Obligatorio Base de Datos

Segunda Entrega - Modelo Entidad Relación.

Ingeniería en Informática

2020

Integrantes del grupo

Agustín Picos
Franco Gai
Micaela Olivera

Índice

Introducción

Se solicita realizar un sistema que permita gestionar usuarios y roles con sus determinadas responsabilidades, implementar un sistema de autenticación y autorización eficiente que posteriormente pueda ser escalable para integrar con aplicaciones de cualquier tipo de problemática.

El programa debe permitir a un usuario loguearse y según el rol que tenga en el mismo acceder a determinadas funcionalidades y/o menús equivalentes a su nivel de responsabilidad.

Deberá existir un usuario administrador el cual será el único con la potestad de autorizar la creación de usuarios y asignar roles a los mismos. Así mismo el sistema deberá contar con un módulo de auditoría para poder identificar que usuarios realizan determinadas actividades en el mismo.

Se debe comenzar con una funcionalidad que permite crear, actualizar y modificar roles y usuarios , así como también asignarle a los usuarios sus correspondientes roles. Se deberá implementar medidas de seguridad en la creación de usuarios, como por ejemplo establecer pautas para la creación de contraseñas y posteriormente su encriptado y la asignación de una pregunta secreta de verificación que permita al usuario identificarse en caso de olvidar la misma.

Además todas las solicitudes estarán sujetas a aprobación de un colega de rango superior, o de no haberlo, de un par (siempre y cuando este último exista).

Análisis del Problema

Se identifican distintos requerimientos en el análisis del problema:

- En primer lugar se nota la necesidad de implementar una correcta gestión de usuarios (esto implica creación eliminación y modificación de los mismos).

- La misma necesidad del punto anterior se aplica a la gestión de los roles que deben existir en el sistema, indicando la responsabilidad que le corresponde a cada rol sobre el sistema.

- Se debe implementar la lógica correspondiente para poder autenticar a los usuarios, mediante un login, brindando la seguridad correspondiente sobre el usuario y contraseña.

- Los usuarios deberán contar con una interfaz en la cual puedan actualizar sus datos personales. Un mismo sujeto podrá contar con varios usuarios.

- Se entiende el usuario y la persona como entidades diferentes, de esta manera se puede relacionar una persona a varios usuarios. Por lo tanto se necesita tener tanto el formulario de ingreso de persona, como el de creación de usuario.

- Asimismo el administrador del sistema deberá contar con una interfaz que le permita gestionar usuarios, roles y menús.

- Se debe contar con un mecanismo de autorización, es decir el asignar a cada usuario su rol o roles correspondiente.

- Se detecta la necesidad de crear una aplicación escalable y adaptable a cualquier tipo de problemática.

- Auditoría: se deberá llevar un registro de todos los cambios que se hacen, tales como creación y eliminación de usuarios o asignación de permisos. Se debe elaborar una estructura que permita evaluar quién hizo los cambios, cuándo los realizó, y el detalle del cambio en sí mismo, es decir, qué variables fueron modificadas.

- Oposición de interés: existen tareas en las que es prioritario que sean gestionadas por más de una persona, es decir, que una sola persona no sea la única involucrada, sino que sea requerida la aprobación de otra, como por ejemplo la creación de un usuario. La finalidad de esto es generar cierto control sobre las acciones que se toman.

Desarrollo de la Solución

Para el desarrollo de la solución se deben tener en cuenta varios puntos y cómo los se van a resolver individualmente.

Gestión de personas y usuarios.

El sistema contará con dos formas diferentes de crear un usuario; la primera será por parte del administrador, el cual podrá ingresar personas al sistema y crearle un usuario. Posteriormente le asignará su/sus rol/roles correspondiente y será el sistema el cual le asignará una clave autogenerada a la persona, quien deberá modificarla posteriormente.

En la segunda opción, la persona ingresa a la aplicación por primera vez y decide crearse un usuario, para ello en la pantalla de login selecciona una opción para crear un usuario nuevo. En este caso, La persona tendrá un formulario a su disposición, el cual deberá llenar con sus datos personales junto con los datos de su primer usuario y lo deberá confirmar. Luego de realizado este proceso, el administrador (quien puede ver un lista de personas y usuarios con pendiente aprobación) podrá o no aprobar la creación de dicho perfil y asignarle su rol correspondiente.

Las aprobaciones o rechazos deben quedar registradas con sus respectivos comentarios, para garantizar la transparencia de la gestión.

Para la creación de un usuario se solicitará la siguientes información:

- Nombre y apellido.
- Nombre de usuario.
- Contraseña.
- Cédula de identidad.
- Correo electrónico.
- Fecha de nacimiento.
- Sexo.

Una vez aprobada la persona y logueada en el sistema, esta podrá actualizar sus datos y solicitar la creación de más usuarios asignados a sí misma.

Gestión de Roles.

Para la creación de un nuevo rol se solicitarán los siguientes datos:

- Nombre del rol.
- Menús a los que puede acceder dicho rol.

Cabe destacar que solo el administrador podrá gestionar este módulo.

Autorización y autenticación.

En términos generales, es común que cuando una persona física utiliza un sistema, lo hace a través de un usuario dentro del sistema. Este usuario tiene un parámetro que lo identifica de forma única, como lo es el nombre de usuario. La persona además de utilizar ese nombre o identificador, debe tener algún mecanismo con el cual compruebe su identidad.

El concepto más básico es el de contraseña. En términos simples, la contraseña suele ser un atributo del usuario dentro del sistema. Para el usuario, es una cadena de caracteres. Esta contraseña deberá ser conocida únicamente por la persona física que utiliza ese usuario. Los usuarios y contraseñas deben ser individuales, es decir, un usuario es utilizado por una única persona física.

Es importante el concepto de confidencialidad de la contraseña. Ni siquiera los administradores del sistema deben conocer o tener acceso a esta. En estos casos, las contraseñas deben ser cifradas dentro del sistema para no ser guardadas en texto plano.

También existen otros mecanismos más avanzados para la autenticación del usuario, como pueden ser el PIN, certificados digitales, tokens, verificaciones de dos pasos con distintos dispositivos, o por ejemplo, como en el caso de los celulares, escaneos de rostro o sensores de huellas dactilares. La idea de estas herramientas es garantizar por otros medios que la persona es quien dice ser, ya que, por ejemplo, una contraseña simple podría ser robada o incluso adivinada por otra persona.

Existen también medidas de seguridad, para dificultar por ejemplo, un ataque de fuerza bruta, en el que se toma un usuario y se prueban todas las permutaciones posibles de contraseña dentro de un rango. Para este caso, se recomienda que las contraseñas posean una longitud de al menos 8 caracteres, que posean mayúsculas, minúsculas, números, caracteres especiales y además no formen palabras de diccionario

Una vez accedido al sistema, debe estar definido qué tipo de acceso tiene el usuario utilizado. Existen términos comunes como lo son el acceso de administrador, que generalmente puede acceder a todos los recursos del sistema y modificar todas la variables; o el usuario básico con permisos mínimos, que suelen ser de solo lectura, y sobre un conjunto determinado de datos. Luego existen permisos intermedios que poseen más privilegios que un usuario básico, pero sin llegar a ser administrador. Estos permisos intermedios se ajustan a la función del usuario dentro del sistema y están relacionados con los permisos, privilegios y funciones de la persona física que utiliza el usuario del sistema.

Es importante tener definido el conjunto de autorizaciones que posee cada uno de estos usuarios. A este conjunto de permisos se lo denomina comúnmente rol.

Otro factor importante a tener en cuenta es que un usuario, con un rol, no debería poseer permisos para auto asignarse permisos más elevados.

Pantalla Administrador.

Una vez que un administrador logue en el sistema tendrá a su disposición una pantalla en la cual podrá ver todos los menús del sistemas, así como también botones que lo lleven al módulo de usuarios, de roles y de solicitudes de usuarios.

Desde esta pantalla principal el administrador podrá también salir del sistema.

Modulo de Usuarios.

Cuando un administrador ingresa al módulo de usuarios, podrá visualizar una lista de todos los usuarios creados, también podrá crear usuarios nuevos y eliminarlos.

En este módulo también se llevará a cabo la asignación de roles para los usuarios creados, ya que un usuario sin rol no podrá loguearse en el sistema.

También cabe aclarar que el administrador no podrá ver en texto plano las contraseñas de los usuarios una vez creados los mismo.

Módulo de Roles.

Cuando se ingrese al módulo de roles, al igual que en el módulo de usuarios, se verán listados los roles existentes, así como también la posibilidad de crear nuevos roles y eliminarlos.

Solicitudes de usuarios.

En esta pantalla, el administrador podrá ver la lista de usuarios creados que están a la espera de su aprobación. Estos usuarios pendientes de aprobación, serán aquellos que fueron creados por personas sin rol de administrador. Una vez que el Administrador apruebe la creación de dicho usuario, deberá dirigirse al módulo de usuarios para asignarle su rol correspondiente.

Pantalla Usuario.

Una vez que el usuario logue en el sistema tendrá visibles todos los menu a los que tenga su acceso autorizado, así como también dispondrá de un botón que le mostrará una ventana para actualizar sus datos personales y contraseña.

Desde su pantalla el usuario podrá navegar y salir del sistema.

Auditoría.

Es ideal que en los sistemas exista una figura que auspicie de contralor. El auditor debe ser una persona que no participe activamente en la sección auditada. El por qué es sencillo, no tiene sentido que un auditor investigue sus propias acciones o elementos con los que tenga relación.

El objetivo de la auditoría es controlar que todas las acciones realizadas dentro del sistema fueron correctas o investigar luego de ocurrido algún incidente, quienes fueron los involucrados, que hicieron y cómo.
En bases de datos, las operaciones de insertar, modificar y eliminar son las básicas a ser registradas para auditar, además de guardar la fecha y la información previa de los valores modificados y borrados.

Oposición de Interés.

Este es un mecanismo que tiene como objetivo brindar transparencia a las organizaciones.
A fin de evitar el ocultamiento o irregularidades, los procesos de una empresa no son abarcados por una única entidad, sino que se fragmentan y reparten en la organización. De esta forma se ejerce un control cruzado sobre las tareas.

A nivel del sistema planteado en este caso, el manejo de los usuarios no debe ser realizado por una única entidad sino que dicha tarea se debe repartir entre al menos otra persona que sea ajena a posibles intereses que hay dentro de un proceso dado. Un ejemplo de esto podría ser que se requiera la autorización de dos usuarios para la creación de un usuario o que quien lo crea no sea la misma persona que le asigna un rol.

Modelo Entidad Relación

Estructuras creadas

Para cada una de las entidades principales (Persona, Usuario, Menú, Rol, Solicitud, Permiso) fue creada una tabla. Luego, fueron necesarias tablas auxiliares (Usuario_rol, Rol_Permiso, Rol_Menu) para poder modelar relaciones de muchos a muchos entre tablas.
Se corroboró que todas las entidades fueran representadas de alguna forma (como tablas o atributos).

Comprobación de satisfacción de condiciones

La tabla de ***Usuario*** permite la creación, eliminación y actualización de los usuarios. La tabla ***Persona***. A su vez, la existencia de la tabla ***Persona*** permite diferenciar a las entidades y relacionarlas, a modo que una persona pueda tener varios usuarios. En este caso, el modelo no permite que un usuario sea utilizado por varias personas.

La tabla de ***Rol*** tiene la función de especificar un conjunto de permisos y menús a los que podrá acceder un usuario. En base a la tabla de ***Rol***, se puede especificar de forma granular qué permisos y menús se poseen, pudiendo relacionar con gran flexibilidad estos valores. En este caso, un rol puede poseer muchos permisos y menús, pudiéndose dar la situación de que dos roles diferentes puedan acceder a varios componentes en común, pero teniendo diferencias en detalles como algunos permisos.

La tabla ***Auditoria*** permite registrar los eventos del sistema como inserción, actualización y eliminación de los datos de las tablas. Además retiene datos como el usuario involucrado, fechas, menú de origen y los valores previos y posteriores a dicho evento.

La tabla ***Solicitud*** tiene como función dar una base al principio de oposición de interés, reteniendo datos como los usuarios originadores, usuarios autorizantes, la descripción, fechas de solicitud y autorización, además de indicar si el estado de estas se encuentra en pendiente, rechazado o aprobado. Mediante el uso de la aplicación se implementarán los conjuntos disjuntos entre los que se dará esta oposición de interés.

Se considera que el modelo tiene términos muy genéricos, pero completos a la vez, permitiendo la escalabilidad del sistema para poder ser utilizado en cualquier negocio.

Se agregaron reglas para imposibilitar la insercion de datos en casos que no corresponda, como por ejemplo en la tabla persona, el atributo sexo solo admite el valor M o F, cualquier otro valor sera rechazado. Lo mismo ocurre en el caso de Solicitud, cuyo estado solo admite pendiente, aprobado y rechazado.

Conclusiones

Bibliografía

sans.org. (2014). Password Security. [online] Available at: https://www.sans.org/reading-room/whitepapers/basics/password-security-thirty-five-years-35592

sans.org. (2003). The Use and Administration of Shared Accounts:. [online] Available at: https://www.sans.org/reading-room/whitepapers/basics/administration-shared-accounts-1271

sans.org. (2002). The Password Web Page. [online] Available at: https://www.sans.org/reading-room/whitepapers/basics/password-web-page-533

elauditor.info (2017) Control Por Oposición de Intereses.[online] Available at: https://elauditor.info/diccionario-del-control/control_a59c2f0d80041ac58e313c594

Database systems - The complete book – Ullman, Widom, Prentice-Hall, 2°Ed. 2002.

Fundamentos de Bases de Datos – Silberschatz, Korth, Sudarshan, MCGraw-Hill Inc. 4°Ed. 2002.

Introducción a los sistemas de Bases de Datos – Date, Prentice-Hall, 7°Ed. 2000.