Universidad de Buenos Aires
Facultad de Ciencias Económicas

El Control Biométrico de las Personas en los Sistemas de Información

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 de las personas en los Sistemas de Información (SI – *Information Systems*)** constituyen una dimensión crítica dentro del modelo integral de seguridad organizacional. Aunque la tecnología suele ser el foco principal de la ciberseguridad, la evidencia empírica demuestra que el factor humano continúa siendo una de las principales fuentes de riesgo. En consecuencia, los mecanismos de control orientados a regular, autenticar, supervisar y auditar la interacción de las personas con los sistemas digitales resultan esenciales para preservar la confidencialidad, integridad y disponibilidad de la información.

Los controles vinculados a las personas abarcan tanto mecanismos tecnológicos —como la **biometría (Biometrics)**— como políticas administrativas, segregación de funciones, controles de acceso basados en roles y programas de concientización. Estos controles buscan mitigar riesgos asociados a error humano, abuso de privilegios, fraude interno, ingeniería social y negligencia operativa.

Para estudiantes de licenciatura en administración, el análisis de los controles humanos en TI implica comprender que la seguridad no depende exclusivamente de dispositivos o software, sino de la interacción entre tecnología, procesos y comportamiento organizacional. La gestión efectiva del capital humano digital es, por tanto, una cuestión estratégica y no meramente operativa.

Desarrollo

1. El Factor Humano como Variable de Riesgo

Diversos estudios en ciberseguridad muestran que una proporción significativa de incidentes se origina en:

- Errores de usuario.
- Configuraciones incorrectas.
- Compartición indebida de credenciales.
- Phishing (suplantación de identidad).
- Abuso de privilegios internos.

En términos de gestión de riesgos, el empleado puede representar simultáneamente:

- Un activo estratégico.
- Una vulnerabilidad potencial.
- Un agente de mitigación del riesgo.

La ecuación del riesgo (Amenaza × Vulnerabilidad × Impacto) se ve directamente influida por la conducta humana. Si los empleados no reciben capacitación adecuada, la vulnerabilidad organizacional aumenta, incluso ante amenazas relativamente simples.

---

2. Clasificación de los Controles de Personas

Los controles asociados a las personas pueden agruparse en tres grandes categorías:

1. Controles de Identificación y Autenticación.
2. Controles de Autorización y Privilegios.
3. Controles de Supervisión y Cultura Organizacional.

---

3. Identificación y Autenticación

La **identificación (Identification)** implica que el usuario declara quién es; la **autenticación (Authentication)** consiste en verificar esa identidad.

Los mecanismos clásicos de autenticación se basan en tres factores:

1. Algo que el usuario sabe (contraseña).
2. Algo que el usuario tiene (token físico).
3. Algo que el usuario es (biometría).

3.1 Autenticación Multifactor (MFA – Multi-Factor Authentication / Autenticación Multifactor)

La MFA combina al menos dos de los factores mencionados. Por ejemplo:

- Contraseña + código enviado al teléfono.
- Tarjeta inteligente + huella digital.

Desde la administración, la implementación de MFA reduce significativamente la probabilidad de acceso no autorizado y disminuye la exposición al riesgo.

---

4. Biometría en Sistemas de Información

La **biometría (Biometrics)** se refiere al uso de características físicas o conductuales únicas para autenticar a un individuo.

Tipos comunes de biometría:

- Huella dactilar (Fingerprint Recognition).
- Reconocimiento facial (Facial Recognition).
- Escaneo de iris (Iris Scan).
- Reconocimiento de voz (Voice Recognition).
- Dinámica de escritura (Keystroke Dynamics).

Ventajas:

- Mayor seguridad frente al robo de contraseñas.
- Dificultad de suplantación.
- Eliminación de contraseñas débiles.

Riesgos:

- Problemas de privacidad.
- Almacenamiento indebido de datos biométricos.
- Falsos positivos o negativos.

Desde la perspectiva administrativa, la biometría requiere análisis de costo-beneficio y evaluación legal, especialmente en relación con normativas de protección de datos personales.

---

5. Control de Acceso Basado en Roles

El **RBAC (Role-Based Access Control / Control de Acceso Basado en Roles)** es un modelo que asigna permisos según el rol organizacional del usuario.

Ejemplo:

- El área de contabilidad accede a módulos financieros.
- El área comercial accede a CRM.
- El área técnica accede a configuraciones del sistema.

El RBAC reduce el riesgo de abuso de privilegios al limitar el acceso según funciones específicas.

---

6. Principio de Mínimo Privilegio

El **Principio de Mínimo Privilegio (Least Privilege Principle)** establece que cada usuario debe tener únicamente los permisos estrictamente necesarios para realizar su tarea.

Si un empleado posee privilegios excesivos:

- Aumenta la superficie de ataque.
- Incrementa la probabilidad de fraude interno.

- Se amplifica el impacto potencial de un error.

Este principio es central en entornos de sistemas ERP (Enterprise Resource Planning) y bases de datos críticas.

---

7. Segregación de Funciones

La **Segregación de Funciones (SoD – Segregation of Duties / Separación de Funciones)** busca evitar que una sola persona controle múltiples etapas críticas de un proceso.

Ejemplo financiero:

- Un usuario carga facturas.
- Otro usuario autoriza pagos.

En TI:

- Un administrador configura el sistema.
- Otro audita las configuraciones.

Este mecanismo reduce riesgos de fraude y errores intencionales.

---

8. Monitoreo y Auditoría

Los controles humanos deben complementarse con monitoreo constante:

- Logs de acceso.
- Registro de actividades.
- Sistemas SIEM (Security Information and Event Management / Gestión de Eventos de Seguridad).

El monitoreo no implica desconfianza, sino gobernanza responsable.

---

9. Capacitación y Concientización

La tecnología no reemplaza la formación.

Los programas de **Security Awareness (Concientización en Seguridad)** buscan:

- Reducir el impacto de phishing.

- Fomentar buenas prácticas.
- Promover cultura de reporte de incidentes.

Una organización que no capacita a su personal incrementa exponencialmente su vulnerabilidad.

---

10. Controles en el Ciclo de Vida del Empleado

Los controles deben aplicarse en todo el ciclo laboral:

1. Ingreso: verificación de antecedentes.
2. Permanencia: revisiones periódicas de accesos.
3. Desvinculación: revocación inmediata de credenciales.

Errores frecuentes incluyen mantener cuentas activas de ex empleados.

---

11. Riesgos Asociados al Teletrabajo

La expansión del trabajo remoto introduce nuevos desafíos:

- Uso de dispositivos personales.
- Redes domésticas inseguras.
- Mayor exposición a ataques de ingeniería social.

Controles recomendados:

- VPN (Virtual Private Network / Red Privada Virtual).
- Autenticación multifactor.
- Políticas de dispositivos gestionados.

---

12. Dimensión Ética y Legal

El uso de biometría y monitoreo plantea interrogantes:

- ¿Hasta qué punto puede supervisarse a un empleado?
- ¿Cómo se protegen los datos biométricos?

El equilibrio entre seguridad y privacidad es un desafío central para la administración moderna.

---

13. Ejemplo Aplicado

Supongamos una empresa donde:

- Todos los empleados comparten una contraseña común.
- No existe segregación de funciones.
- No se registran accesos.

Amenaza: fraude interno.

Vulnerabilidad: ausencia de controles humanos.

Impacto: pérdida financiera significativa.

La implementación de RBAC, MFA y auditoría reduce considerablemente el riesgo.

---

14. Integración Estratégica

Los controles de personas deben integrarse con:

- Controles técnicos.
- Controles físicos.
- Políticas administrativas.

Un enfoque fragmentado resulta ineficiente.

Conclusión

Los controles de las personas en los sistemas de información constituyen un pilar fundamental de la seguridad organizacional. La biometría, la autenticación multifactor, el control de acceso basado en roles, la segregación de funciones y la capacitación continua son herramientas esenciales para reducir la exposición al riesgo derivado del factor humano.

Desde la perspectiva administrativa, estos controles no deben concebirse como simples medidas técnicas, sino como instrumentos de gobernanza estratégica que alinean comportamiento organizacional, cumplimiento normativo y preservación del valor de la información. La gestión adecuada del factor humano digital es, en definitiva, una condición indispensable para la sostenibilidad y competitividad en entornos tecnológicos complejos.

Preguntas de autoevaluación

1. ¿Qué diferencia existe entre identificación y autenticación en un sistema de información?
2. ¿Cuáles son las ventajas y riesgos de implementar biometría en una organización?
3. ¿Cómo contribuye el RBAC a la reducción de riesgos internos?
4. ¿Por qué es importante la segregación de funciones en sistemas financieros digitales?
5. ¿Cómo influye la capacitación en la reducción de vulnerabilidades humanas?

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.