Política de Seguridad

IVC basa su actividad en el tratamiento de diferentes tipos de datos e información, ello le permite ejecutar procesos básicos propios del negocio. Los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyen el activo principal de IVC, de tal manera que el daño o pérdida de los mismos inciden en la realización de sus operaciones y pueden poner en peligro la continuidad de la organización.

Para que esto no suceda se ha diseñado una Política de Seguridad de la Información cuyos fines principales son:

- **Proteger**, mediante controles/medidas, **los Procesos/activos** frente a amenazas que puedan derivar en incidentes de seguridad.
- **Paliar** los efectos de **los incidentes** de seguridad.
- **Establecer** un sistema de **clasificación de la información** y los datos con el fin de proteger los Procesos/activos críticos de información.
- **Definir las responsabilidades** en materia de seguridad de la información generando la estructura organizativa correspondiente.
- **Elaborar** un conjunto de **reglas, estándares y procedimientos** aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- **Especificar** los efectos que conlleva el **incumplimiento** de la Política de Seguridad en el ámbito laboral.
- **Evaluar los riesgos** que afectan a los Procesos/activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- **Verificar** el funcionamiento de **las medidas/controles de seguridad** mediante auditorías de seguridad internas realizadas por auditores independientes.
- **Formar a los usuarios en la gestión de la seguridad** y en tecnologías de la información y las comunicaciones.
- **Proteger a las personas** en caso de catástrofes naturales, incendios, inundaciones, ataques terroristas, etc., mediante planes de emergencia.
- **Controlar el tráfico de información y de datos** a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- **Observar y cumplir la legislación** en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los Procesos/activos de IVC.
- **Garantizar un servicio eficiente a nuestros clientes** con un alto nivel de calidad, preservando así su confianza.
- **Proteger el capital intelectual de la organización** para que no se divulgue ni se utilice ilícitamente.
- **Obtener las evidencias** que permitan acreditar los incidentes de seguridad y la identificación de su autor.
- **Reducir** las posibilidades de **indisponibilidad** a través del uso adecuado de los Procesos/activos de la organización.
- **Defender los activos** ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- **Controlar el funcionamiento de las medidas de seguridad** averiguando el número de incidencias, su naturaleza y efectos.