Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Los Controles Físicos en los Sistemas de Información

Presentación del tema

Los controles físicos constituyen una dimensión esencial dentro de la gestión integral de seguridad en los Sistemas de Información (SI), especialmente en organizaciones que dependen críticamente de infraestructuras tecnológicas para sostener sus operaciones. Mientras que los controles técnicos y los controles administrativos suelen recibir mayor atención académica, los controles físicos representan la primera línea de defensa para proteger los componentes tangibles del ecosistema tecnológico.

Un sistema de información está compuesto por múltiples elementos físicos: servidores, estaciones de trabajo, dispositivos de red, centros de datos, cableado estructurado, sistemas de energía y dispositivos móviles. La integridad, disponibilidad y confidencialidad de la información —los tres pilares del modelo CIA— dependen, en gran medida, de la adecuada protección física de estos activos. Las amenazas materiales —incendios, robos, sabotaje, fallas eléctricas o acceso no autorizado a instalaciones— pueden comprometer de manera inmediata la continuidad del negocio y generar impactos financieros, legales y reputacionales significativos.

Clasificación de los controles físicos

Controles preventivos. Buscan evitar incidentes antes de que ocurran: cerraduras electrónicas, control de acceso biométrico, tarjetas inteligentes (Smart Cards), seguridad perimetral, barreras físicas y guardias de seguridad. En centros de datos críticos es habitual combinar tarjeta de proximidad y biometría.

Controles detectivos. Permiten identificar incidentes en curso o posteriores: cámaras de videovigilancia (CCTV), sensores de movimiento, alarmas de intrusión, registros de acceso físico y sistemas de monitoreo ambiental. Son fundamentales para auditorías y análisis forense.

Controles correctivos. Reducen el impacto tras un incidente: sistemas de extinción automática de incendios con gas inerte, generadores eléctricos de respaldo, sistemas UPS (Uninterruptible Power Supply), planes de recuperación ante desastres (DRP) y procedimientos de restauración.

Protección del centro de datos

El centro de datos es el núcleo físico del sistema de información. Sus controles incluyen control estricto de acceso, sistemas antiincendios, piso técnico elevado, redundancia eléctrica, climatización controlada y segmentación de zonas de seguridad. El nivel de redundancia suele clasificarse según estándares internacionales: a mayor nivel, mayor disponibilidad garantizada, lo que implica mayor inversión.

La seguridad ambiental considera riesgos como incendios, inundaciones, terremotos y variaciones de temperatura. Su mitigación incluye detectores de humo, sistemas de drenaje, ubicación geográfica estratégica y monitoreo climático continuo. Un administrador debe evaluar el costo de implementación frente al costo potencial de interrupción operativa.

Protección de dispositivos finales e infraestructura de comunicaciones

Las estaciones de trabajo y dispositivos móviles requieren controles específicos: bloqueo automático de pantalla, anclajes físicos, políticas de escritorio limpio (Clean Desk Policy) y protección de puertos USB. La pérdida física de una laptop sin cifrado puede representar una vulnerabilidad crítica.

El cableado estructurado y los racks de comunicaciones deben estar en áreas restringidas, con cerraduras y etiquetado adecuado. La manipulación física de un switch puede habilitar ataques de red internos.

Dimensión estratégica y financiera

Desde la administración, los controles físicos deben analizarse bajo criterios de costo-beneficio, retorno sobre la inversión en seguridad (ROSI), cumplimiento normativo y

continuidad del negocio. No todos los activos requieren el mismo nivel de protección: el principio de proporcionalidad es esencial. Normas como ISO/IEC 27001 e ISO/IEC 27002 incluyen secciones específicas sobre seguridad física y ambiental.

Conceptos clave

- Controles físicos preventivos, detectivos y correctivos como tres categorías complementarias.
- Centro de datos como núcleo físico crítico que requiere protección integral.
- Seguridad ambiental como mitigación de amenazas naturales y eléctricas.
- UPS y generadores como controles correctivos de continuidad eléctrica.
- Principio de proporcionalidad entre nivel de protección y criticidad del activo.
- Integración con controles técnicos y administrativos.

Preguntas de repaso del tema

1. ¿Cuál es la diferencia entre controles físicos preventivos, detectivos y correctivos?
2. ¿Por qué la protección del centro de datos es estratégica para la continuidad del negocio?
3. ¿Cómo se integran los controles físicos con los controles técnicos en un sistema de información?
4. ¿Qué riesgos surgen cuando no se protegen adecuadamente los dispositivos finales?
5. ¿Cómo puede un administrador justificar financieramente la inversión en controles físicos?
6. ¿Por qué los controles físicos son la primera línea de defensa en la seguridad informática?

7. ¿Qué función cumplen los sistemas UPS en la continuidad operativa?
8. ¿Cómo impacta la ubicación geográfica de un centro de datos en la gestión de riesgos físicos?
9. ¿Por qué la Clean Desk Policy es un control físico relevante?
10. ¿Qué estándares internacionales regulan la seguridad física en sistemas de información?