Laboratorio # 07

Sesión # 07 Segmentación de Redes y VLANs

Título del Laboratorio: Implementación de Seguridad, Cifrado y Políticas para Datos Sensibles en Azure
Duración: 2 horas
Objetivos del Laboratorio:

1. **Creación de DATA Sensible:**
   - Diseñar y configurar una Cuenta de almacenamiento para datos sensibles.
2. **Configuración de Cifrado con Azure Key Vault:**
   - Proteger los datos almacenados en Azure utilizando Azure Key Vault.
3. **Implementación de Monitoreo y Alertas:**
   - Supervisar y analizar eventos de seguridad en Azure utilizando Azure Log Analytics y Azure Monitor.
4. **Documentación del Flujo de Datos y Políticas:**
   - Documentar el flujo de datos y las políticas de seguridad implementadas en Azure.
5. **Evaluación de la Efectividad de los Controles Implementados:**
   - Validar la efectividad de los controles de seguridad implementados en Azure.

Materiales Necesarios:

- Cuenta activa de Microsoft Azure (puede ser una cuenta gratuita o de estudiante).
- Navegador web actualizado (Edge, Chrome, Firefox).
- Conexión a internet estable.
- Acceso a Azure Cloud Shell o Azure CLI instalado localmente.

Documento de Ayuda:

- Documentación oficial de Azure Regions
- Documentación oficial de Azure Storage Account
- Documentación oficial de Azure Key Vault
- Documentación oficial de Azure Monitor
- Documentación oficial de Azure Activity Logs

- Documentación oficial de Network Security Groups (NSG)

Historia del Laboratorio:

Clínica Vida Segura se enfrenta al reto de garantizar la confidencialidad, integridad y disponibilidad de los datos médicos de sus pacientes. Esto incluye información altamente sensible como historiales clínicos, resultados de laboratorio, diagnósticos y datos personales, que deben estar protegidos contra accesos no autorizados, alteraciones malintencionadas y posibles pérdidas.

Para lograr este objetivo, la clínica ha decidido implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en el **estándar ISO/IEC 27001**, asegurando el cumplimiento normativo y la gestión eficiente de riesgos de ciberseguridad en su infraestructura digital.

Estructura del Laboratorio:

1. Introducción y Comprensión del Entorno (5 minutos)

Lectura Teórica: Contexto y Teoría
Cifrado de Datos
Azure ofrece cifrado en reposo y en tránsito para proteger los datos sensibles. Azure Key Vault gestiona claves y secretos de cifrado.

Monitoreo y Alertas
Azure Monitor permite supervisar el estado de los recursos. La integración con Log Analytics y Azure Alerts facilita la detección de incidentes.

Políticas de Seguridad

El uso de Network Security Groups (NSG) y Azure Policy permite aplicar controles de acceso y cumplimiento de normativas.

2. Actividades del Laboratorio (95 minutos):

Paso 1: Creación grupo de recursos (5 min)

Objetivo: Diseñar un Grupo de recursos para almacenar lo necesario en este lab

1. **Iniciar sesión en Azure:**

2. Crear dos grupos de recursos en diferentes regiones

Paso 2: Políticas para el control de datos de la cuenta de almacenamiento (20 minutos)

Objetivo:

Garantizar la seguridad y cumplimiento en la gestión de datos mediante la aplicación de políticas que protejan las cuentas de almacenamiento

Aplicar Políticas de Seguridad a las cuentas de almacenamiento

Políticas>Agregar Directiva> Ingresar su Json (ANALIZAR)> Asignarlo a su grupo de recursos

Política 1: Requerir cifrado con claves administradas por el cliente

Esta política asegura que todas las cuentas de almacenamiento utilicen cifrado con claves de cliente desde Azure Key Vault.

```
{
  "properties": {
    "displayName": "Requerir cifrado con claves administradas por el cliente en cuentas de almacenamiento",
    "policyType": "Custom",
    "mode": "All",
    "description": "Esta política asegura que todas las cuentas de almacenamiento utilicen cifrado con claves de cliente desde Azure Key Vault.",
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Storage/storageAccounts"
          },
          {
            "field": "Microsoft.Storage/storageAccounts/encryption.keySource",
            "notEquals": "Microsoft.Keyvault"
          }
        ]
      },
```

```
        "then": {
          "effect": "deny"
        }
      }
    }
}
```

Política 2: Requerir TLS mínimo 1.2 en cuentas de almacenamiento

Esta política asegura que las cuentas de almacenamiento solo acepten conexiones con TLS 1.2 o superior.

```
{
  "properties": {
    "displayName": "Requerir TLS mínimo 1.2 en cuentas de almacenamiento",
    "policyType": "BuiltIn",
    "mode": "All",
    "description": "Esta política asegura que las cuentas de almacenamiento solo acepten conexiones con TLS 1.2 o superior.",
    "policyRule": {
      "if": {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Storage/storageAccounts"
          },
          {
            "field": "Microsoft.Storage/storageAccounts/minimumTlsVersion",
            "notEquals": "TLS1_2"
          }
```

```
            ]
        },
        "then": {
            "effect": "deny"
        }
    }
  }
}
```

Paso 3: Configuración Seguridad en redes para SGSI (10 minutos)

1. Crear la Red Virtual (VNet)

Define una red virtual para aislar los recursos. Usa un nombre acorde a la infraestructura.

2. Configurar Subredes

Segmenta los recursos en subredes específicas:

- **subnet-storage**: Destinada a la cuenta de almacenamiento.
- **subnet-keyvault**: Exclusiva para Azure Key Vault.

3. Crear un Grupo de Seguridad de Red (NSG)

Establece un NSG para controlar el tráfico de red de forma segura.

4. Definir Reglas del NSG

Configura las siguientes reglas de seguridad:
Permitir tráfico HTTPS (puerto 443) solo desde tu IP
Bloquear todo el tráfico entrante que no sea HTTPS

5. Asociar el NSG a la Red Virtual

Aplica el NSG a la VNet para que las reglas definidas entren en vigor.

Paso 4: Configuración de Cifrado con Azure Key Vault (10 minutos)

Objetivo: Implementar mecanismos de cifrado para proteger la confidencialidad de los datos almacenados.

1. **Crear Key Vault en ambas regiones:**

Crear un Key Vault en **la región de LAB14**

Generar claves de cifrado:

- Generar una clave de cifrado.
- De ser necesario cree una identidad administrada y proporciónele roles.

Paso 5: Configuración de Seguridad en la Cuenta de Almacenamiento (CMK y TLS 1.2) (10 minutos)
Objetivo:

Configurar una **cuenta de almacenamiento** en Azure con **cifrado mediante claves administradas por el cliente (CMK)** y establecer **TLS 1.2 como versión mínima permitida**.

1 Crear la Cuenta de Almacenamiento

1. En el portal de **Azure**, busca y selecciona **Cuentas de almacenamiento**.
2. Haz clic en **+ Crear**.
3. Completa los siguientes valores:
    - **Suscripción:** Selecciona tu suscripción.
    - **Grupo de recursos:** Usa uno existente o crea uno nuevo.
    - **Nombre de la cuenta:** Escribe un nombre único (Ejemplo: `storagecmksecure`).
    - **Región:** Selecciona la región deseada.
    - **Redundancia:** Selecciona **LRS (Local Redundant Storage)** o la que prefieras.
4. Ve a la pestaña **Opciones avanzadas** y asegúrate de que:
    - **TLS mínimo** está configurado en **1.2**.
    - **Habilitar clave administrada por el cliente (CMK)** está activado.
    - DE SER NECESARIO ASOCIE LA IDENTIDAD ADMINISTRADA
5. Haz clic en **Revisar + Crear** y luego en **Crear**.

---

2 Asociar la Clave del Key Vault a la Cuenta de Almacenamiento

1. Abre la **Cuenta de Almacenamiento** creada.
2. En el menú de la izquierda, selecciona **Cifrado**.
3. Cambia el método de cifrado a **Claves administradas por el cliente (CMK)**.
4. En **Seleccionar un Key Vault y una clave**, haz clic en **Elegir un Key Vault** y selecciona el que tenga la clave configurada.
5. Luego, haz clic en **Elegir una clave** y selecciona la clave generada.
6. Guarda los cambios.

Paso 6: Generación de Archivos de Datos Sensibles Médicos (15 minutos)
Objetivo:

Crear un conjunto de datos sintéticos de historiales médicos utilizando Python, asegurando la generación estructurada de información sensible para pruebas o simulaciones.

Paso a Paso (CLI de Azure)
1) Instalar Python en la CLI de Azure

Ejecuta el siguiente comando en la terminal de Azure para instalar Python:

```
sudo apt update && sudo apt install -y python3 python3-pip
```

Verifica la instalación con:

```
python3 --version
```

---

2) Instalar las bibliotecas necesarias

Ejecuta el siguiente comando para instalar `pandas` y `faker`:

bash
CopiarEditar

```
pip install pandas faker
```

---

3) Crear el script para generar datos médicos
Crea un nuevo archivo con el editor `nano`:

```
nano generar_historial.py
```

Copia y pega el siguiente código en el archivo:
python:

```
import pandas as pd
import random
from faker import Faker

# Configuración
fake = Faker('es_ES')
n_pacientes = 50
consultas_por_paciente = 5

# Diagnósticos y especialidades
especialidades = {
    'Cardiología': ['Hipertensión', 'Arritmia', 'Insuficiencia cardíaca'],
    'Neurología': ['Migraña', 'Epilepsia', 'Esclerosis múltiple'],
    'Neumología': ['Asma', 'EPOC', 'Neumonía'],
    'Gastroenterología': ['Gastritis', 'Colitis', 'Hepatitis']
}

# Generar registros
registros = []
```

```
for i in range(n_pacientes):
    id_paciente = f'P{str(i + 1).zfill(3)}'
    nombre = fake.name()
    fecha_nacimiento = fake.date_of_birth(minimum_age=18, maximum_age=90).strftime('%Y-%m-
%d')
    seguro = random.choice(['Seguro A', 'Seguro B', 'Seguro C', 'Seguro D'])

    especialidad, diagnosticos = random.choice(list(especialidades.items()))

    for _ in range(consultas_por_paciente):
        fecha_consulta = fake.date_this_decade().strftime('%Y-%m-%d')
        diagnostico = random.choice(diagnosticos)
        medicamento = random.choice(['Losartán', 'Metformina', 'Salbutamol', 'Atorvastatina',
'Ibuprofeno'])
        notas = fake.sentence()

        registros.append({
            'ID_Paciente': id_paciente,
            'Nombre': nombre,
            'Fecha_Nacimiento': fecha_nacimiento,
            'Seguro': seguro,
            'Especialidad': especialidad,
            'Fecha_Consulta': fecha_consulta,
            'Diagnóstico': diagnostico,
            'Medicamento': medicamento,
            'Notas': notas
        })

# Guardar como CSV y JSON
archivo_csv = 'historiales_clinicos.csv'
archivo_json = 'historiales_clinicos.json'

df = pd.DataFrame(registros)
df.to_csv(archivo_csv, index=False)
df.to_json(archivo_json, orient='records', indent=4)

print(f"Archivos generados con {n_pacientes * consultas_por_paciente} registros: {archivo_csv},
{archivo_json}")
```

Guarda los cambios y cierra el editor

4) Ejecutar el script para generar los archivos

Corre el script con:

```
python3 generar_historial.py
```

Debería mostrar la respuesta esperada:

```
Archivos generados con 250 registros: historiales_clinicos.csv,
historiales_clinicos.json
```

5) Descargar los archivos generados

Ejecuta los siguientes comandos para descargar los archivos:

```
download historiales_clinicos.csv
download historiales_clinicos.json
```

Paso 7: Cree un Blob y suba los dos archivos generados y agregue su ip en Habilitado desde redes virtuales y direcciones IP seleccionadas (15 minutos)

Objetivo:

Garantizar el almacenamiento seguro de los datos sensibles generados, asegurando que solo dispositivos autorizados puedan acceder a ellos mediante restricciones de red en Azure.

1) Crear un contenedor en el almacenamiento de blobs

1. Dentro de la cuenta de almacenamiento, en el menú lateral izquierdo, selecciona **Contenedores**.
2. Haz clic en **+ Contenedor**.
3. Asigna un nombre, por ejemplo, historiales
4. Haz clic en **Crear**.

2) Subir los archivos al Blob Storage

1. Entra al contenedor historiales que creaste.
2. Haz clic en **Cargar**.
3. En la ventana emergente, selecciona **Examinar** y elige los archivos historiales_clinicos.csv y historiales_clinicos.json.
4. Asegúrate de que la opción **Tipo de blob** esté en **Bloque**.
5. Haz clic en **Cargar** y espera a que termine la subida.

3) Agregar tu IP en las reglas de acceso

1. Regresa a la cuenta de almacenamiento y selecciona **Redes** en el menú lateral.
2. En la sección **Habilitado desde redes virtuales y direcciones IP seleccionadas**, haz clic en **Agregar dirección IP**.
3. Se detectará automáticamente tu dirección IP pública. Confirma que sea la correcta.
4. Haz clic en **Guardar**.

Paso 8: Intentar acceder a los blobs desde otra dirección IP no especificada (15 minutos)

Objetivo:

Validar que las restricciones de acceso configuradas en el almacenamiento de blobs funcionan correctamente, permitiendo únicamente el acceso desde las direcciones IP autorizadas.

Paso a Paso: Verificación de acceso en la GUI de Azure

1. **Acceder desde la IP autorizada**
    1. Asegúrate de estar conectado a la red con la dirección IP que registraste en la configuración del almacenamiento.
    2. Ve al portal de Azure.
    3. Dirígete a **Cuentas de almacenamiento** y selecciona la cuenta configurada.
    4. En el menú lateral, entra a **Contenedores** y selecciona el contenedor `historiales`.
    5. Selecciona uno de los archivos subidos (`historiales_clinicos.csv` o `historiales_clinicos.json`).
    6. Haz clic en **Descargar** y verifica que se descargue correctamente.
        - **Resultado esperado:** Acceso permitido, archivo descargado.

2) Intentar acceder desde otra IP no autorizada

1. Cambia de red (por ejemplo, usa datos móviles en otro dispositivo o una VPN con una IP diferente).
2. Intenta acceder nuevamente al almacenamiento de blobs a través del portal de Azure.
3. Intenta descargar uno de los archivos.

   Resultado esperado: Acceso denegado, error de conexión.

3) Simulación de desconexión y reconexión

1. Desconéctate de la red actual y vuelve a la conexión que tiene la IP autorizada.
2. Repite los pasos para acceder a los blobs.
    - **Resultado esperado:** Acceso permitido solo después de reconectar la IP válida.

3. Cierre y Evaluación (10 minutos)

Resumen y Discusión de Resultados

A lo largo de este laboratorio, implementamos medidas clave para la protección de datos en Azure Storage, asegurando su confidencialidad e integridad. Configuramos claves administradas por el cliente (CMK) en Key Vault, restringimos el acceso a los blobs mediante direcciones IP específicas y verificamos que solo las IP autorizadas pudieran acceder a los datos. Estas acciones fortalecen la seguridad de la

información y garantizan el cumplimiento de buenas prácticas en la gestión de datos sensibles dentro de un Sistema de Gestión de Seguridad de la Información (SGSI).

Evaluación Rápida

1. ¿Por qué es fundamental documentar el flujo de datos y las políticas de seguridad en una organización dentro de un SGSI?
2. ¿Cómo contribuye la restricción de acceso por IP a la protección de la información en un SGSI?

Conclusión

Este laboratorio permitió explorar cómo aplicar controles de acceso en Azure Storage dentro de un SGSI para proteger datos sensibles. La correcta configuración de cifrado, la restricción de direcciones IP y el uso de claves seguras garantizan una estrategia de seguridad efectiva y alineada con las mejores prácticas de protección de la información. La implementación de estas medidas refuerza la capacidad de una organización para gestionar riesgos y asegurar el cumplimiento de estándares como la norma ISO 27001.

Recomendaciones

- Eliminar recursos: Una vez finalizado el laboratorio, eliminen todos los recursos creados (almacenamiento, claves, configuraciones de acceso) para evitar costos innecesarios.
- Mantenerse actualizados: Consultar regularmente la documentación de Azure y normativas de seguridad para mejorar continuamente la protección de la información en el SGSI.