ningún caso se le solicitará que incluya la contraseña en ningún cuestionario o formulario que reciba por correo electrónico.

No es recomendable incluir sugerencias (hints) para recordar contraseñas. No habilite tampoco la funcionalidad de 'pregunta secreta' y si es obligatorio, no incorpore información verídica relacionada con usted.

No escriba jamás su contraseña en ordenadores públicos, compartidos o aquellos en que se desconozca su nivel de seguridad o se estime que pueden estar monitorizados de

forma remota, por ejemplo, si se conecta desde un cibercafé o un terminal de acceso a Internet de un aeropuerto.

No escriba su contraseña y la almacene cerca de su lugar de trabajo habitual. Tampoco guarde sus contraseñas en un fichero en su ordenador, teléfono móvil o Tablet salvo que dicho fichero se almacene cifrado.

No escriba su contraseña si el acceso a la web del servicio no se realiza mediante protocolo web seguro (‘https’)

No emplee la opción ‘Recordar contraseña’ que ofrecen los navegadores, especialmente cuando se trate de ordenadores compartidos.

Ante cualquier sospecha de que su contraseña ha podido ser comprometida, avise a soporte técnico y cámbiela.

Políticas de administración de recursos del equipo:

El usuario tendrá solo acceso a las herramientas preinstaladas en el ordenador.

Solo el administrador podrá realizar cambios en el equipo, y solo el tendrá acceso a la configuración de este.

El usuario no tiene permitido retirar ninguna de las piezas de hardware del equipo.

El usuario no tiene permitido conectar ningún tipo de hardware al equipo aparte del que se ha provisto por parte de la empresa.

Con respecto al uso del internet las siguientes actividades están prohibidas:

- No se permite el uso personal excesivo de Internet y correo electrónico que interfieran con el trabajo del empleado.
- Exhibición o almacenamiento de cualquier material obsceno.
- Actividades de juego
- Descarga de juegos personales, etc.
- Almacenamiento de aplicaciones no relacionadas con el negocio en computadoras personales.
- Hacer negocios de cualquier tipo para uso personal
- Eliminar registros de la compañía sin permiso.
- Envío de imágenes personales.
- Uso de dispositivos electrónicos sin permiso.
- Descargar o hacer circular material pirateado.
- Circulación de cualquier mensaje que contenga acoso, comportamiento difamatorio o amenazante.
- Sitios web que consuman mucho ancho de banda
- Descargar cualquier tipo de programa
- Cualquier tipo de redes sociales
- Acceso a paginas web que no cumpla con el protocolo https

Políticas de Seguridad físicas del equipo:

- Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.
- Colocarlas fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico (balastras, equipo industrial, etc.), agua, etc.
- Todos los servidores deberán ubicarse en lugares de acceso físico restringido y deberán contar para acceder a ellos con puertas con chapas. El lugar donde se instalen los servidores contará con una instalación eléctrica adecuada, entre sus características con tierra física. Y dichos equipos deberán contar con NO-BREAKS. En los lugares donde se encuentren equipo de cómputo queda prohibido el consumo de bebidas y alimentos.
- El lugar donde se encuentre los servidores mantendrá condiciones de higiene.
- Deberá contarse con extintores en las salas de cómputo. El personal deberá estar capacitado en el uso de extintores.
- Las salas de cómputo deberán contar con una salida de emergencia

Políticas de Cuentas:

- Sean miembros vigentes de la empresa
- Participen en proyectos especiales y tenga la autorización del jefe del área.
- Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
- La asignación de cuentas la hará el administrador del servidor del área en cuestión y al usuario sólo le dará derecho de acceder a los recursos al servidor donde se realiza el registro.
- El administrador podrá deshabilitar las cuentas que no sean vigentes.
- La cuenta y contraseña personales son intransferibles.

Políticas de control de accesos:

- Todos los administradores que den un servicio de acceso remoto deberán contar con aplicaciones que permitan una comunicación segura y encriptada.
- Todos los usuarios deberán autentificarse con su cuenta y no podrán hacer uso de sesión es activas de otros usuarios.
- Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y encriptada.
- Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
- Si un usuario está fuera del sitio de trabajo, debe conectarse a una máquina pública del sitio y, únicamente desde ésta, hacer la conexión a la computadora deseada.

- Al momento de ingresar a un sistema, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual permitirá detectar fácilmente el uso no autorizado del sistema.
- El usuario tendrá el derecho a cambiar su contraseña.

Políticas de respaldos:

Para el usuario:

- Será responsabilidad del usuario mantener una copia de la información de su cuenta.

Para el administrador del sistema:

- El administrador del sistema es el responsable de realizar respaldos de la información crítica, siempre que tenga los medios físicos para realizarla. Cada treinta días deberá efectuarse un respaldo completo del sistema. Y deberá verificar que se haya realizado correctamente.
- El administrador del sistema es el responsable de restaurar la información.
- La información respaldada deberá ser almacena da en un lugar seguro.
- Deberá mantenerse una versión reciente de los archivos más importantes del sistema.
- En el momento en que la información respalda da deje de ser útil al a organización, dicha información deberá ser borrada antes de deshacerse del medio.

Reflexión

La existencia de las políticas es de suma importancia para establecer un estándar de seguridad mínimo dentro de una corporación, así como una normalización de las medidas que se utilizan para implementarla, de modo que se vuelve más sencillo revisar la integridad de la seguridad en escala empresarial y es posible mejorar esa seguridad de manera general implementando políticas más estrictas a todos los empleados. Vemos como las políticas no se limitan a la seguridad de contraseñas, sino que se extienden a los diferentes ámbitos en el contexto de autenticación, privacidad, integridad física y respaldo de los equipos y la información.

Referencias

- Cisco Security: Cybersecurity Essentials, 2.2.1.4 Leyes y responsabilidades. Recuperado el 26/03/2021
- Cisco Security: Cybersecurity Essentials, 2.4.3.1 Politics. Recuperado el 26/03/2021
- Cisco Security: Cybersecurity Essentials, 7.2.2.3 Políticas de grupo. Recuperado el 26/03/2021