Lista de protección contra ransomware

- [ ] Hay al menos una copia de los datos críticos que no se puede borrar desde la red de trabajo, ni siquiera con permisos de administrador.
- [ ] En el último trimestre has restaurado al menos un sistema crítico desde la copia y has apuntado cuántas horas tardó.
- [ ] El MFA está activado para todos en correo, VPN y paneles en la nube, sin excepciones para la dirección.
- [ ] RDP y otros servicios de acceso remoto no están expuestos directamente a internet.
- [ ] Los equipos del perímetro (VPN, cortafuegos, router) tienen el firmware al día y hay una persona responsable.
- [ ] Solo tiene permisos de administrador quien los necesita, y la administración se hace con cuentas separadas.
- [ ] El equipo sabe dónde avisar de un correo sospechoso, y se ha comprobado con una simulación de phishing.
- [ ] El plan de respuesta con los teléfonos del proveedor de TI, el abogado, la policía y el CERT nacional está impreso.
- [ ] Los accesos de tu proveedor de TI están identificados, limitados y protegidos con MFA.

¿Quiere repasar esta lista conjuntamente? Escríbanos y revisaremos su alcance.
veiltrack.io/es/contact