Actividad 10. ISO 27002-2022

8.2. DERECHOS DE ACCESO PRIVILEGIADOS

1. Describir un control de la ISO 27002-2022.
2. Los términos para definir se encuentran en el documento controles. El docente asignará a cada alumno un control.
3. Cada alumno buscará información del control asignado en la norma ISO 27002-2022 y elaborará una descripción de este, indicando la variación respecto a la versión anterior de la norma.
4. El alumno debe elaborar un documento explicando el control asignado.
5. Cada alumno explicará los términos asignados en clase.

8.2. DERECHOS DE ACCESO PRIVILEGIADOS

Tipo de control	**Información (propiedades de seguridad)**	**La seguridad cibernética (conceptos)**	**Capacidad operativa (Habilidades)**	**Dominios de seguridad**
# Preventivo	# Confidencialidad # Integridad # Disponibilidad	# Proteger	#identidad_y_access_management	# Proteccion

La asignación y el uso de derecho de acceso privilegiado deben registrarse y gestionarse.

Su propósito es garantizar que sólamente los usuarios, componentes y servicios de software autorizados reciban derechos de acceso privilegiados.

GUÍA:

1. **Proceso de Autorización**:

a. Identificar a los usuarios que necesiten derechos de acceso privilegiado para cada sistema o proceso.
b. Asignar derechos de acceso privilegiado de manera individual según la política específica de control de acceso.
c. Mantener el registro y proceso de la autorización de todos los privilegios asignados.

2. **Gestión de Derechos**:

    a. Definir los requisitos para la expiración de los derechos de acceso privilegiado.
    b. Informar a los usuarios sobre sus derechos de acceso privilegiado cuando estén en modo de acceso privilegiado.
    c. Asegurar que los requisitos de autenticación para los derechos de acceso privilegiado sean más altos que para los procesos normales.

3. **Revisión y Actualización**:

    a. Si hay algún cambio organizacional, se revisa periódicamente la necesidad de los usuarios de seguir teniendo los derechos de acceso privilegiado.
    b. Establecen reglas para evitar el uso de identificadores de usuario de administración genéricas, gestionando y protegiendo así la información de autenticación de dichas identidades.

4. **Acceso Temporal**:

    a. Otorgar el acceso privilegiado temporal sólo durante el tiempo necesario para realizar cambios o actividades específicas, utilizando procedimientos automatizados si es posible.

5. **Registro y Auditoría**:

    a. Registrar todos los accesos privilegiados a los sistemas para fines de auditoría.

6. **Identidades Separadas**:

a. No compartir las identidades con los derechos de acceso privilegiado entre múltiples personas.
b. Usar identidades separadas para tareas administrativas y tareas generales del día a día.

INFORMACIÓN ADICIONAL:

a. Los derechos de acceso privilegiado permiten realizar actividades que los usuarios típicos no pueden realizar.
b. El uso inapropiado de privilegios administrativos es un factor importante en fallas o violaciones del sistema.
c. Se puede encontrar más información sobre la gestión de acceso en la ISO/IEC 29146.

En definitiva, la asignación y uso de derechos de acceso privilegiado deben estar restringidos y gestionados mediante un proceso de autorización. Esto asegura que sólo los usuarios autorizados deben realizar tareas críticas, se revisen regularmente los permisos y se registren las actividades para auditorías.