Ciberconsejos para empresas, estudios, escuelas y cooperativas

Definí un responsable de seguridad de la información
Aunque la ley no te exija un CISO o DPO aún, alguien tiene que coordinar políticas, incidentes y relación con proveedores.
Si nadie es responsable, en la práctica
nadie se ocupa.

Capacitá a tu equipo de forma periódica.

El eslabón más débil suele ser humano. Hacé talleres breves sobre phishing, uso seguro del correo, manejo de datos personales y reporte de incidentes. La repetición construye hábitos.

Clasificá la información y restringí accesos.

No todas las personas necesitan ver todo.

Definí qué es público, interno y confidencial, y limitá accesos según el rol. Menos accesos innecesarios = menos riesgo.

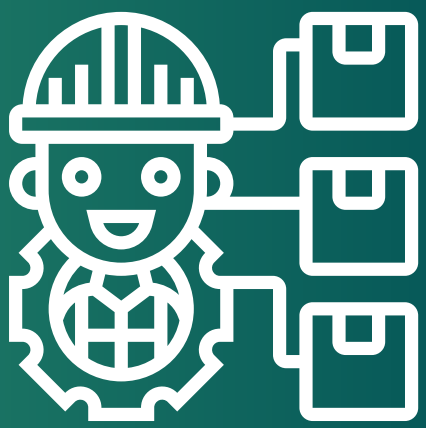
Documentá políticas de uso aceptable de tecnología

Dejá por escrito qué se puede y qué no se puede hacer con dispositivos, correo, nube y mensajería.

Ordena internamente y sirve como respaldo jurídico frente a conflictos.

Gestioná bien a proveedores y terceros Plataformas de e-learning, marketing.

RRHH o nube también manejan datos de tus clientes y empleados. Firmá acuerdos de confidencialidad, revisá sus medidas de seguridad y su cumplimiento normativo.

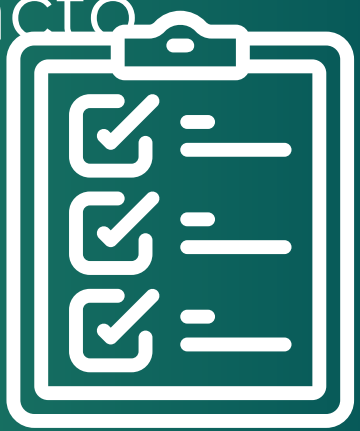


De la reacción a la prevención

Tené un plan de respuesta ante incidentes

No se trata de “si me atacan”, sino de “cuándo”.

Definí a quién avisar, cómo aislar sistemas, cómo comunicar a clientes y cómo documentar el incidente para cumplir con la normativa y reducir impacto reputacional.



Realizá copias de seguridad probadas y fuera de línea.

Hacer backup no alcanza: hay que probar regularmente que se pueda restaurar.

Mantené al menos una copia desconectada o en un entorno separado para resistir ransomware.

Revisá contratos, avisos de privacidad y consentimientos

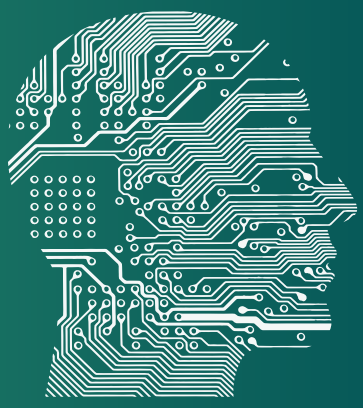
Alineá la práctica real (formularios, CRM, apps) con lo que prometés en tus textos legales.

No sirve una política perfecta en papel si en la operación diaria se hace otra cosa.

Regulá el uso de herramientas de IA en la organización

Definí reglas claras para que el personal no copie en chatbots documentos internos, datos de clientes o código fuente.

La “Shadow AI” puede filtrar información valiosa sin que nadie se dé cuenta.



Medí y mejorá: la ciberseguridad es un proceso continuo.

Programá revisiones periódicas (checklists, auditorías, asesoría externa) para identificar avances y puntos débiles.

La ciberseguridad no es un proyecto aislado, es una cultura que se construye en el tiempo.