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**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Configurar Usuarios, Roles y Perfiles en el Despliegue de Tecnologías

Presentación del tema

La configuración adecuada de usuarios, roles y perfiles durante el despliegue de un sistema constituye uno de los pilares fundamentales de la gobernanza en Tecnologías de la Información (IT). En el momento del go-live, el sistema deja de ser un proyecto técnico y pasa a integrarse en la operación real del negocio. En ese punto, la correcta definición de accesos determina no solo la seguridad de la información, sino también la integridad de los procesos, el cumplimiento normativo y la eficiencia operativa.

Desde la perspectiva de la administración, la gestión de accesos se vincula directamente con el control interno, la segregación de funciones, la prevención de fraudes, la protección de activos digitales y la responsabilidad organizacional. La configuración de usuarios y roles define quién puede hacer qué, cuándo y bajo qué condiciones dentro del sistema.

Conceptos fundamentales

Usuario (User Account). Es la identidad digital asociada a una persona física o entidad técnica dentro del sistema.

Rol (Role). Es un conjunto de permisos agrupados según funciones organizacionales. Por ejemplo, el rol “Contador” agrupa los permisos de acceso a módulos financieros.

Perfil (Profile). Es una configuración específica que determina el alcance operativo del usuario dentro de ciertos módulos o procesos.

Control de acceso basado en roles (RBAC, Role-Based Access Control). Es el modelo de seguridad donde los permisos se asignan a roles y los roles a usuarios, reduciendo la complejidad administrativa y facilitando el control, la escalabilidad y el cumplimiento de auditorías.

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**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Segregación de funciones

La segregación de funciones (SoD, Segregation of Duties) es un principio de control interno que establece que ninguna persona debe tener control completo sobre todas las etapas de un proceso crítico. En sistemas empresariales se traduce en separar roles de creación, aprobación y ejecución: quien registra facturas no debería poder aprobar pagos ni modificar reportes financieros. Este principio reduce el riesgo de fraude, los errores no detectados y los conflictos de interés. Durante el despliegue, deben realizarse análisis de SoD para detectar incompatibilidades en la asignación de roles.

Cuentas de servicio

Las cuentas de servicio (Service Accounts) son identidades técnicas utilizadas por aplicaciones, procesos automáticos o integraciones entre sistemas. No están asociadas a personas, sino a procesos batch, integraciones automáticas, servicios web o tareas programadas. Por ejemplo, una cuenta de servicio permite que el sistema de ventas actualice automáticamente el sistema contable cada noche.

Sus características distintivas son que poseen permisos específicos y restringidos, tienen contraseñas controladas, no deben usarse para acceso interactivo humano y deben estar documentadas. Si poseen permisos excesivos pueden ser explotadas; si no se controlan, pueden comprometer la seguridad. Desde la administración, deben estar inventariadas, tener propietarios asignados y ser auditadas periódicamente.

Principios clave de seguridad en el acceso

Mínimo privilegio (Least Privilege). Establece que cada usuario o cuenta debe tener únicamente los permisos necesarios para cumplir su función. Reduce la superficie de ataque, minimiza errores y permite un control más eficiente.

Gestión de accesos privilegiados. Las cuentas administrativas deben gestionarse mediante controles especiales, como PAM (Privileged Access Management), registro de auditoría y autenticación multifactor (MFA).

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**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

Trazabilidad y auditoría. Un sistema bien configurado registra accesos, mantiene historial de cambios, identifica responsables y permite el seguimiento de incidentes. Sin trazabilidad, la responsabilidad organizacional se diluye. En sectores regulados, la auditoría es obligatoria.

Conceptos clave

- RBAC: permisos agrupados en roles asignados a usuarios.
- SoD: nadie debe tener control completo sobre un proceso crítico.
- Cuentas de servicio: identidades técnicas con permisos restringidos y documentadas.
- Mínimo privilegio: solo los permisos necesarios para la función asignada.
- Trazabilidad como requisito de control interno y cumplimiento regulatorio.

Preguntas de repaso del tema

1. ¿Cuál es la diferencia entre un rol y un perfil dentro de un sistema empresarial?
2. ¿Por qué es fundamental la segregación de funciones en sistemas financieros?
3. ¿Qué riesgos presentan las cuentas de servicio con permisos excesivos?
4. ¿Qué implica aplicar el principio de mínimo privilegio?
5. ¿Cómo contribuye el modelo RBAC a la gestión de accesos?
6. ¿Por qué la auditoría y la trazabilidad son componentes obligatorios en sectores regulados?
7. ¿Qué análisis deben realizarse durante el despliegue para detectar incompatibilidades de roles?

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**.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

8. ¿Por qué las cuentas de servicio deben estar inventariadas y auditadas periódicamente?
9. ¿Cómo puede una mala configuración de accesos generar pérdidas financieras?
10. ¿Cómo impacta la gestión de accesos en la gobernanza de TI?