

Trabajo Práctico de Prácticas Profesionalizantes 2

Germán bisutti Moscatelli

Primera Parte: Tarea posterior a los videos: Después de ver el video, debe reflexionar y escribir un análisis crítico.

1 - ¿Por qué es importante tener roles y perfiles bien definidos en los sistemas? Pueden explicarlo dando un ejemplo. (no los detallados en el video).

2 - ¿Qué desafíos pueden surgir si los roles y perfiles no están correctamente gestionados?

3 - ¿Cómo podrían los roles y perfiles mal diseñados afectar a la experiencia del usuario o a la seguridad del sistema?

1- Es importante tener bien definidos los roles y perfiles en los sistemas porque permite mantener una estructura organizada, segura y controlada. Al asignar distintos niveles de acceso según el perfil del usuario, se protege la información sensible y se evita el uso indebido de funcionalidades críticas del sistema. Además, esto facilita la administración, ya que permite gestionar permisos de forma eficiente.

Por ejemplo, dentro de un hospital, un médico necesita acceder a los historiales clínicos de los pacientes, mientras que un administrativo sólo debería poder ver información relacionada con turnos o datos de contacto. Si no se definen bien estos roles, cualquier empleado podría acceder a información confidencial, lo cual representaría un riesgo tanto ético como legal.

Otro ejemplo podría ser en una escuela, un docente puede cargar notas, pero solo el administrador puede modificar datos personales de los alumnos. Definir roles, evita accesos indebidos y mantiene el orden en el sistema.

2- Puede surgir que algunos roles o perfiles accedan a información que no les corresponde y esto dificulta el trabajo en equipo, además representa un riesgo en la seguridad. Cuando un miembro del equipo accede o modifica datos sin tener la responsabilidad o el contexto necesario, se puede distorsionar el flujo de trabajo, entorpecer la toma de decisiones e incluso generar conflictos entre áreas.

3- Los roles y perfiles mal diseñados pueden comprometer la seguridad al permitir accesos no autorizados a información sensible, y afectar la experiencia del usuario al generar confusión, restricciones innecesarias o sobrecarga de funciones, lo que reduce la eficiencia y confianza en el sistema.

Segunda Parte:

Tarea Caso1: Analicen qué roles y perfiles deberían existir en este sistema y justifiquen la asignación de permisos y accesos. ¿Cómo podrían manejar los perfiles para asegurar que no se filtren datos sensibles?

Empleado

- Acceso a su información personal.
- Cargar horas trabajadas o tareas realizadas
- Consultar los avisos generales

Justificación: Permitir que el empleado pueda realizar sus tareas sin poner en riesgo datos sensibles.

Supervisor

- Acceso a todas las funciones del empleado
- Revisión y aprobación de tareas del equipo
- Generar reportes del equipo

Justificación: Permitir la normal gestión operativa del equipo a su cargo.

Gerente

- Acceso a todas las funciones del supervisor
- Visualizar informes de distintas áreas
- Realizar análisis de productividad, ausentismo y desempeño de los equipos

Justificación: Debe tener una visión más global para una mejor toma de decisiones.

Administrador

- Gestión de todo el Sistema
- Gestión de altas, bajas y modificaciones de usuarios
- Gestión de acceso a los recursos y configuración de los mismos

Justificación: Es el responsable del funcionamiento técnico y operativo del sistema.

Medidas para evitar que se filtren datos sensibles:

- Acceso limitado al rol necesario (Principio del mínimo privilegio)
- Para el acceso a datos críticos (Autenticación multifactorial (MFA))
- Para tener una trazabilidad de los movimientos (Auditoría y registros de actividad).
- Para protegerse de posibles brechas (Encriptación de datos confidenciales)
- Segmentar el acceso para las distintas áreas y jerarquías
- Revisar periódicamente los accesos y los roles asignados

Tarea Caso2: discutir cómo se pueden rediseñar los perfiles y roles en el sistema para garantizar una mayor seguridad.

¿Qué medidas se deben tomar?

Se deben implementar medidas de control de acceso y organización de perfiles, asignando a cada usuario un límite específico según su tarea y responsabilidad. Esto permitirá garantizar que cada persona tenga acceso solo a la información y las tareas que le corresponden, evitando así posibles errores o accesos no autorizados. De esta manera, se puede mantener la seguridad y la integridad de la información, y asegurarse de que cada tarea sea realizada por la persona adecuada.

¿Deberían los roles ser más estrictos o más flexibles?

Los roles deberían ser más estrictos y bien definidos para garantizar que cada usuario tenga acceso solo a las tareas y responsabilidades que le corresponden, evitando así posibles errores o interferencias en el trabajo de otros usuarios. De esta manera, se puede mantener la integridad y la estructura del trabajo, y asegurarse de que cada persona se concentre en sus tareas específicas sin sobrepasar sus límites. Esto también ayudará a prevenir posibles conflictos o problemas que puedan surgir debido a la superposición de tareas o responsabilidades.