CONTROLES

1. Falta de cifrado de datos sensibles

Control seleccionado:

- **Cifrado de datos en tránsito y en reposo**:
  - **Norma aplicable**: ISO/IEC 27001, Anexo A.10.1 (Cifrado de la Información).
  - **Descripción**: Implementar cifrado fuerte (AES-256) para proteger la confidencialidad de los datos tanto en tránsito (mediante TLS) como en reposo (mediante soluciones como **VeraCrypt** o cifrado nativo de bases de datos).
  - **NIST SP 800-53**: Control SC-13 (Uso de cifrado en la protección de datos).

Roles y responsabilidades:

- **Equipo de IT**: Implementar y gestionar las soluciones de cifrado.
- **Personal de seguridad**: Monitorear el cumplimiento del cifrado y realizar auditorías periódicas para asegurar que esté activo.

Plan de implementación:

- **Cronograma**:
  - Implementación en el plazo de 3 meses para datos en reposo y 1 mes para datos en tránsito.
- **Recursos necesarios**: Licencias para soluciones de cifrado (por ejemplo, VeraCrypt para datos locales), capacitación del personal técnico.
- **Dependencias**: Actualización de políticas de seguridad para asegurar que todo almacenamiento nuevo o intercambio de información sensible esté protegido por cifrado.

2. Contraseñas débiles o falta de autenticación multifactor (MFA)

Control seleccionado:

- **Política de autenticación robusta**:
  - **Norma aplicable**: ISO/IEC 27001, Anexo A.9.2 (Control de Acceso).

- **Descripción**: Implementar políticas de contraseñas fuertes (mínimo de 12 caracteres, mezcla de mayúsculas, minúsculas, números y símbolos), y habilitar la **autenticación multifactor (MFA)** para todas las cuentas que accedan a datos sensibles o servicios críticos como Microsoft 365 y Google Workspace.
- **NIST SP 800-63B**: Recomendación para autenticación digital, que incluye el uso de MFA y políticas de contraseñas fuertes.

Roles y responsabilidades:

- **Administradores de sistemas**: Configurar y gestionar el uso de MFA en las plataformas clave.
- **Usuarios finales**: Cumplir con las políticas de contraseñas y usar MFA en cada inicio de sesión.

Plan de implementación:

- **Cronograma**:
  - Implementación en 2 meses.
  - Primera fase: Habilitar MFA en Microsoft 365 y Google Workspace.
  - Segunda fase: Políticas de contraseñas para todos los sistemas críticos.
- **Recursos necesarios**: Licencias para servicios de autenticación (como Microsoft Azure MFA), capacitaciones breves para el personal.
- **Dependencias**: Capacitación y concientización del personal para asegurar una transición fluida a MFA.

3. Sistemas desactualizados o sin parches de seguridad

Control seleccionado:

- **Gestión de parches y actualizaciones automáticas**:
  - **Norma aplicable**: ISO/IEC 27001, Anexo A.12.6 (Gestión de Vulnerabilidades Técnicas).
  - **Descripción**: Implementar un programa de actualización de software y parches de seguridad automatizado en todos los sistemas (Windows 11, servidores, routers, switches) para reducir el riesgo de vulnerabilidades conocidas.
  - **NIST SP 800-53**: Control SI-2 (Gestión de actualizaciones y parches de software).

Roles y responsabilidades:

- **Equipo de IT**: Configurar actualizaciones automáticas y realizar auditorías periódicas para verificar la implementación correcta.
- **Personal de seguridad**: Monitorear posibles vulnerabilidades no cubiertas por actualizaciones automáticas y escalarlas.

Plan de implementación:

- **Cronograma**: Implementación dentro de 1 mes, con revisiones mensuales para verificar que las actualizaciones se estén aplicando.

- **Recursos necesarios**: Software de gestión de parches (por ejemplo, **WSUS** para servidores Windows), personal de IT dedicado a supervisar actualizaciones.
- **Dependencias**: Inventario actualizado de todo el software y hardware que requiera gestión de parches.

4. Falta de segmentación de red

Control seleccionado:

- **Segmentación de red y control de acceso basado en roles (RBAC)**:
  - **Norma aplicable**: ISO/IEC 27001, Anexo A.13.1 (Seguridad en las Redes).
  - **Descripción**: Implementar la segmentación de la red con VLANs y control de acceso basado en roles para separar áreas críticas (servidores, almacenamiento de datos sensibles) de las redes públicas y de empleados generales. Además, aplicar control de acceso restringido basado en roles para asegurar que solo personal autorizado acceda a sistemas críticos.
  - **CIS Controls v8**: Control 12 (Defensas en la red).

Roles y responsabilidades:

- **Equipo de redes**: Configurar la segmentación de la red, crear VLANs y gestionar reglas de acceso.
- **Personal de IT**: Revisar y actualizar las políticas de acceso basado en roles.

Plan de implementación:

- **Cronograma**: Segmentación completa de la red en un plazo de 2 meses.
- **Recursos necesarios**: Capacitación para el personal de redes en configuración de VLANs, equipo de red compatible.
- **Dependencias**: Inventario de dispositivos en la red y auditoría inicial para determinar áreas críticas a segmentar.

5. Mal uso o configuración incorrecta de herramientas de seguridad

Control seleccionado:

- **Revisión y auditoría de la configuración de seguridad**:
  - **Norma aplicable**: ISO/IEC 27001, Anexo A.18.2 (Cumplimiento técnico de seguridad).
  - **Descripción**: Realizar auditorías técnicas periódicas para asegurar que herramientas como Fortinet, VeraCrypt, Wazuh y Wireshark estén configuradas correctamente según las mejores prácticas de seguridad. Además, implementar sistemas de detección y prevención de intrusiones (IDS/IPS) para identificar configuraciones incorrectas en tiempo real.
  - **NIST SP 800-53**: Control CA-7 (Monitoreo continuo y revisión).

Roles y responsabilidades:

- **Equipo de seguridad de la información**: Realizar las auditorías técnicas y revisar configuraciones de seguridad.
- **Auditor interno**: Coordinar las revisiones periódicas de cumplimiento con las políticas y normativas internas.

Plan de implementación:

- **Cronograma**: Auditoría inicial en 3 meses, con revisiones trimestrales.
- **Recursos necesarios**: Software de monitoreo y auditoría (por ejemplo, **Wazuh** ya implementado), capacitación para el equipo de IT en revisiones de configuración.
- **Dependencias**: Documentación y políticas claras de configuración de seguridad que deban cumplirse.