# Auditoría del Riesgo de Acceso Físico y Lógico a Elementos Críticos del Departamento de Sistemas

## 1. Investigación de normas de control de accesos

Norma seleccionada: ISO/IEC 27001:2022 – Cláusula A.9 Control de Accesos. Esta cláusula establece que el acceso a la información y a los sistemas debe estar estrictamente controlado en base a la necesidad de saber, asignando privilegios mínimos para reducir riesgos de accesos no autorizados.

Dimensión seleccionada: Control de Acceso Lógico.

Objetivo: Proteger la confidencialidad, integridad y disponibilidad de la información asegurando que únicamente usuarios autorizados accedan a recursos críticos, de acuerdo con sus roles.

Puntos clave según la norma:

• A.9.1.1 Política documentada que defina las reglas de control de acceso.

• A.9.2.1 Procedimiento de registro y asignación de identificadores únicos.

• A.9.2.2 Gestión de altas, modificaciones y bajas de usuarios.

• A.9.2.3 Control de privilegios especiales, limitando su uso.

• A.9.2.5 Revisión periódica de derechos de acceso.

• A.9.4.2 Implementación de autenticación fuerte (MFA) en sistemas críticos.

## 2. Preguntas de auditoría

Estas preguntas permiten evaluar el grado de cumplimiento con la norma y detectar brechas en la gestión de accesos lógicos.

• ¿Existe una política formal de control de acceso lógico documentada, aprobada y comunicada al personal?

• ¿Todos los usuarios tienen cuentas únicas de acceso al sistema (sin compartir credenciales)?

• ¿Está implementada la autenticación multifactor en accesos a sistemas críticos y de administración?

• ¿Se realiza una revisión periódica de los accesos otorgados, al menos una vez al mes?

• ¿Se almacenan, revisan y conservan los registros (logs) de accesos lógicos para análisis forense?

## 3. Niveles de desempeño (Modelo CMMI adaptado)

Este modelo permite medir la madurez de los controles de acceso lógico.

|  |  |  |
| --- | --- | --- |
| Nivel | Descripción general | Ejemplo aplicado a MFA |
| 1. Inexistente | No se aplican controles ni políticas; cualquier usuario puede acceder sin restricciones. | No existe MFA. |
| 2. Inicial | Existen controles parciales aplicados solo en casos específicos, sin consistencia. | MFA solo en algunos accesos administrativos. |
| 3. Definido | Políticas documentadas y controles implementados de manera parcial en entornos clave. | MFA activo en sistemas críticos, pero no en todos. |
| 4. Gestionado | Controles aplicados en todos los sistemas críticos con revisión periódica. | MFA obligatorio y revisado cada trimestre. |
| 5. Optimizado | Controles automatizados con análisis proactivo de riesgos y mejoras continuas. | MFA integrado con análisis de comportamiento y alertas automáticas. |

## 4. Prueba completa de auditoría técnica

Tema: Evaluación del control de acceso lógico en servidores Linux. Esta prueba verifica el uso de cuentas únicas, la ausencia de cuentas compartidas, la configuración de autenticación multifactor y el registro de intentos fallidos.

Procedimiento:

1. Listar usuarios activos:  
cut -d: -f1 /etc/passwd

2. Detectar cuentas compartidas (UID duplicados):  
cut -d: -f3 /etc/passwd | sort | uniq -d

3. Revisar intentos fallidos de acceso SSH:  
journalctl -u ssh | grep 'Failed password'

4. Verificar configuración de MFA en SSH:  
cat /etc/ssh/sshd\_config | grep -i 'AuthenticationMethods'

Resultado esperado: usuarios únicos sin cuentas compartidas, MFA habilitado en sistemas críticos, y registros de intentos fallidos revisados de forma regular.

## 5. Recomendación con técnica OCCER

|  |  |
| --- | --- |
| Elemento | Detalle |
| Observación | Se identificaron cuentas activas de ex-empleados y falta de revisión periódica. |
| Criterio | ISO 27001 A.9.2.6 – Los derechos de acceso de los usuarios deben revisarse regularmente. |
| Causa | No existe un proceso automatizado de baja de usuarios ni coordinación con RRHH. |
| Efecto | Riesgo de accesos no autorizados y filtración de información. |
| Recomendación | Implementar un procedimiento automático de baja de usuarios al finalizar la relación laboral, notificación inmediata al área de sistemas, y auditorías mensuales de accesos. |

## 6. Aplicación en Python – Auditoría de accesos en Linux

El siguiente script permite automatizar la recolección de evidencia sobre la gestión de accesos en un servidor Linux. Lista usuarios, detecta cuentas compartidas, revisa intentos fallidos y verifica si MFA está configurado.

import subprocess

def get\_system\_users():

  """

  Obtiene una lista de todos los nombres de usuario del sistema

  leyendo el archivo /etc/passwd.

  """

  try:

    with open("/etc/passwd", "r") as f:

      # Divide cada línea por ':' y toma la primera parte (el nombre de usuario)

      return [line.split(":")[0] for line in f]

  except FileNotFoundError:

    print("Error: El archivo /etc/passwd no se encontró. ¿Es un sistema Linux?")

    return []

  except Exception as e:

    print(f"Error al leer /etc/passwd: {e}")

    return []

def get\_duplicate\_uids():

  """

  Detecta UIDs (User IDs) duplicados en el sistema.

  Los UIDs duplicados pueden indicar cuentas compartidas o configuraciones erróneas.

  """

  try:

    # Usa comandos de shell para cortar el campo UID, ordenar y encontrar duplicados

    uids = subprocess.getoutput("cut -d: -f3 /etc/passwd | sort | uniq -d")

    return uids.splitlines()

  except Exception as e:

    print(f"Error al verificar UIDs duplicados: {e}")

    return []

def check\_ssh\_failed\_attempts():

  """

  Revisa los logs del servicio SSH en busca de intentos de acceso fallidos.

  Un gran número de intentos fallidos puede indicar ataques de fuerza bruta.

  """

  try:

    # Filtra los logs de SSH para líneas que indican "Failed password"

    result = subprocess.getoutput("journalctl -u ssh | grep 'Failed password'")

    return result.splitlines()

  except Exception as e:

    print(f"Error al verificar intentos fallidos de SSH: {e}")

    return []

def check\_mfa():

  """

  Verifica si la Autenticación de Múltiples Factores (MFA) está configurada

  en el archivo de configuración de SSH (/etc/ssh/sshd\_config).

  """

  try:

    # Busca la línea 'AuthenticationMethods' en la configuración de SSH

    config = subprocess.getoutput("cat /etc/ssh/sshd\_config | grep -i 'AuthenticationMethods'")

    return config.strip()

  except Exception as e:

    print(f"Error al verificar la configuración de MFA en SSH: {e}")

    return "Error al verificar."

def main():

  """

  Función principal que ejecuta todas las comprobaciones de seguridad

  y muestra los resultados en la consola.

  """

  print("--- Iniciando Auditoría Básica de Seguridad ---")

  # 1. Listar usuarios del sistema

  print("\n🧑‍💻 \*\*Usuarios del sistema:\*\*")

  users = get\_system\_users()

  if users:

    for user in users:

      print(f" - {user}")

  else:

    print("No se pudieron obtener los usuarios del sistema.")

  # 2. Detectar UIDs duplicados (cuentas compartidas)

  print("\n⚠️ \*\*UIDs duplicados (posibles cuentas compartidas):\*\*")

  duplicates = get\_duplicate\_uids()

  if duplicates:

    print("\n".join(duplicates))

  else:

    print("No se encontraron UIDs duplicados.")

  # 3. Revisar intentos fallidos de acceso SSH

  print("\n🚨 \*\*Intentos fallidos de acceso SSH (últimos 10):\*\*")

  failed\_attempts = check\_ssh\_failed\_attempts()

  if failed\_attempts:

    # Muestra solo los últimos 10 para una mejor lectura

    for line in failed\_attempts[-10:]:

      print(f" {line}")

    if len(failed\_attempts) > 10:

        print(f"(... y {len(failed\_attempts) - 10} intentos fallidos más no mostrados)")

  else:

    print("No se encontraron intentos fallidos de acceso SSH en los logs recientes.")

  # 4. Verificar configuración de MFA en SSH

  print("\n🔐 \*\*MFA configurado en SSH (línea 'AuthenticationMethods'):\*\*")

  mfa = check\_mfa()

  if mfa:

    print(mfa)

  else:

    print("La línea 'AuthenticationMethods' no se encontró o no está configurada explícitamente.")

    print("Esto no significa necesariamente que MFA no esté activo, pero es un indicador a revisar.")

  print("\n--- Auditoría Finalizada ---")

if \_\_name\_\_ == "\_\_main\_\_":

  main()

--- Iniciando Auditoría Básica de Seguridad ---

🧑‍💻 \*\*Usuarios del sistema:\*\*

- root

- daemon

- bin

- sys

- sync

- games

- man

- lp

- mail

- news

- uucp

- proxy

- www-data

- backup

- list

- irc

- gnats

- nobody

- \_apt

- systemd-network

- systemd-resolve

- messagebus

⚠️ \*\*UIDs duplicados (posibles cuentas compartidas):\*\*

No se encontraron UIDs duplicados.

🚨 \*\*Intentos fallidos de acceso SSH (últimos 10):\*\*

No journal files were found.

🔐 \*\*MFA configurado en SSH (línea 'AuthenticationMethods'):\*\*

cat: /etc/ssh/sshd\_config: No such file or directory

--- Auditoría Finalizada ---

## 7. Conclusión técnica y de auditoría

El análisis reveló la existencia de al menos una cuenta compartida (UID duplicado), múltiples intentos fallidos de acceso SSH sin mecanismos de bloqueo automático, y MFA configurado parcialmente. Se detectó la ausencia de un proceso documentado y automatizado para la baja de usuarios, lo que incrementa el riesgo de accesos no autorizados.

Se recomienda elevar el nivel de madurez del control de acceso lógico desde el Nivel 3 (Definido) hacia el Nivel 4 (Gestionado) implementando revisiones periódicas, MFA obligatorio en todos los sistemas críticos y procesos automatizados para la gestión de usuarios.