Seguro de ciberriesgo Empresas – Servicios preventivos

En la era digital actual, la protección contra ciberataques no es solo una opción, es una necesidad. Cada día, se detectan millones de intentos de ciberataques en todo el mundo. Según el balance de Incibe (Instituto Nacional de ciberseguridad), en 2023, se incrementaron un 24% los incidentes de ciberseguridad. **22.000 empresas españolas** se vieron afectadas por incidentes cibernéticos.

En este entorno, es necesario estar siempre al lado de nuestro cliente industrial, protegiéndole diariamente. De esta forma, nuestra póliza de ciberriesgo no solo te ofrece cobertura en el momento del siniestro, sino que también proporciona **servicios de protección desde el minuto uno de la contratación**.

Desde el primer día, el cliente tendrá acceso a herramientas y recursos diseñados para fortalecer su seguridad cibernética y minimizar los riesgos. Ofreciéndole una cobertura integral que protege su negocio contra una amplia gama de amenazas cibernéticas, incluyendo ataques de malware, ransomware y violaciones de datos.

Nos enfocamos en la prevención proactiva, ofreciendo servicios de monitoreo continuo y evaluaciones de vulnerabilidad para identificar y mitigar riesgos antes de que se conviertan en problemas.

A continuación, detallamos los servicios que brindamos al cliente al contratar nuestra póliza de ciberriesgo. Estos servicios se brindan en colaboración con nuestro proveedor tecnológico externo, **Lazarus Technology**, reconocido por su experiencia y eficacia en el campo de la ciberseguridad.

Todos estos recursos están diseñados para ofrecer al cliente una protección completa y una tranquilidad total desde el primer momento.

1. Servicios de Infraestructura

Análisis de vulnerabilidades de la conexión	Se analiza la conexión a Internet, ya sea a través de un dispositivo móvil o un equipo conectado a Internet.
Corrección de vulnerabilidades	Un especialista analiza los resultados del análisis de vulnerabilidades y si existen nos ayudará a solucionarlas.
Análisis de la página web	Se analiza si las páginas web están expuestas a algún ciberataque y en caso afirmativo, se propondrán medidas preventivas de mejora
Análisis tecnológico de tus dispositivos,	Se revisarán todas las vulnerabilidades de los equipo y se establecerán los mecanismos necesarios para navegar por internet de una manera más segura.

2. Ransomware

El ransomware es un tipo de malware que cifra los archivos y la información del sistema informático, no permitiendo al usuario acceder a sus datos (archivos, fotos, etc.) para luego pedir el pago de un rescate a cambio de devolver el acceso a los mismos.

Para protegernos del mismo, se facilita la posibilidad de la **instalación de una aplicación** que bloqueará proactivamente la instalación de ransomware o el secuestro información, para que los equipo tenga seguridad contra este ataque. (La aplicación es valida exclusivamente para Windows).

3. Vigilancia digital

Análisis en la Internet Abierta	Se buscará en Internet la información pública sobre el tomador, la empresa y empleados, con el fin de evaluarla.
Análisis en Deep y Dark Web,	Se buscará en la Deep y dark web, la información disponible sobre el tomador, la empresa y empleados, con el fin de evaluarla
Análisis de credenciales	Se analizarán las cuentas de los usuarios, para comprobar si están en riesgo de quebrantamiento o usurpación.

4. Compliance

Evaluación LOPD\GDPR	Se evaluará el grado de adaptación de la empresa al Reglamento General de Protección de Datos (RGPD).
Adaptación de la empresa a la LOPD	Se ayudará a la empresa a cumplir con la legislación vigente en materia de protección de datos.