Digitalización e Interconexión

El proceso de digitalización e interconexión en los negocios a través de tecnología basada en internet y otros sistemas de comunicación se ha incorporado en las operaciones (comercio electrónico, producción, logística, suministros), los servicios y soporte a clientes y en la gestión y control interno de las diferentes áreas de las Organizaciones. Todo ello con el desarrollo de soluciones de software, aplicaciones de comunicación y distribución / acceso a información, la robotización de las industrias y multitud de soluciones para una interconexión creciente y exponencial.

Estas soluciones permiten una mejora de la eficiencia de las Organizaciones y una mejora sustancial de la experiencia de marca y las funcionalidades a las que tienen acceso los clientes. Todo ello está generando una optimización y reducción de costes, al mismo tiempo que la mejora de la fidelización y desarrollo de negocio.

CiberRiesgos

Todo el desarrollo tecnológico y las constantes y crecientes innovaciones en digitalización e interconexión llevan asociados nuevos retos y responsabilidades en el ámbito de la ciberseguridad y en la privacidad / protección de la información.

Los ciberataques pueden causar daños económicos, reputacionales y generar posibles responsabilidades frente a terceros y/o las autoridades. Este ámbito de riesgos debe ser contemplado por aquellas entidades especialmente vulnerables, como pueden ser las que disponen de soluciones de comercio electrónico, procesos de producción y operaciones fuertemente automatizados y/o interconectados, y todas aquellas con información asociada a altos deberes de privacidad / protección.

Los ciberdelincuentes disponen de multitud de herramientas y recursos para aprovechar los fallos y vulnerabilidades de seguridad, especialmente en dispositivos de menor nivel de protección, junto con mecanismos de engaño y suplantación de identidad para realizar ciberataques a través de los usuarios.

Como resultado de la alta interconexión y comunicación a través de dispositivos digitales, los ciberataques tienen repercusión entre Organizaciones, donde la vulnerabilidad de una Organización puede ser utilizada para realizar ataques a otras Organizaciones o personas relacionadas con esta, pudiendo generar riesgos y responsabilidades más allá de la propia Organización.

CiberSeguridad

Por todo lo anterior, es necesario que toda Organización implante un plan de ciberseguridad adaptado a su riesgo y al nivel de automatización, digitalización e interconexión de sus actividades y operaciones para así prevenir y mitigar las implicaciones de un posible ciberataque, entre las cuales destacan:

- La prevención de riesgos de carácter reputacional y valor de marca.
- La prevención de costes y pérdidas de ingresos como consecuencia de un ciberataque.
- Las responsabilidades y deberes de carácter legal en relación con el deber de protección de datos e información confidencial.
- Las responsabilidades contractuales con clientes en materia de garantía del servicio y de seguridad y protección de la información.

Desde BONET consulting, con la colaboración de Profesionales en materia de seguridad y corredores especializados en diseño de seguros en el ámbito de las responsabilidades frente a los CiberRiesgos, hemos desarrollado un plan de soporte global en materia de CiberSeguridad adaptable a la estrategia y riesgos de la Entidad. Asimismo, como elemento de valor de marca y confianza para clientes y colaboradores de la Entidad, disponemos, dentro de nuestra área de certificaciones de *compliance*, el **Certificado "Ciber Risk Care"**, que acredita (a nivel interno y externo) el compromiso y responsabilidad de la Entidad en disponer de un sistema para la prevención y gestión de los CiberRiesgos que detalla los elementos fundamentales del mismo.

Quedamos a su disposición para comentar las implicaciones y recomendaciones de todo lo mencionado anteriormente para su Entidad.

Atentamente.

BONET consulting