Informática Los Llanos
Pagola & Valderrama Soluciones Informáticas

CIBERSEGURIDAD PARA SU EMPRESA

Por qué un Plan Director marca la diferencia

antes, durante y después de un ataque

La realidad que nadie quiere vivir

Imagine llegar un lunes por la mañana a su oficina y encontrar todos sus archivos cifrados. Sus datos de clientes, sus contratos, sus facturas: inaccesibles. En la pantalla, un mensaje exigiendo dinero para recuperarlos.

No es un escenario de película. Es lo que ocurre cada día en micropymes como la suya. Y la diferencia entre cerrar el negocio o recuperarse en pocos días no depende de la suerte: depende de si tenía un plan.

Lo que dicen los datos

70% de los ciberataques en España afectan a pymes y micropymes.

20.000 € es el coste medio de un incidente para una pequeña empresa, sin contar daño reputacional.

72 horas es el plazo máximo legal para notificar una brecha de datos a la AEPD. El incumplimiento acarrea sanciones.

ANTES del ataque: la preparación lo es todo

La mayoría de micropymes no descubren que no estaban preparadas hasta que el incidente ya ha ocurrido. Para entonces, es demasiado tarde para muchas cosas.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

Sin un Plan Director

- No sabe exactamente qué información tiene ni dónde está almacenada.
- No ha evaluado qué pasaría si perdiera el acceso a sus sistemas durante una semana.
- Sus empleados no saben reconocer un correo fraudulento ni qué hacer si hacen clic en uno.
- Sus copias de seguridad no se han probado nunca: puede que no funcionen cuando las necesite.
- No tiene claro qué obligaciones legales debe cumplir en materia de protección de datos.

Con un Plan Director

- Tiene un inventario de todos sus activos de información y sabe cuáles son críticos.
- Ha identificado los riesgos más probables y ha tomado medidas para reducirlos.
- Sus empleados conocen las normas básicas y saben cómo actuar ante una amenaza.
- Sus copias de seguridad se realizan y verifican periódicamente: funcionarán cuando las necesite.
- Tiene activada la autenticación en dos pasos (MFA) en todas las cuentas críticas.
- Conoce sus obligaciones legales y tiene documentación que lo demuestra.

> **Un dato clave sobre la prevención**
>
> La mayoría de los controles más importantes tienen coste cero: activar MFA, cifrar el disco del portátil, configurar copias de seguridad automáticas. Lo que requieren es tiempo y conocimiento. Precisamente lo que un Plan Director proporciona.

DURANTE el ataque: la respuesta ordenada salva el negocio

Cuando un ataque ocurre, los primeros minutos son decisivos. Las decisiones que se toman en ese momento determinan si el daño se contiene o se multiplica.

Sin un Plan Director

- Pánico generalizado: nadie sabe exactamente qué hacer ni en qué orden.
- Se apagan los equipos por instinto, destruyendo evidencias que podrían permitir la recuperación.
- El ataque se propaga a otros equipos de la red porque no se actúa con rapidez suficiente.
- Se pierde tiempo valioso buscando a quién llamar y qué pasos seguir.
- Las decisiones de comunicación se toman sin criterio, pudiendo agravar el daño reputacional.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

Con un Plan Director

- Cada persona sabe su rol: quién toma decisiones, quién contiene el incidente y quién comunica.
- La respuesta es inmediata: desconexión de la red sin apagar, aislamiento de equipos afectados.
- Se preservan las evidencias que pueden permitir la recuperación sin pagar rescate.
- Se evalúa rápidamente si hay datos personales afectados y se activa el protocolo legal.
- Se contacta con INCIBE (017) con información clara y estructurada sobre lo ocurrido.

> ⚠ **La regla más contraintuitiva**
>
> **Ante un ransomware activo:** desconecte el equipo de la red inmediatamente, pero no lo apague. La memoria RAM puede contener la clave de cifrado u otras evidencias que desaparecen al apagar y que un especialista podría usar para recuperar sus datos sin pagar. Este tipo de conocimiento es el que marca la diferencia entre recuperarse o no.

DESPUÉS del ataque: recuperarse y aprender

La fase posterior a un incidente es donde se juega la supervivencia del negocio a medio plazo. Un incidente mal gestionado puede hundir una empresa que técnicamente sobrevivió al ataque.

Sin un Plan Director

- No tiene copias de seguridad válidas o no sabe cómo restaurarlas: los datos se pierden.
- Desconoce si hay datos personales afectados ni qué debe comunicar a la AEPD.
- No puede demostrar a sus clientes que ha actuado con diligencia.
- El negocio puede estar semanas sin operar mientras intenta reconstruir desde cero.
- Paga el rescate sin garantía de recuperar nada, y se convierte en objetivo conocido para futuros ataques.

Con un Plan Director

- Restaura desde la copia de seguridad más reciente, verificada y protegida.
- Notifica a la AEPD dentro del plazo de 72 horas con la documentación preparada.
- Puede demostrar a clientes y reguladores que disponía de controles adecuados.
- Identifica la causa raíz del incidente y cierra la vulnerabilidad antes de reconectar.
- Documenta lecciones aprendidas que hacen a la empresa más resiliente frente a futuros ataques.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

¿Qué impacto real tiene en su empresa?

Un incidente de ciberseguridad no es solo un problema tecnológico. Tiene consecuencias en cuatro dimensiones que afectan directamente a la viabilidad del negocio:

Impacto económico

Rescates, recuperación de sistemas, horas sin facturar, contratación de especialistas externos, posibles sanciones de la AEPD de hasta 20 millones de euros o el 4% de la facturación global anual.

Impacto legal

Obligación de notificar brechas de datos a la AEPD en 72 horas. Responsabilidad frente a clientes cuyos datos hayan sido comprometidos. Incumplimiento del RGPD con consecuencias administrativas y civiles.

Impacto reputacional

Los clientes que pierden la confianza tras un incidente raramente vuelven. La percepción de negligencia puede ser más dañina que el propio ataque, especialmente en sectores donde la confidencialidad es clave.

Impacto operativo

Un ransomware puede paralizar la actividad durante días o semanas. Sin un plan de continuidad, cada hora sin operar es pérdida directa y daño acumulado difícil de cuantificar.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

El Plan Director: su seguro de vida empresarial

Un Plan Director de Ciberseguridad no garantiza que nunca le vayan a atacar. Ninguna medida puede garantizarlo. Lo que sí garantiza es que cuando ocurra algo, usted sabrá qué hacer, habrá minimizado el daño posible y podrá demostrar que actuó con la diligencia debida.

Es además un documento vivo: se revisa, se actualiza y mejora con cada incidente y con cada cambio en su negocio. No es un proyecto puntual, sino una forma de gestionar su empresa de manera más inteligente y segura.

Lo que incluye un Plan Director básico para su micropyme:

- Inventario de activos: saber qué tiene y qué valor tiene para su negocio
- Análisis de riesgos: identificar qué puede fallar y con qué consecuencias
- Controles técnicos básicos: MFA, cifrado, backups verificados, actualizaciones
- Políticas claras para sus empleados: qué pueden y qué no pueden hacer
- Procedimiento de respuesta ante incidentes: qué hacer si algo sale mal
- Cumplimiento legal: RGPD, notificación a la AEPD, derechos de los afectados

¿Listo para proteger su negocio?

Le ayudamos a elaborar su Plan Director de forma sencilla, adaptada a su empresa y sin necesidad de conocimientos técnicos previos.

Informática los Llanos SL – 948 555 339 – tecnico@informaticalosllanos.com

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com