| Costo: $$ | Impacto: MEDIO | Complejidad: MEDIO |
|---|---|---|

**2.C:** ¿Requiere el WWS credenciales únicas y diferentes para que los usuarios accedan a las redes de TO y TI?

**Recomendación:** Requiera que cada usuario individual tenga dos nombres de usuario y contraseñas diferentes; una cuenta para acceder a la red de TI y la otra cuenta para acceder a la red de TO, para reducir el riesgo de que un atacante pueda desplazarse entre ambas redes mediante un mismo inicio de sesión.

### ¿Por qué es importante este control?

Si un atacante puede determinar el inicio de sesión de un usuario en una red, utilizará esa información de inicio de sesión para intentar acceder a otras cuentas o redes. Los delincuentes también pueden utilizar la función de recuperación de contraseña de una cuenta para acceder a cualquier cuenta que utilice la misma dirección de correo electrónico. El uso de nombres de usuario y contraseñas diferentes para los usuarios de las redes de TO y TI es una parte integral de una estrategia de defensa en profundidad.

### Consejos de implementación

**ORIENTACIÓN ADICIONAL**

- Cuando sea factible, nunca permita que varios usuarios compartan un único inicio de sesión o que un solo usuario utilice el mismo inicio de sesión para las redes de TO y TI.

Desarrolle una política que requiera que las personas utilicen cuentas diferentes para TO y TI. Si su WWS tiene un solo dominio de Windows que cubre los sistemas de TO y TI, evalúe dividir ese dominio en dos para evitar que los usuarios compartan cuentas entre tipos de sistemas. Si los usuarios ya tienen cuentas diferentes para TO y TI, anímelos a no usar una contraseña común para estas cuentas.

Los dos sistemas operativos más comunes son Microsoft Windows y Linux. Ambos sistemas permiten que un administrador del sistema pueda gestionar cuentas y credenciales de cuenta para cada usuario final. Los recursos a continuación proporcionan detalles sobre cómo gestionar cuentas de usuario para cada sistema.

### Recursos

**Mejorar la ciberseguridad del sistema de control industrial con estrategias de defensa en profundidad:** La página 25 proporciona información sobre la gestión de cuentas de la red de TO. Nota: La CISA utiliza el término “sistema de control industrial” (ICS) para referirse a una red de TO.
*https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf*

**Gestión de cuentas de usuario en Linux:** Proporciona más información sobre cómo gestionar cuentas de usuario en Linux. *https://www.makeuseof.com/user-management-linux-guide/*