ES-05 REGISTRO DE EVENTOS

1. Normatividad Relacionada

NO-02 Herramientas de Seguridad: Operación y Protección
NO-06 Almacenamiento de la Información
NO-07 Responsabilidad de Usuarios
NO-13 Comandos Especiales y Administración de Componentes Tecnológicos
NO-14 Administración y Configuración de Parámetros de Seguridad
NO-37 Seguridad y Uso Adecuado de Computadores de Escritorio
NO-40 Software y Hardware Utilizado

2. Objetivos

Establecer los parámetros de control de los accesos y el uso de los Componentes Tecnológicos de la UAEAC.

3. Componentes Tecnológicos Afectados

Todos los Componentes Tecnológicos de la UAEAC que requieran o usen registro de eventos.

4. Descripción

En todos los Componentes Tecnológicos, deben habilitarse los registros de auditoria (logs) para monitorear como mínimo los siguientes eventos:

- Actividades de administración del componente tecnológico, entre otros:
  - ✓ Encendido, reinicio y apagado de servidores
  - ✓ Cambio de fecha y hora del sistema
  - ✓ Actividades de administración de cuentas de usuario y grupos de usuarios (creación, bloqueo o inactivación, modificación y eliminación de cuentas, asignación de privilegios y manejo de contraseñas)
- Mensajes de alerta y error de los dispositivos
- Cambios a nivel de hardware de los servidores
- Tipo de conexiones activas:
  - ✓ Inicio de sesión local en servidores
  - ✓ Accesos remotos registrando como mínimo: identificación de usuarios, recursos accedidos y tiempos de conexión.

- Ejecución de comandos remotos entre servidores.
- Inicio de sesión, autenticación y cierre de sesión de cuentas inhabilitadas, cuentas de usuarios privilegiados, reactivación de cuentas expiradas, cuentas de acceso remoto.
- Eventos definidos por el Administrador o Responsable del Componente Tecnológico o por el Grupo Seguridad de la Información.
- Acceso a archivos y objetos definidos previamente de interés para auditar.
- Modificación y eliminación de datos de acuerdo con la clasificación de la información previamente acordada con los Responsables de la Información.
- Cambios a la parametrización de los Sistemas de Información.
- Registro de eventos o Logs generados por los Sistemas de Información.
- Se deben considerar los siguientes patrones para la administración de Logs:
  - ✓ Tiempo de almacenamiento en el sistema:
    - ✓ Sistema Operativo Servidores Unix y Linux: 6 meses
    - ✓ Sistema Operativo Servidores Windows: 2 semanas
    - ✓ Elementos activos de red: 2 semanas
    - ✓ Base de Datos Oracle: 3 meses
    - ✓ Correo Electrónico: 1 semana
  - ✓ Tiempo de retención en backups: Según la Tablas de Retención de la UAEAC las evidencias de incidentes de seguridad de la información deben permanecer 1 año en archivo de gestión y 10 años en archivo central.
    - ✓ Sistema Operativo Servidores Unix y Linux: 2 años
    - ✓ Sistema Operativo Servidores Windows: 1 año
    - ✓ Elementos activos de red: 1 año
    - ✓ Base de Datos Oracle: 5 años
    - ✓ Correo Electrónico: 1 mes

- En los Sistemas Windows Server y Windows Cliente se deberán auditar los siguientes eventos tanto **Exitosos como Fallidos**:
  - ✓ Auditar el acceso a objetos
  - ✓ Auditar el acceso del servicio de directorio
  - ✓ Auditar el cambio de directivas
  - ✓ Auditar el seguimiento de procesos
  - ✓ Auditar la administración de cuentas
  - ✓ Auditar sucesos de inicio de sesión
  - ✓ Auditar sucesos del sistema
- En cada una de las opciones de log se deben configurar los siguientes parámetros:
- En el área de **Tamaño de Log**, existen los siguientes campos:
  - ✓ Tamaño Mínimo del Registro**: 512 MB para Servidores y Equipos Cliente.**
  - ✓ Tamaño Máximo del Registro**: 10 GB para Servidores y 4 GB para Equipos Cliente.**
  - ✓ Cuando se alcance el tamaño máximo del registro de eventos**: Sobrescribir eventos**