Reto# 2

Roberto Blanco

Definición de Objetivos de Ciberseguridad

1. Garantizar la protección física y lógica de los activos de TI
2. Asegurar la disponibilidad de los equipos críticos para funciones académicas y administrativas
3. Proteger la integridad de la información procesada y almacenada en los dispositivos
4. Definir responsables de la seguridad de cada activo
5. Monitorear y gestionar el estado de los activos tecnológicos
6. Implementar medidas de respaldo y recuperación ante pérdida de equipo o daño físico

Desarrollo de la Estrategia Integral

1. Reducir el puntaje de riesgo del equipo Dell Optiplex 3080 (Sala de Sistemas - Bloque I) a menos de 30/100 en los próximos 4 meses

    - Indicadores de cumplimiento: Evaluación de riesgos técnica usando una herramienta de análisis (ej. NIST SP 800-30 o herramienta institucional).
    - Actividades: Actualización de sistema operativo, instalación de antivirus corporativo, configuración de firewall local, revisión de permisos.
    - Responsable: Ing. Juan Pérez

2. Implementar autenticación multifactor (MFA) en todas las cuentas institucionales de correo y sistemas académicos antes de 90 días

    - **Indicadores de cumplimiento:** 100% de cuentas docentes y administrativas protegidas con MFA.
    - **Actividades:** Configuración de MFA en correo institucional, capacitación rápida para usuarios, verificación por el equipo de TI.
    - **Responsable:** Dirección de Tecnología / Área de Seguridad Informática

3. Realizar respaldo semanal automatizado en los equipos portátiles y de escritorio usados para fines administrativos
    - **Plazo:** En 60 días, tener en marcha un sistema de respaldo automatizado para:
        - Dell Optiplex 3080
        - Laptop Lenovo ThinkPad L14
    - **Indicadores de cumplimiento:** Existencia de historial de respaldos verificados.
    - **Responsable:** Ing. Juan Pérez / Ing. Carlos Díaz

4. Realizar evaluación de vulnerabilidades trimestral en todos los equipos institucionales de uso crítico

    - **Plazo:** Primera evaluación en el próximo trimestre, luego cada 3 meses.
    - **Objetivo:** Identificar y corregir vulnerabilidades en SO, software de impresión (Epson L3150), y redes conectadas.
    - **Responsables:** Área de TI / Auditoría Interna

5. Usar un sistema de inventario actualizado con:

    - Estado de funcionamiento
    - Ubicación física
    - Historial de mantenimiento y observaciones (como "requiere mantenimiento" en la impresora)

6. Garantizar que los dispositivos, especialmente laptops y CPUs, estén configurados con:

    - Copias de seguridad periódicas
    - Cifrado de disco
    - Software de localización o borrado remoto (cuando sea posible)

Roadmap de Implementación

Horizonte temporal: 6 meses (junio – noviembre 2025)

✓ Fase 1: Planificación y Evaluación (Junio 2025)

Actividad	Objetivo	Responsable	Fecha objetivo
Identificación y clasificación de activos críticos	Tener un inventario validado y priorizado	Área de TI / Responsables de cada área	15 junio 2025
Evaluación inicial de riesgos (puntaje de riesgo de cada equipo)	Medir exposición actual de equipos clave	Área de Seguridad Informática	25 junio 2025
Selección de herramientas para respaldos y MFA	Establecer tecnologías compatibles	Dirección de Tecnología	30 junio 2025

- ✓ Fase 2: Implementación Técnica Inicial (Julio – Agosto 2025)

Actividad	Objetivo	Responsable	Fecha objetivo
Instalación de antivirus, firewall local y actualizaciones en CPU Dell y Laptop Lenovo	Reducir el puntaje de riesgo a < 30/100	Ing. Juan Pérez / Ing. Carlos Díaz	20 julio 2025
Implementación de sistema de respaldo automático	Garantizar recuperación de datos en caso de fallo	Área de TI	31 julio 2025
Implementación de MFA en cuentas institucionales críticas	Fortalecer autenticación	Área de Seguridad Informática	15 agosto 2025
Capacitación básica en ciberseguridad (1ra ronda)	Sensibilizar a docentes y personal administrativo	Departamento de Formación / TI	30 agosto 2025

- ✓ Fase 3: Verificación y Monitoreo (Septiembre – Octubre 2025)

Actividad	Objetivo	Responsable	Fecha objetivo
Auditoría interna de configuración de seguridad	Validar cumplimiento de medidas técnicas	Auditoría Interna	15 septiembre 2025
Revisión de respaldos automáticos y restauración de prueba	Verificar integridad de los respaldos	Área de TI	30 septiembre 2025
Primera evaluación trimestral de vulnerabilidades	Identificar nuevas debilidades	Seguridad Informática / Externos si aplica	10 octubre 2025

- ✓ Fase 4: Ajustes, Documentación y Reporte Final (Noviembre 2025)

Actividad	Objetivo	Responsable	Fecha objetivo
Ajustes post-auditoría y refuerzo de controles	Corregir hallazgos	Dirección de Tecnología / TI	5 noviembre 2025
Documentación de políticas, procedimientos y resultados	Formalizar procesos y reportes	Responsable de Seguridad / Rectoría	20 noviembre 2025
Presentación de resultados y recomendaciones	Mostrar impacto de la implementación	Comité de Seguridad / Rectorado	30 noviembre 2025

Resultados esperados al finalizar el roadmap:

- Reducción de riesgos tecnológicos en equipos críticos.
- Respaldo automático funcional.
- MFA implementado en cuentas clave.
- Evaluación de vulnerabilidades institucionalizada.
- Conciencia de ciberseguridad mejorada entre usuarios.
- Base sólida para futuras certificaciones o auditorías externas.