Universidad de Buenos Aires
Facultad de Ciencias Económicas

Controles Físicos

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

Presentación del Tema

Los **controles físicos** constituyen una dimensión esencial dentro de la gestión integral de seguridad en los **Sistemas de Información (SI – *Information Systems*)**, especialmente en organizaciones que dependen críticamente de infraestructuras tecnológicas para sostener sus operaciones. Mientras que los controles técnicos (como firewalls o cifrado) y los controles administrativos (políticas y procedimientos) 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, dispositivos de almacenamiento, sistemas de energía, equipos de telecomunicaciones y dispositivos móviles. La integridad, disponibilidad y confidencialidad de la información —los tres pilares clásicos del modelo **CIA (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad)**— dependen, en gran medida, de la adecuada protección física de estos activos.

Para estudiantes de licenciatura en administración, comprender los controles físicos implica reconocer que la seguridad informática no es exclusivamente digital. 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.

Desarrollo

1. Naturaleza y Objetivos de los Controles Físicos

Los **controles físicos (Physical Controls)** son mecanismos diseñados para prevenir, detectar o mitigar daños a los activos tecnológicos mediante la protección del entorno físico donde estos operan.

Sus objetivos principales son:

1. Prevenir el acceso físico no autorizado.
2. Proteger los equipos contra daños ambientales.
3. Garantizar la continuidad operativa.
4. Reducir la probabilidad de sabotaje o robo.
5. Minimizar el impacto de desastres naturales o accidentes.

Desde una perspectiva administrativa, estos controles forman parte del sistema integral de **Gestión de Riesgos (Risk Management / Gestión del Riesgo)** y deben alinearse con la estrategia organizacional.

---

2. Componentes Físicos de un Sistema de Información

Un sistema de información moderno incluye:

- Centros de datos (Data Centers).
- Servidores físicos.
- Equipos de almacenamiento (Storage Systems).
- Dispositivos de red (Routers, Switches).
- Estaciones de trabajo.
- Dispositivos móviles corporativos.
- Sistemas de energía y climatización.

- Infraestructura de telecomunicaciones.

Cada uno de estos componentes requiere controles físicos específicos según su criticidad y exposición al riesgo.

---

3. Clasificación de Controles Físicos

Los controles físicos pueden clasificarse en tres categorías principales:

3.1 Controles Preventivos

Buscan evitar incidentes antes de que ocurran.

Ejemplos:

- Cerraduras electrónicas.
- Control de acceso biométrico.
- Tarjetas inteligentes (Smart Cards).
- Seguridad perimetral.
- Barreras físicas.
- Guardias de seguridad.

En centros de datos críticos, es habitual implementar sistemas de autenticación multifactor que combinen tarjeta de proximidad y biometría.

3.2 Controles Detectivos

Permiten identificar incidentes en curso o posteriores.

Ejemplos:

- Cámaras de videovigilancia (CCTV – *Closed-Circuit Television* / Circuito Cerrado de Televisión).
- Sensores de movimiento.
- Alarmas de intrusión.
- Registros de acceso físico.
- Sistemas de monitoreo ambiental.

Estos controles son fundamentales para auditorías y análisis forense.

3.3 Controles Correctivos

Reducen el impacto tras un incidente.

Ejemplos:

- Sistemas de extinción automática de incendios.
- Generadores eléctricos de respaldo.
- Sistemas UPS (*Uninterruptible Power Supply* / Sistema de Alimentación Ininterrumpida).
- Planes de recuperación ante desastres (DRP – *Disaster Recovery Plan* / Plan de Recuperación ante Desastres).

La presencia de UPS y generadores reduce el riesgo de pérdida de datos por cortes eléctricos.

---

4. Protección del Centro de Datos

El centro de datos es el núcleo físico del sistema de información.

Controles típicos incluyen:

- Control estricto de acceso.
- Sistemas antiincendios con gas inerte.
- Piso técnico elevado.
- Redundancia eléctrica.
- Climatización controlada.
- Segmentación de zonas de seguridad.

La clasificación por niveles de redundancia suele basarse en estándares como los **Tier Levels** definidos por el Uptime Institute.

Desde la administración, la inversión en infraestructura Tier III o Tier IV debe justificarse en función del impacto financiero de la interrupción del servicio.

---

5. Seguridad Ambiental

Los riesgos ambientales incluyen:

- Incendios.
- Inundaciones.
- Terremotos.
- Variaciones de temperatura.
- Humedad excesiva.

La mitigación implica:

- Detectores de humo.
- Sistemas de drenaje.
- Ubicación geográfica estratégica.
- Monitoreo climático continuo.

Un administrador debe evaluar el costo de implementación frente al costo potencial de interrupción operativa.

---

6. Protección de Dispositivos Finales

Las estaciones de trabajo y dispositivos móviles también requieren controles físicos:

- Bloqueo automático de pantalla.
- Anclajes físicos (Kensington locks).
- Políticas de escritorio limpio (Clean Desk Policy).
- Protección de puertos USB.

La pérdida física de una laptop sin cifrado puede representar una vulnerabilidad crítica.

---

7. Seguridad en Infraestructura de Telecomunicaciones

El cableado estructurado y los racks de comunicaciones deben:

- Estar en áreas restringidas.
- Contar con cerraduras.
- Tener etiquetado adecuado.

- Evitar exposición pública.

La manipulación física de un switch puede permitir ataques de red internos.

---

8. Integración con Controles Técnicos y Administrativos

Los controles físicos no funcionan de manera aislada.

Ejemplo:

- El acceso físico debe integrarse con el control lógico de usuarios.
- El registro de acceso físico debe correlacionarse con registros digitales.

Sistemas como SIEM (*Security Information and Event Management* / Gestión de Eventos e Información de Seguridad) pueden integrar información física y lógica.

---

9. Evaluación del Riesgo Físico

El análisis de riesgo físico debe considerar:

- Probabilidad de ocurrencia.
- Impacto financiero.
- Tiempo de recuperación.
- Dependencia operativa.

La **exposición al riesgo** disminuye cuando se implementan controles proporcionales al nivel de amenaza.

---

10. Dimensión Estratégica y Financiera

Desde la administración, los controles físicos deben analizarse bajo criterios de:

- Costo-beneficio.
- Retorno de la inversión en seguridad (ROSI – *Return on Security Investment* / Retorno sobre la Inversión en Seguridad).
- Cumplimiento normativo.
- Continuidad del negocio (BCP – *Business Continuity Plan* / Plan de Continuidad del Negocio).

No todos los activos requieren el mismo nivel de protección; el principio de proporcionalidad es esencial.

---

11. Ejemplo Aplicado

Supongamos una empresa financiera que aloja sus servidores en una oficina común sin control de acceso.

Amenaza: robo físico.

Vulnerabilidad: acceso libre al área de servidores.

Impacto: pérdida de datos críticos.

Solución: implementar sala cerrada, control biométrico y monitoreo CCTV.

El riesgo disminuye significativamente mediante controles físicos básicos.

---

12. Gobernanza y Normativas

Normas internacionales como:

- ISO/IEC 27001.
- ISO/IEC 27002.

incluyen secciones específicas sobre seguridad física y ambiental.

El cumplimiento normativo fortalece la estructura de control organizacional.

Conclusión

Los controles físicos de los componentes de un sistema de información constituyen una dimensión estratégica de la seguridad organizacional. Protegen la infraestructura tangible que sostiene los procesos digitales y garantizan la continuidad operativa frente a amenazas materiales.

Desde la perspectiva administrativa, estos controles deben integrarse dentro del modelo global de gestión de riesgos, equilibrando inversión, criticidad de activos y exposición al riesgo. La protección física adecuada reduce vulnerabilidades, fortalece la resiliencia organizacional y preserva el valor de la información como activo estratégico.

En entornos altamente digitalizados, la seguridad no puede limitarse a lo lógico o virtual: la protección física sigue siendo la base estructural sobre la cual se sostiene todo sistema de información.

Preguntas de autoevaluación

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?

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.