[Políticas de Seguridad]

Código	PS Políticas de Seguridad
Versión	06
Fecha Versión	07-10-2024
Creado por	José Enrique de Juan
Aprobado por	Antonio Huedo
Nivel Confidencialidad	Público

HISTORIAL DE CAMBIOS

Fecha Versión	Versión	Descripción de Modificaciones
01-10-2012	01	Primera versión del documento.
26-12-2012	02	Se incluye el Alcance del SGSI
09-04-2013	03	Se modifica Alcance del SGSI, conforme a la redacción del certificado de AENOR.
23-12-2015	04	Se incluyen las siguientes políticas de seguridad: - política de puesto despejado pantalla limpia - política de desarrollo seguro - política de seguridad de la información en las relaciones con los proveedores Se crea una Política de Seguridad de la Información General
03-12-2021	05	Nueva denominación de la compañía.
07-10-2024	06	Adaptación a nueva versión de ISO 27001 y eliminación de NR inexistentes

TABLA DE CONTENIDOS

1. OBJETO

El objeto del presente documento es la definición de un marco para la fijación de objetivos, estableciendo una orientación general sobre las directrices y principios de actuación en relación con la seguridad de la información y el alcance del Sistema de Gestión de Seguridad de la Información de ACTIONS.

2. ALCANCE DEL SGSI

El Alcance del SGSI desarrollado por ACTIONS contempla, los sistemas de información que dan soporte a las actividades de: Diseño, Desarrollo, Prestación, gestión y mantenimiento de servicios avanzados de marketing. La creación o adquisición de Bases de Datos de particulares, profesionales y empresas. El Análisis de los datos recabados o suministrados de Bases de Datos de particulares, profesionales y empresas. El Diseño y desarrollo de software de aplicación en entorno web y cliente/servidor adaptado para la realización de dichas acciones, según la vigente declaración de aplicabilidad.

3. POLÍTICA DE SEGURIDAD

3.1. Estrategia de la Dirección.

La Dirección ha definido y documentado esta Política de Seguridad asegurando que:

- Es adecuada al propósito de la Organización.
- Incluye el compromiso de cumplir con los requisitos de los clientes y requisitos legales en materia de seguridad de la información
- Mantener un compromiso de mejorar continuamente la eficacia del Sistema de Gestión
- Proporciona un marco de referencia para establecer y revisar los objetivos.
- Garantizar la confidencialidad, integridad y disponibilidad de la información, analizando y controlando los riesgos asociados a los activos, proponiendo los planes de tratamiento necesarios para la minimización de los mismos.
- Se comunica a todos los empleados de ACTIONS y a las personas que trabajan en su nombre.

ACTIONS tiene en cuenta sus requisitos de actividad empresarial, los requisitos legales y las obligaciones de seguridad contractuales para la definición de sus políticas.

Las Políticas de ACTIONS, están alineadas con el contexto de la estrategia de gestión de riesgos de la organización.

La política de ACTIONS se establece según los criterios de estimación de riesgos de la organización.

La Dirección de ACTIONS procede al establecimiento y aprobación de Políticas de obligado cumplimiento tanto para el personal de la empresa, como para todos los que colaboren con ella. De este modo, la empresa pretende establecer las medidas y la seguridad de la información adoptadas.

3.2. Objetivos de la Política de Seguridad

Los objetivos sobre los que se sustenta la Política de Seguridad, se centran en los siguientes principios:

- Cumplimiento de las normativas legales y otros requisitos de los clientes relacionados con la seguridad de la información que puedan surgir.
- Cumplimiento de requisitos para futuras contrataciones con Administraciones Públicas u organizaciones privadas para prestar nuestros servicios.
- Mejora continua de los procedimientos, de los procesos de seguridad y de nuestros propios servicios ofrecidos al cliente.
- Asegurar la confidencialidad, disponibilidad e integridad de la información generada para llevar a cabo nuestros servicios bajo un SGSI.
- Adaptar la empresa a la evolución tecnológica.
- Analizar y planificar la reducción del riesgo de pérdida, robo o revelación de información.

3.3. Políticas de Seguridad

3.3.1. Política de Seguridad General (NR-01)

La Política de Seguridad mantiene las directrices a seguir en ACTIONS para definir de forma genérica las normas de orden interno relacionadas con todos y cada uno de los aspectos contemplados dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

3.3.2. Política de Usuarios (NR-02)

Se incluye en esta política un extracto de la normativa de seguridad establecida por ACTIONS, que contenga todos aquellos aspectos relevantes que atañen directamente y que deben conocer tanto el personal propio de la Organización como externo a la misma, que trate dicha información y/o los activos que la soportan.

3.3.3. Política de Clasificación, Tratamiento de Información y Gestión de Activos de la Información Confidencial (NR-03)

La presente norma pretende establecer los criterios bajo los que se deberá gestionar y clasificar tanto la información de ACTIONS como los demás activos que las mantienen y soportan con el fin mantener el control sobre los mismos y poder aplicar distintos niveles de protección en base a la clasificación realizada. Por otro lado, también pretende fijar las medidas de seguridad a aplicar para el tratamiento (envío, entrega, lugar de almacenamiento, cifrado, retención y destrucción) de la información de ACTIONS en base a la clasificación de seguridad que se haya establecido en cada caso. Estas medidas se aplicarán a lo largo de todo el ciclo de vida de la información e incluyen aquellas relativas al almacenamiento, intercambio, traslado, retención y destrucción de la información.

3.3.4. Política de seguridad de la información en las relaciones con los proveedores (NR 04)

La Política de seguridad de la información en las relaciones con los proveedores de ACTIONS, tiene como objetivo establecer los acuerdos documentados pertinentes para mitigar los riesgos asociados con el acceso del proveedor a los activos de la organización.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ACTIONS, es una compañía de servicios de marketing dedicada a la obtención, explotación y análisis de datos, con el objetivo de transformarlos en conocimiento de calidad. Un activo imprescindible para las empresas de hoy, por ello, es consciente de la importancia de la seguridad de la información, dada la sensibilidad de la información que maneja en el desarrollo de sus actividades de negocio y asume su compromiso con la misma, siguiendo los criterios establecidos en la Norma de referencia ISO 27001, por lo que la Alta Dirección establece los siguientes principios:

- Velar por garantizar la **satisfacción de nuestros clientes**, incluyendo las partes interesadas en los resultados de la empresa, en todo lo referente a la realización de nuestras actividades y su repercusión en la sociedad.
- Velar por garantizar la seguridad de la información de los sistemas de información de ACTIONS, así como de los sistemas de información que dan soporte a los servicios prestados por ACTIONS a sus clientes.
- Establecer objetivos y metas enfocados hacia la evaluación del desempeño en materia de seguridad de la información, así como a la **mejora continua** en nuestras actividades, reguladas en el Sistema de Gestión que desarrolla esta política.
- Cumplimiento de los requisitos de la **legislación aplicable y reglamentaria** a nuestra actividad, los compromisos contractuales adquiridos con los clientes y todas aquellas normas internas o pautas de actuación a los que se someta ACTIONS.
- Mantenimiento de una **comunicación** fluida tanto a nivel interno, entre los distintos estamentos de la empresa, como con clientes.
- Evaluar y garantizar la **competencia técnica del personal**, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos. Así como, realizar actividades de formación y concienciación en materia de procesos de seguridad de la información para todo el personal.
- Desarrollar un proceso de análisis del riesgo sobre los activos de información y establecer los objetivos de control y los controles correspondientes para mitigar los riesgos detectados.
- Establecer la responsabilidad de los empleados en relación a:
    - reportar las violaciones a la seguridad,
    - preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política

- y cumplir las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.

- Velar por la permanente búsqueda de la mejora continua como elemento fundamental de la seguridad de la información.

Estos principios son asumidos por la Alta Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política de Seguridad de la Información.