Desafío - Control de acceso basado en roles

En este desafío validaremos nuestros conocimientos de políticas basados en roles . Para lograrlo, necesitarás aplicar los conocimientos vistos hasta el momento en la unidad , utilizando de apoyo la información proporcionada en el siguiente documento.

Lee todo el documento antes de comenzar el desarrollo **individual** para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

// Tiempo asociado: 1 hora cronológica.

Descripción

A continuación se proponen las políticas que tiene la empresa CYBEROPS S.A implementado en su organización, en donde nuestro objetivo será el análisis como también la propuestas de nuevas políticas basadas en roles en este caso.

Requerimientos

Leer la siguiente política de acceso y luego responder las preguntas propuestas.
Política Control de Acceso Empresa “CYBEROPS”

1. Para lograr una efectiva protección de los recursos de información de CYBEROPS, es indispensable contar con las capacidades para otorgar acceso de acuerdo a las reales necesidades de los usuarios y considerando el principio del “menor privilegio posible”, es decir, a cada usuario debe autorizársele únicamente el nivel de acceso necesario para cumplir con sus funciones.

2. A continuación se establecen los lineamientos generales para definir las políticas de acceso de los distintos activos de información de CYBEROPS. Estos lineamientos deberán ser tomados en consideración por los “dueños de la información” y por el Oficial de Seguridad, a fin de que se logre un apropiado balance de funcionalidad y seguridad en el uso de la tecnología de información en la empresa.

3. Requerimiento de negocio para el control de acceso: todos los accesos a los recursos de información de CYBEROPS, deben basarse en las necesidades en

función del negocio de la empresa y del rol del usuario.

4. Gestión de acceso de los usuarios: con el propósito de impedir accesos no autorizados a los recursos de información, deben establecerse procedimientos formales para asignar los derechos de acceso a los sistemas. Estos procedimientos deben abarcar el ciclo de vida completo de los usuarios en la organización, es decir, su ingreso, mantenimiento y terminación de la condición de empleado. Estos procedimientos son de particular importancia en el caso de la asignación de derechos de acceso con privilegios elevados. Para efectos de lograr la cobertura de los aspectos más relevantes, los procedimientos deberán considerar:
    - Registro de usuarios
    - Gestión de accesos privilegiados
    - Gestión de contraseñas
    - Revisión periódica de derechos de los usuarios

5. Responsabilidad de los usuarios: los usuarios deben ser informados de sus responsabilidades y de la importancia de su cooperación en el éxito de las medidas de seguridad. Los tópicos a cubrir en las actividades de sensibilización y educación de las responsabilidades deben considerar al menos los siguientes temas:
    - Uso de contraseñas
    - Equipos desatendidos.

6. Control de acceso a la red: el acceso a los recursos de red, tanto internos como externos, debe ser controlado, de manera que los usuarios no comprometan la seguridad de los activos de información. En las políticas específicas de esta materia deben considerarse los siguientes puntos:
    - Política de uso de la red.
    - Ruta de acceso forzada, en los casos en que, por la criticidad de los recursos involucrados, se estime conveniente y/o necesario.
    - Autenticación de los usuarios para los accesos remotos.
    - Autenticación de nodos intermediarios de enlace.
    - Protección de puertos de diagnóstico remoto de servicios o sistemas que tengan esta capacidad.
    - Segmentación de redes.
    - Control de conexiones a redes con base en políticas.
    - Controles de enrutamiento de redes.
    - Seguridad en los servicios de red.

7. Control de acceso al sistema operativo: el acceso al sistema operativo de los sistemas computacionales en uso en la empresa debe ser debidamente controlado, a fin de evitar accesos no autorizados a recursos o información. Dentro de los aspectos que deben ser tomados en consideración para definir las políticas de acceso y sus respectivos controles, se incluyen:
    - Identificación automática de terminales.

- Procedimientos de inicio de sesión seguros.
- Identificación y autenticación de usuarios.
- Sistema de gestión de contraseñas.
- Uso de herramientas utilitarias del sistema operativo.
- Sistema de alarma ante asalto o coerción del usuario.
- Desconexión automática de terminales por tiempo de inactividad.
- Limitación del tiempo de conexión.

8. Control de acceso a las aplicaciones: con el propósito de impedir el acceso a la información que se mantiene en las aplicaciones, debe restringirse el acceso a los usuarios debidamente autorizados.

9. Aislamiento de sistemas con información.

10. Monitoreo del uso de los sistemas: con el propósito de detectar actividades no autorizadas, los sistemas deben ser monitoreados en función de las políticas de acceso establecidas, de manera que se registre la evidencia en caso de incidentes de seguridad.

11. Registro de eventos.

12. Registro de uso de los sistemas.

13. Sincronización de relojes para exactitud de los registros de tiempo.

14. Computación móvil y teletrabajo: a pesar de la indiscutible conveniencia de las facilidades actuales de teletrabajo y computación, debe considerarse el riesgo que representa para los activos de información de CYBEROPS, por lo que deberán evaluarse las medidas de seguridad que proporcionen un nivel de seguridad acorde a la sensibilidad de la información que se maneja en estos escenarios, así como los potenciales riesgos.

15. Control de acceso lógico: todos los recursos computacionales, de comunicaciones electrónicas y, en general, todos los recursos electrónicos de CYBEROPS, deben contar con, al menos, un Control de Acceso Específico.

16. Acceso lógico restringido: el acceso a todos los recursos está limitado a aquellos usuarios y/o sistemas que cuenten con la autorización necesaria. El acceso de cualquier usuario o sistema sin autorización previa facultará a CYBEROPS para emprender acciones legales o sanciones disciplinarias, según corresponda, contra el o los infractores.

17. Derecho de admisión acceso lógico: CYBEROPS podrá denegar o bloquear el acceso a cualquier usuario sistema unilateralmente en casos justificados.

18. Lista de acceso lógico autorizado: los ingenieros a cargo de cada plataforma confeccionarán, administrarán y pondrán a disposición de quienes requieran la información para su trabajo, las listas de usuarios, sistemas con acceso autorizado y tipo de control de acceso.

A continuación, responder las siguientes preguntas:

1. ¿A qué tipo de usuarios de la compañía afecta esta política? ¿Le parece razonable dicha definición? (1 punto)

2. ¿A qué tipo de Información de aplica esta política? **(1 Punto)**

3. ¿A qué se refiere con "ciclo de vida completo de un usuario"? **(1 Punto)**

4. ¿Cuáles son los aspectos que considera la política descrita en el documento? **(1 Punto)**

5. ¿Quién es responsable que la política se cumpla? **(1 Punto)**

6. ¿Qué dice la política frente al caso de un usuario que se levanta de su puesto de trabajo y NO activa el protector de pantalla? **(1 Punto)**

7. ¿Qué dice la política en caso de que un usuario NO la cumpla y esto produzca algún perjuicio a la empresa? **(1 Punto)**

8. ¿Qué dice la política respecto del acceso físico a las dependencias de la empresa? **(1 Punto)**

9. Realizar una tabla que indique área o departamento de la empresa, el rol respectivo y las políticas que esta tendría implementada en esta organización. Explicar el por que de estos niveles. **(2 Puntos)**