Universidad de Buenos Aires
Facultad de Ciencias Económicas

Configurar Usuarios, Roles y Perfiles al momento del Despliegue de Tecnologías

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

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 (TI). En el momento del Go-Live (puesta en producción), 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 no es un asunto exclusivamente técnico. Se vincula directamente con:

- Control interno.
- Segregación de funciones.
- Prevención de fraudes.
- Protección de activos digitales.
- Cumplimiento regulatorio.

- Responsabilidad organizacional.

En entornos empresariales como ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales), CRM (Customer Relationship Management – Gestión de Relaciones con Clientes), sistemas financieros, plataformas logísticas o sistemas de recursos humanos, la configuración de usuarios y roles define quién puede hacer qué, cuándo y bajo qué condiciones.

Asimismo, la correcta gestión de **cuentas de servicio** —cuentas técnicas utilizadas por aplicaciones o procesos automáticos— constituye un componente crítico para la estabilidad y seguridad del sistema.

Desarrollo

1. Conceptos fundamentales

La administración de accesos en sistemas empresariales se basa en principios estructurados.

Usuario (User Account – Cuenta de Usuario)

Es la identidad digital asociada a una persona física o entidad técnica dentro del sistema.

Rol (Role – Rol)

Es un conjunto de permisos agrupados según funciones organizacionales.

Perfil (Profile – Perfil)

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

RBAC (Role-Based Access Control – Control de Acceso Basado en Roles)

Es un modelo de seguridad donde los permisos se asignan a roles y los roles a usuarios, reduciendo la complejidad administrativa.

Desde la administración, el modelo RBAC permite:

- Escalabilidad.
- Control centralizado.
- Reducción de errores en asignación de permisos.

- Cumplimiento de auditorías.

---

2. Importancia estratégica en el despliegue

Durante el despliegue, la configuración de usuarios y roles no debe improvisarse. Es parte integral del plan de implementación.

Una mala configuración puede generar:

- Accesos indebidos.
- Conflictos de segregación de funciones.
- Exposición de datos sensibles.
- Errores operativos.
- Incumplimiento regulatorio.

Por el contrario, una configuración adecuada permite:

- Trazabilidad.
- Responsabilidad individual.
- Control financiero.
- Protección de información estratégica.

Ejemplo:

En un sistema contable, el usuario que registra facturas no debería tener permisos para aprobar pagos, en cumplimiento del principio de segregación de funciones.

---

3. Segregación de funciones (SoD – Segregation of Duties)

La segregación de funciones 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, esto se traduce en:

- Separar roles de creación, aprobación y ejecución.
- Limitar permisos administrativos.

- Evitar concentración de poder digital.

Desde la administración, este principio reduce:

- Riesgo de fraude.
- Errores no detectados.
- Conflictos de interés.

Durante el despliegue, deben realizarse análisis de SoD para detectar incompatibilidades.

---

4. Configuración de perfiles por área funcional

Los perfiles deben alinearse con la estructura organizacional.

Ejemplo en ERP:

- Perfil Contador: acceso a módulos financieros.
- Perfil Compras: acceso a órdenes y proveedores.
- Perfil Logística: acceso a inventarios.
- Perfil Auditoría: acceso de solo lectura.

La configuración incorrecta puede generar:

- Retrasos operativos.
- Accesos excesivos.
- Riesgo de manipulación de datos.

Desde la administración estratégica, los perfiles deben diseñarse en conjunto entre TI y áreas funcionales.

---

5. Cuentas de servicio (Service Accounts – Cuentas de Servicio)

Las **cuentas de servicio** 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.
- Automatizaciones.
- Tareas programadas.

Características:

- Permisos específicos.
- Contraseñas controladas.
- No utilizadas para acceso interactivo humano.
- Deben estar documentadas.

Ejemplo:

Una cuenta de servicio permite que el sistema de ventas actualice automáticamente el sistema contable cada noche.

Riesgos asociados:

- Si poseen permisos excesivos, pueden ser explotadas.
- Si no se controlan adecuadamente, pueden comprometer seguridad.

Desde la perspectiva administrativa, las cuentas de servicio deben:

- Estar inventariadas.
- Tener propietarios asignados.
- Ser auditadas periódicamente.
- Poseer controles de acceso restringidos.

---

6. Principio de mínimo privilegio (Least Privilege – Mínimo Privilegio)

Este principio establece que cada usuario o cuenta debe tener únicamente los permisos necesarios para cumplir su función.

Beneficios:

- Reducción de superficie de ataque.
- Minimización de errores.

- Control más eficiente.

En el despliegue, aplicar el mínimo privilegio es una medida preventiva crítica.

---

7. Gestión de accesos privilegiados

Las cuentas administrativas o con permisos elevados deben gestionarse mediante controles especiales.

Incluye:

- PAM (Privileged Access Management – Gestión de Accesos Privilegiados).
- Registro de auditoría.
- Autenticación multifactor (MFA – Multi-Factor Authentication).

Desde la administración, estas medidas protegen activos críticos.

---

8. Auditoría y trazabilidad

Un sistema bien configurado debe permitir:

- Registro de accesos.
- Historial de cambios.
- Identificación de responsables.
- Seguimiento de incidentes.

Sin trazabilidad, la responsabilidad organizacional se diluye.

En sectores regulados, la auditoría es obligatoria.

---

9. Impacto financiero y reputacional

Una configuración deficiente puede generar:

- Fraudes internos.
- Pérdida de información.
- Sanciones regulatorias.
- Daño reputacional.
- Interrupción operativa.

Desde la administración, la gestión de usuarios es una inversión en control y prevención.

---

10. Ejemplo integral

En una empresa que implementa un sistema financiero:

- Se definen roles por área.
- Se aplican reglas de segregación.
- Se configuran cuentas de servicio para integraciones.
- Se limita acceso administrativo.
- Se auditan permisos antes del Go-Live.

Este proceso protege la integridad financiera.

Conclusión

La configuración de usuarios, roles y perfiles durante el despliegue de sistemas constituye un componente estratégico esencial de la gobernanza en TI. No se trata de una tarea técnica secundaria, sino de un elemento central del control interno, la seguridad y la continuidad operativa.

La correcta definición de accesos protege la información, reduce riesgos financieros y asegura cumplimiento normativo. Asimismo, la adecuada gestión de cuentas de servicio garantiza estabilidad técnica sin comprometer seguridad.

Desde la perspectiva de la administración, la gestión de accesos debe abordarse como un proceso estructurado, documentado y alineado con la estrategia organizacional. En un entorno digital cada vez más complejo, la seguridad comienza con la correcta definición de quién puede hacer qué dentro del sistema.

Preguntas de autoevaluación

1. ¿Qué diferencia existe 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 mal configuradas?
4. ¿Qué implica aplicar el principio de mínimo privilegio?
5. ¿Cómo impacta la gestión de accesos en la gobernanza de TI?

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.