

Roles y permisos

Crear roles, asignar permisos, entender la herencia, invitar empleados, obligatoriedad de dos factores, representantes legales y el bloqueo por turno. Con los errores típicos.

unitlify.de/docs/rollen-rechte · 2026-10-22

Cómo funcionan los permisos en Unitlify

Cada persona tiene uno o varios **roles**. Cada rol lleva una lista de **permisos**, por ejemplo «Ver reservas» o «Crear turnos». Lo que una persona puede hacer es la suma de los permisos de sus roles. Los permisos valen para toda la empresa.

Unitlify crea dos roles al dar de alta la empresa:

- **Administrador:** tiene todos los permisos, también todos los futuros. Los permisos no se pueden cambiar y el rol no se puede eliminar. La primera persona de la empresa es administrador y representante legal (véase más abajo).
- **Empleado:** el rol base. Cada persona invitada lo recibe automáticamente. Al principio está **vacío**, usted decide qué puede hacer cada persona en la empresa.

Menú **Administración** → **Roles**. Necesita el permiso «Ver roles» para consultarlos y «Crear roles/Editar roles» para cambiarlos.

Configurar el rol base «Empleado»

Es el paso más importante tras el inicio. Todo lo que cada persona de la empresa debe ver pertenece al rol base, por ejemplo:

- Ver turnos propios y solicitar turnos abiertos
- Solicitar vacaciones, presentar baja por enfermedad, ver ausencias propias
- Fichar y ver la cuenta de horas propia
- Chat, noticias, directorio

Sin estos permisos, los empleados invitados no ven casi nada tras iniciar sesión; incluso la página «Mis turnos» solo aparece con el permiso correspondiente.

A la inversa: lo que tiene el rol base lo tienen automáticamente **todos** los roles superiores. Por eso, los permisos que solo deben tener los responsables no pertenecen al rol base.

Los puestos como «Jefe de turno» o «Entrenador» se crean como roles propios. Solo llevan los permisos que van más allá del rol base.

Crear roles

Nuevo rol: código (único por empresa), nombre, opcionalmente descripción y salario por hora. Después marque los permisos, agrupados por áreas: Dashboard, Comunicación, Sistema de reservas, Ticketing y vales, Finanzas, Personal, Formaciones, Contratos y formularios, Administración.

Un rol nuevo se coloca directamente encima del rol base en el orden de rangos.

Si marca **todos** los permisos, el rol se convierte en un rol con derechos completos como el administrador, incluidos todos los permisos que se añadan más adelante. Úselo de forma consciente.

Plantilla «Asesoría fiscal (solo lectura)»

Mediante **Plantilla** crea un rol de lectura listo para el asesor fiscal: solo lectura de facturas, reservas, finanzas, facturas de Unitlify y gastos. No hereda nada y queda directamente debajo del administrador. Tenga en cuenta: cada persona invitada recibe además el rol base y cuenta en los paquetes con precio por empleado.

Herencia y orden de rangos

Los roles están ordenados por rango (rango 1 arriba del todo). **Un rol hereda todos los permisos de los roles que están debajo de él.** Los permisos heredados aparecen marcados en azul y se pueden desmarcar individualmente por rol si un rol superior expresamente no debe tener un permiso concreto.

Ordene arrastrando y soltando. Ejemplo: rol base «Empleado» abajo, encima «Entrenador», encima «Jefe de turno», encima «Dirección de operaciones». La dirección de operaciones tiene así todo lo que tienen los tres roles inferiores, más sus propios permisos.

Dos cosas nunca se heredan: la marca de derechos completos («todos los permisos») y el bloqueo por turno (abajo).

Los cambios de permisos, las asignaciones de roles, reordenar y eliminar roles tienen efecto inmediato, sin nuevo inicio de sesión.

Bloqueo por turno

Tres permisos existen en la variante «solo durante el turno propio»: reservas, envíos de formularios y Service Center. Una persona con esta variante solo ve los datos mientras está de servicio según el plan de turnos (hora de Berlín, sin margen). Fuera de él aparece «Fuera de su turno no tiene acceso a estos datos».

Importante: el bloqueo afecta a la **persona entera** en cuanto uno de sus roles lo lleva, a menos que otro rol tenga derechos completos. Por eso no asigne el bloqueo a un rol que los responsables también lleven adicionalmente. Y: quien no tiene turno en el plan no tiene acceso.

Sedes

En **Administración** → **Sedes** crea sedes con áreas y subáreas y asigna empleados. La asignación controla lo que una persona ve en el directorio, en los canales de chat, en las tareas y en el almacenamiento, y sirve como filtro en las listas de personal. Los permisos en sí valen para toda la empresa independientemente de la sede.

Invitar empleados

Menú **Personal** → **Empleados** → **Invitar empleado**. Obligatorios: nombre, correo electrónico y al menos un rol; el rol base siempre está incluido. Opcional: sedes. Hasta 50 personas a la vez.

- La invitación se envía por correo electrónico, el enlace es válido **7 días**. Si el correo no llega, copie el enlace desde la lista.
- La persona invitada debe registrarse con **exactamente esta** dirección de correo, contraseña de al menos 8 caracteres.
- **Reenviar** genera un nuevo enlace válido 7 días, el anterior queda invalidado.
- Si ya existe una cuenta activa o una invitación abierta para la dirección, la invitación se rechaza.
- Una cuenta eliminada anteriormente con la misma dirección se reactiva, con nuevos roles y sin la antigua configuración de dos factores.
- Si exige el cuestionario de personal, la persona recibe la petición de rellenarlo tras aceptar.

Representantes legales

Los representantes legales son las personas que representan legalmente a la empresa. Solo ellos pueden aceptar o rechazar las CGC y el contrato de encargo, cancelar la cuenta de Unitlify, y reciben la confirmación al cancelar módulos. La pestaña **Configuración** → **Legal** solo es visible para ellos.

- El derecho solo lo concede un representante legal, y solo a administradores.
- El último representante legal no puede perder el derecho ni ser eliminado.

Autenticación de dos factores

Cada persona puede configurar un segundo factor en **Mi perfil**: app de autenticación (con códigos de respaldo) o passkey. La configuración solo es posible en la web; la app pide el código después.

En **Configuración** → **Operativa** → **Seguridad** puede **exigir** el segundo factor a todos los empleados o a roles concretos. Quien aún no lo haya configurado solo ve entonces en la web la pantalla de configuración y no puede iniciar sesión en la app. Anuncie por tanto la obligación y dé tiempo al equipo antes de activar el interruptor. Mientras la obligación esté activa, nadie puede eliminar su último factor.

Sesiones y contraseñas

- Si una persona cambia su contraseña o su correo electrónico, se cierra la sesión en todos los demás dispositivos.
- Si un empleado es desactivado o eliminado, sus sesiones terminan de inmediato.
- Tras 10 intentos de inicio de sesión fallidos, la cuenta queda bloqueada 30 minutos.
- Al iniciar sesión desde un dispositivo nuevo, la persona recibe un correo de aviso.
- Contraseña olvidada: código de 6 dígitos por correo, válido 15 minutos.

Directorio

Cada persona activa aparece en el directorio, con nombre, roles y sedes. Si el correo, el teléfono, la biografía y la imagen son visibles lo ajusta cada persona en **Mi perfil** («Perfil visible dentro de la organización» y los interruptores por campo). Los contactos externos tienen su propia pestaña con permiso propio.

Lista de comprobación ante problemas

- **Un empleado nuevo no ve nada tras iniciar sesión:** el rol base «Empleado» no tiene permisos. Añada allí los permisos para turnos, vacaciones, baja por enfermedad y fichaje.
- **De repente todos ven las finanzas:** se asignó un permiso al rol base o a un rol inferior y se heredó hacia arriba.
- **El jefe de turno no puede ver las reservas:** uno de sus roles lleva el bloqueo por turno y ahora mismo no tiene turno en el plan.
- **No se puede aceptar la invitación:** enlace de más de 7 días, otra dirección de correo, o ya existe una cuenta.
- **El inicio de sesión en la app falla tras activar la obligación de dos factores:** la persona debe configurar primero el segundo factor en la web en «Mi perfil».
- **Falta «Legal» en la configuración:** la persona no es representante legal.