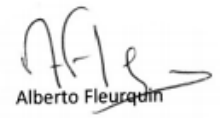
Política del Sistema de Gestión de Seguridad de la Información - SGSI

Multiline, empresa dedicada al Outsource de Contact Centers y Servicios BPO, para pymes y grandes empresas, nacionales e internacionales, ha decidido implantar un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001 con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información, proteger a ésta de un amplio grupo de amenazas y destinado a asegurar la continuidad de las líneas de negocio, minimizando los daños y maximizando el retorno de las inversiones, de las oportunidades de negocio y la mejora continua.

La Dirección de **Multiline** es consciente de que la información es un activo que tiene un elevado valor para la Organización y requiere por tanto una protección adecuada. Por ello establece los siguientes objetivos de seguridad y compromisos como punto de partida:

- La protección de los datos de carácter personal y la intimidad de las personas.
- La salvaguarda de los registros de la organización.
- La protección de los derechos de propiedad intelectual.
- La documentación de la política de seguridad de la información.
- La asignación de responsabilidades de seguridad.
- La formación y capacitación para la seguridad de la información.
- El registro de las incidencias de seguridad.
- La gestión de la continuidad del negocio.
- Controlar el acceso físico y lógico de nuestras instalaciones, Sistemas y Aplicaciones.
- Mantenimiento preventivo de nuestros activos.
- Contar con una infraestructura tecnológica que está planificada y dimensionada de acuerdo a los estándares y normas más exigentes.
- Comunicación eficiente, significa, contar con herramientas y componentes tecnológicos que facilitan la operativa, minimizan los costos y optimizan los tiempos de respuesta frente a cambios operativos y/o de negocio.
- La gestión de los cambios que pudieran darse en la empresa relativa a la seguridad
- Desarrollar servicios conformes con los requisitos de nuestros clientes y demás partes interesadas.
- Definir los requisitos de formación en seguridad y proporcionarla según corresponda.
- Prevención y detección de virus y otro software malicioso, mediante el desarrollo de políticas específicas y el establecimiento acuerdos contractuales con organizaciones especializadas.
- Gestión de la continuidad del negocio, desarrollando planes de continuidad conformes a metodologías de reconocido prestigio internacional.
- Establecimiento de sanciones derivadas de las violaciones de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y subcontratistas.
- Actuar en todo momento dentro de la más estricta ética profesional.
- Esta Política proporciona el marco de referencia para la mejora continua del Sistema de Gestión de Seguridad de la Información la misma es comunicada a toda la Organización a través de los medios previstos y es revisada anualmente para su adecuación y extraordinariamente cuando concurran situaciones que lo ameriten.



Director

Montevideo, 03 de mayo 2024.