

MAS VALE PREVENIR... QUE LAMENTAR

Muy [Sr@s nuestr@s](mailto:Sr@s_nuestr@s):

Agradecemos sobremanera el tiempo que dedican a leer estas líneas. **Confiamos en que podremos aportarles interesante información para el progreso de su compañía.**

Probablemente su empresa y actividad, en buena medida, depende directa o indirectamente de la gestión informática, programas y datos almacenados.

El 92% de los empresarios Españoles reconocen que un incidente informático en sus sistemas de gestión supondría una paralización parcial o total de su actividad productiva y/o comercial. Por contra, solo el 11% de las PYMES tienen un conocimiento exhaustivo de los riesgos y vulnerabilidades que existen en su sistema informático.



- ¿ Conocen Ustedes el grado de seguridad y vulnerabilidad de sistema informático y telecomunicaciones ?
- ¿ Tienen valorado el riesgo de una perdida parcial o total de datos ?
- ¿ Tienen un plan de contingencias en caso de incidencia grave o bloqueante ?
- ¿ Que pérdida económica supondría cada día por falta de acceso a sus programas y datos informáticos ?

Estas y otras preguntas forman parte del análisis de riesgos informáticos que podemos realizar para su compañía. **Tras nuestro diagnóstico ustedes tendrán una visión completa de las vulnerabilidades y riesgos existentes en sus sistemas de gestión y protección de datos.**

Ponemos a su disposición un servicio de análisis de riesgos informáticos, de fácil aplicación y reducido costo, que les permitirá tener el control en la toma de decisiones para la aplicación de medidas de seguridad. Nuestro informe incluye las recomendaciones personalizadas que le sugeriremos acometer para minimizar riesgos y garantizar la continuidad de su actividad empresarial.

Acompañamos en páginas posteriores un esquema de los elementos que podemos analizar así como el modelo de resultados que entregaremos tras nuestro análisis.

Si lo desean podremos atenderles y ampliar información telefónica, a través de correo electrónico o en sus propias instalaciones mediante visita personal.

Quedando a su entera disposición, reciban un afectuoso saludo.

Atte.

Dpto. Comercial
comercial@ingenium2000.com

Elementos Analizados

El trabajo de análisis y diagnóstico cubre las áreas indicadas en la siguiente tabla:

Análisis	Estándar
Contexto de la organización: <ul style="list-style-type: none">• Ubicaciones• Organigrama interno• Relación con entidades externas	S S S
Seguridad física de la infraestructura <ul style="list-style-type: none">• Acceso físico a la infraestructura informática	S
Inventario de: <ul style="list-style-type: none">• Puestos de trabajo• Servidores• Aplicaciones• Protocolos• Servicios	S S S S S
Gestión de datos <ul style="list-style-type: none">• Sistemas de almacenamiento• Política de copias de seguridad	S S
Infraestructura de comunicaciones <ul style="list-style-type: none">• Topología interna• Puntos de acceso• Conexiones	S S S
Seguridad de redes <ul style="list-style-type: none">• Accesos internos• Accesos remotos	S S
Seguridad del usuario <ul style="list-style-type: none">• Sistemas de autenticación• Políticas de gestión de credenciales	S S
Presentación de informe in-situ	S
Medidas correctoras: <ul style="list-style-type: none">• Recomendación• Implantación• Control	S O O

Tabla 1: Aspectos cubiertos en el análisis de seguridad (S: Sí; O: Opcional)

¿ Que obtendrán del informe de resultados ?

El informe detallará cada uno de los aspectos analizados, identificando:

- **Los puntos débiles y los puntos fuertes detectados en cada área.**
- **La clasificación de cada uno de los hallazgos en función del nivel de riesgo que pueden representar para la continuidad de su negocio.**
- **Guía de recomendaciones para que sus proveedores habituales de informática implementen las medidas correctoras necesarias.**

Prestación del servicio

A partir de la confirmación y encargo de los servicios, les remitiremos firmado un acuerdo de confidencialidad con el que garantizamos que todo el análisis y resultados serán tratados única y exclusivamente con la persona que ustedes designen como intermediario de las comunicaciones.

Nuestros técnicos pactarán una visita a sus instalaciones en las fechas y horarios mas convenientes para ustedes. Para la realización del análisis los técnicos utilizarán equipos y herramientas de chequeo y verificación, pero en ningún caso se realizarán copias o accesos a los datos del cliente. La analítica se focaliza en la evaluación de vulnerabilidades e integridad de sistemas y datos, sin entrar a valorar o analizar el contenido de los ficheros analizados.

Los informes de resultados le serán entregados en documento confidencial en un plazo aproximado de 7 días tras el análisis. Si posteriormente ustedes desean ampliar servicios para que sean nuestros técnicos los que apliquen medidas correctoras pondremos nuevamente a su disposición un proyecto personalizado y el plan de implementación posible.

OFERTA 2018 – Ecija y Comarca

- Análisis Estándar.- 190 euros. + iva (para 5 equipos)
- Puesto adicional.- 15 euros + iva

NOTA: Para empresas se hallen envueltas en contingencias o incidentes informáticos graves también disponemos de un servicio de recuperación de datos e intervención ante situaciones graves o bloqueantes.