CIBER PROTECCIÓN

En un mundo totalmente dependiente de la tecnología y los sistemas de información, los ciber riesgos constituyen una de las tres principales amenazas para empresas, gobiernos e instituciones.

El equipo de Riskmedia junto a sus partners tecnológicos, legales, y aseguradores, consumados especialistas en sus respectivas disciplinas, hemos unido nuestros esfuerzos, conocimientos y experiencias, creando una solución integral para hacer frente a estas amenazas.

Gracias al estudio de los siniestros que hemos gestionado, contamos con una posición privilegiada para identificar y anticipar tendencias y valorar su impacto, con atención y gestión de siniestros e incidencias 24/7.

Nuestra solución 360, se articula en base a TRES bloques:

- *PREVENCIÓN*
- *PROTECCIÓN*
- *GESTIÓN DE INCIDENCIAS*

www.riskcyber360.com

RISKMEDIA
CYBER360

PREVENCIÓN:

- Identificación de riesgos.
- Formación y concienciación en materia de ciberseguridad: el usuario es el eslabón más débil.
- Auditoría de sistemas y procedimientos de seguridad.
- Test de intrusión: analiza tu infraestructura.
- Servicios de SOC- Security Operations Center.
- Control de Endpoint.
- Chequeo de cumplimiento con legislación en la materia.
- Análisis forense de ciberseguridad.
- Protección de negocio, continuidad de negocio, plan de contingencias, y Cloud empresarial.

PROTECCIÓN: ***SEGURO DE CIBER RIESGOS***

Protege a las empresas ante el perjuicio económico producido por un incidente en sus sistemas de información o recursos informáticos. Además, garantiza los servicios de Contención tecnológica y primera respuesta, ante un incidente desde el primer momento.

RIESGOS Y ASEGURAMIENTO:

- Ciberataques de cualquier tipo
- Robo o pérdida de datos personales.
- Virus informático.
- Uso no autorizado de los sistemas de información.
- Fallo o subida del suministro eléctrico.
- Incidentes del proveedor de servicios tecnológicos.
- Actos malintencionados por terceros o empleados.
- Error humano.
- Actos tecnológicos incorrectos.
- Actos fraudulentos.

CONSECUENCIAS:

Daños propios:

- Gastos de recuperación de datos.
- Incremento del coste de explotación.
- Gastos de rehabilitación de imagen pública por pérdida de reputación.
- Honorarios de consultores especializados (informática forense, Legal,…).
- Descontaminación de virus informáticos.
- Pérdida de Beneficios.
- Coste de investigación e indagación.
- Costes de notificación.
- Carencia de proveedor de servicios informáticos.
- Multas y sanciones interpuestas por la Agencia de Protección de Datos.
- Ciber Delito: Suplantación de identidad/Fraude en transferencias de fondos.
- Extorsión cibernética.
- Modificación de precios on line .
- Hacking Telefónico.

Daños a Terceros:

- Vulneración de los derechos de propiedad intelectual.
- Vulneración de la integridad o divulgación de datos de carácter personal.
- Vulneración del derecho a la intimidad de las personas.
- Transmisión de virus informáticos.
- Delitos contra el honor, injurias y calumnias.
- Constitución de fianzas civiles.
- Gastos de defensa.

GESTIÓN DE INCIDENCIAS:

- Servicios de primera respuesta y contención tecnológica.
- Servicio de informática forense.
- Identificación de la posible violación de seguridad de los datos.
- Proceso de recuperación de datos.
- Notificaciones a afectados.
- Gestión de reclamaciones de terceros.
- Expediente de pérdida de beneficios.
- Consultoría de imagen.
- Defensa, asesoramiento y negociación frente a extorsión.
- Pago de indemnizaciones.
- Atención de incidencias 24/7

CYBER RISKS