# Cuentas Zombi: El enemigo silencioso en tu Directorio Activo

En ciberseguridad, solemos imaginar ataques sofisticados con exploits de última generación. Sin embargo, la mayor vulnerabilidad de una empresa suele ser mucho más mundana: **una puerta que alguien olvidó cerrar.**

**El peligro de lo invisible**

Las "cuentas olvidadas" o huérfanas son aquellas que pertenecen a empleados, consultores o servicios que ya no tienen relación con la empresa, pero que permanecen activas en el sistema. No hacen ruido, no generan alertas de intrusión y, a menudo, poseen privilegios elevados que nunca fueron revocados. Para un atacante, encontrar una de estas cuentas es como encontrar una llave maestra tirada en la acera.

**¿Por qué fallan los sistemas de baja?**

El problema no suele ser técnico, sino de **procesos**. La desconexión entre Recursos Humanos e IT es la causa principal:

- **La trampa de lo evidente:** Se desactiva el correo electrónico, pero se olvidan accesos a bases de datos, VPNs secundarias o herramientas SaaS.
- **Dependencia de la memoria:** Sin un inventario centralizado, la baja de un usuario depende de que el administrador "recuerde" dónde le dio permisos hace dos años.
- **Falta de comunicación:** Sistemas que no "hablan" entre sí (el software de nóminas no avisa automáticamente al Active Directory).

**Cerrando las puertas: Una estrategia de higiene**

No hace falta una inversión millonaria para solucionar esto. La seguridad comienza con la disciplina operativa:

1. **Checklist de Salida (Offboarding):** Un protocolo estandarizado que enumere cada sistema que debe ser revisado tras una baja.
2. **Revisiones Trimestrales:** Cruzar la lista de empleados en nómina con la lista de usuarios activos en AD. Si alguien no está en la primera, no debería estar en la segunda.

3. **Auditoría de Privilegios:** Identificar cuentas administrativas que no han registrado actividad en los últimos 30 o 60 días y deshabilitarlas preventivamente.

**La pregunta que todo administrador debería hacerse hoy es:** Si un empleado descontento que se fue hace seis meses intentara entrar hoy a la VPN, ¿podría hacerlo?

**Ejercicio de Clase: "Caza de Cuentas Zombi"**

**Objetivo:** Diseñar un proceso de *Offboarding* (baja de personal) que elimine los puntos ciegos.

**Escenario:**

La empresa "Logística Global" ha sufrido una fuga de datos. El atacante utilizó las credenciales de **Roberto F.**, un consultor externo de bases de datos cuyo contrato finalizó hace 8 meses.

**El rastro del error:**

- RRHH avisó a IT de su baja por email, pero el técnico que lo recibió estaba de vacaciones.
- Se desactivó su cuenta de Office 365, pero su acceso a la base de datos SQL y su token de la VPN seguían activos.
- No existía un inventario de los sistemas a los que Roberto tenía acceso.

**Tareas para el alumno:**

1. **Análisis de Causas:** Enumera 3 fallos organizativos que permitieron que la cuenta de Roberto siguiera activa.
2. **Diseño del "Checklist Maestro":** Crea una lista de al menos 6 puntos que el departamento de IT deba marcar obligatoriamente cada vez que un empleado o consultor deje la empresa.
3. **Propuesta de Automatización:** Imagina que tienes que conectar el sistema de RRHH con el Active Directory. ¿Qué dato clave debería disparar una alerta o la desactivación automática de la cuenta?
4. **Simulación de Auditoría:** ¿Qué comando de PowerShell o qué filtro en el AD usarías para encontrar cuentas que no han

iniciado sesión en los últimos 90 días? (Escribe el razonamiento lógico, no hace falta el código exacto).