Selección de Controles de Seguridad para la Universidad de California

1. Revisión de Normas Relevantes

La selección de controles se basa en marcos de referencia ampliamente aceptados en la industria que ofrecen directrices específicas para la protección de información sensible y la mitigación de riesgos:

- **ISO/IEC 27001:**
  Este estándar internacional establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Proporciona un enfoque sistemático para gestionar los riesgos de seguridad de la información mediante controles organizativos, técnicos y físicos. Es particularmente relevante para la UC por su enfoque integral en la gestión de riesgos y el cumplimiento normativo.
- **NIST SP 800-53:**
  Este marco, desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, ofrece un conjunto de controles de seguridad y privacidad que son altamente detallados. Entre las categorías clave están la protección contra amenazas cibernéticas, la gestión de accesos y la respuesta ante incidentes. Es adecuado para sistemas de información con altos requisitos de seguridad, como los utilizados en universidades.
- **CIS Controls:**
  Una lista priorizada de acciones prácticas divididas en 18 controles fundamentales. Los controles incluyen gestión de inventario, análisis continuo de vulnerabilidades y monitoreo de actividades. Este marco es especialmente útil para identificar acciones de rápida implementación que mejoran significativamente la postura de seguridad de una organización.
- **Regulaciones sectoriales específicas:**
  - **FERPA:** Protege la privacidad de los registros educativos de los estudiantes y establece requisitos específicos sobre el acceso y manejo de esta información.
  - **HIPAA:** Garantiza la seguridad de los datos de salud, aplicable a centros médicos y sistemas de investigación médica en la UC.

2. Controles de Seguridad Seleccionados

La selección de controles se enfoca en abordar los riesgos críticos identificados mediante una combinación de controles técnicos, administrativos y físicos:

Técnicos:

- **Autenticación Multifactor (MFA):**
  - **Objetivo:** Prevenir accesos no autorizados a sistemas críticos mediante la exigencia de múltiples factores de autenticación, como contraseñas y tokens.
  - **Implementación:** Integración de herramientas MFA en sistemas administrativos, académicos y de investigación.
  - **Ventajas:** Mitiga significativamente el riesgo de acceso no autorizado, incluso si las contraseñas son comprometidas.
- **Actualizaciones automatizadas:**
  - **Objetivo:** Garantizar que los sistemas operativos y aplicaciones estén protegidos contra vulnerabilidades conocidas mediante la instalación automática de parches de seguridad.
  - **Implementación:** Configuración de servidores y estaciones de trabajo para ejecutar actualizaciones fuera de horario laboral para minimizar interrupciones.
  - **Ventajas:** Reduce la exposición a ataques de día cero y exploits conocidos.
- **Sistemas de detección de intrusiones (IDS):**
  - **Objetivo:** Identificar actividades anómalas en tiempo real y alertar sobre posibles ataques.
  - **Implementación:** Implementación en redes internas y puntos de acceso externos.
  - **Ventajas:** Proporciona visibilidad y capacidad de respuesta ante amenazas emergentes.

Administrativos:

- **Política de contraseñas robustas:**
  - **Objetivo:** Asegurar que las contraseñas utilizadas sean seguras y cambien periódicamente.
  - **Implementación:** Configuración de requisitos mínimos de longitud y complejidad en el sistema de gestión de credenciales.
  - **Ventajas:** Reduce el riesgo de accesos no autorizados debido a contraseñas débiles.
- **Capacitación periódica:**
  - **Objetivo:** Educar al personal y estudiantes sobre mejores prácticas en ciberseguridad.
  - **Implementación:** Talleres trimestrales sobre detección de phishing, uso seguro de redes y políticas internas.
  - **Ventajas:** Disminuye la probabilidad de errores humanos y fomenta una cultura de seguridad.

Físicos:

- **Control de acceso a instalaciones críticas:**
  - **Objetivo:** Proteger centros de datos, laboratorios y oficinas administrativas sensibles.
  - **Implementación:** Uso de tarjetas de identificación con autenticación biométrica para áreas restringidas.
  - **Ventajas:** Minimiza el riesgo de acceso físico no autorizado.
- **Sistemas de videovigilancia:**
  - **Objetivo:** Monitorear áreas clave para disuadir robos o accesos no autorizados.
  - **Implementación:** Instalación de cámaras con almacenamiento en servidores seguros y revisiones periódicas.
  - **Ventajas:** Aumenta la capacidad de respuesta ante incidentes físicos.

3. Documentación de la Implementación

Para cada control, se especifican los pasos de implementación, roles responsables y métricas para evaluar su eficacia:

Control Seleccionado	Pasos de Implementación	Responsable	Métrica de Éxito
Autenticación multifactor	Configurar herramientas MFA en sistemas clave, capacitar usuarios y monitorear actividad.	Equipo de TI	100% de sistemas críticos con MFA habilitado.
Actualizaciones automatizadas	Activar políticas de actualizaciones automáticas en estaciones y servidores, revisar logs mensualmente.	Equipo de TI	90% de sistemas actualizados en tiempo real.
Política de contraseñas robustas	Definir políticas en el sistema, comunicar requisitos a usuarios y realizar auditorías periódicas.	Administradores de sistemas	Reducción de incidentes relacionados con credenciales.
Capacitaciones periódicas	Diseñar contenido de talleres, realizar sesiones prácticas y medir conocimiento adquirido mediante encuestas.	Recursos Humanos y TI	80% de participantes superan evaluaciones.
Control de acceso físico	Instalar cerraduras electrónicas, configurar autenticación biométrica y realizar auditorías de acceso.	Administradores de campus	Incidentes físicos reportados reducidos a cero.

4. Planificación de la Implementación

Un plan detallado garantiza que los controles se implementen dentro de los plazos y recursos disponibles. A continuación, se describen las actividades principales:

- **Autenticación Multifactor:**
  - **Duración:** 2 meses.
  - **Requerimientos:** Tokens de seguridad, capacitación del personal.
  - **Actividades:** Configuración inicial, pruebas en entornos controlados, implementación masiva.
- **Actualizaciones Automatizadas:**
  - **Duración:** 1 mes.
  - **Requerimientos:** Software de gestión de actualizaciones.
  - **Actividades:** Instalación de sistemas automatizados, revisión de compatibilidad, monitoreo continuo.
- **Capacitaciones en Seguridad:**
  - **Duración:** 2 semanas por taller.
  - **Requerimientos:** Material educativo, presupuesto para facilitadores.
  - **Actividades:** Desarrollo de contenido, ejecución de talleres, evaluación post-taller.

Conclusión

La selección y planificación de estos controles permiten mitigar riesgos críticos en el Sistema de la Universidad de California. Este enfoque integrado asegura la protección de activos clave, fomenta una cultura de seguridad y garantiza la continuidad operativa frente a amenazas crecientes.