ProfCheck

El empleado más peligroso ya presentó su carta de renuncia

Esa ventana, entre el aviso y el último día, es el período de mayor riesgo de todo el ciclo de empleo. Y no se reduce al robo dramático. También se ve así: copiar una lista de clientes para uso personal. Enviar documentos de precios al correo personal para conservar muestras de trabajo. Fotografiar metodologías que el propio empleado escribió y que por eso da por suyas. Y a veces sin ninguna mala intención: una cuenta en la nube que queda abierta meses después de la salida, porque nadie sabía que existía.

Así se cierra. Seis pasos:

1. El día del aviso es el día del reporte. La carta de renuncia llega al oficial de seguridad y al departamento de informática ese mismo día. No al final de la semana, no después de fijar una fecha.

2. Mapeo inmediato de accesos. A qué sistemas, bases de datos y carpetas tiene acceso el empleado, y cuáles de ellos son especialmente sensibles a la luz del lugar al que se va.

3. Reducción gradual. Lo que no se necesita para el traspaso se cierra ahora, no el último día.

4. Control de la ventana. Descargas de volumen inusual, envíos al correo personal, conexión de dispositivos portátiles. En el período de la ventana esto no es desconfianza, es el punto débil más conocido.

5. Tareas para el último día. Una lista cerrada de cuentas por desactivar, incluidos sistemas en la nube y proveedores externos que no están conectados a la gestión central de usuarios. Esos son los que siempre se olvidan.

6. Una entrevista de salida ordenada. Un recordatorio de las obligaciones de confidencialidad y propiedad intelectual, y una conversación abierta sobre el siguiente destino. No por desconfianza, por gestión de riesgos.

El departamento de reclutamiento sabe exactamente cuándo entra un empleado en la organización. La pregunta es quién se hace cargo del momento en que sale.