POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Responsable de Seguridad de la Información

Contenido

1. CONTROL DE VERSIONES

Número	Fecha	Autor	Comentarios	Revisado por
v.1.0	15/01/2021	Responsable de Seguridad	Versión inicial	Responsable de Calidad
v.1.1	14/04/2021	Responsable de Seguridad	Actualización	Responsable de Calidad

2. INTRODUCCIÓN

En Ingeniería y Soluciones Informáticas, S.L. (en adelante, "ISOIN" o la "Compañía"), la información es un activo fundamental para la prestación de nuestros servicios y la consecución de nuestros objetivos. Existe un compromiso expreso de proteger la disponibilidad, integridad y confidencialidad de la información de forma adecuada contra posibles amenazas, intencionadas o accidentales, como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Esto es lo que conocemos como **seguridad de la información**.

La dirección, ha aprobado, a propuesta del Comité de Seguridad de la Información, la presente Política de Seguridad de la Información (en adelante, también la "Política"), que establece los principios y directrices con los que ISOIN protegerá su información, de conformidad con la normativa aplicable y con sus valores éticos, definidos en el Código de Ético y Normativa Interna, así como lo previsto en otra normativa interna que resulte de aplicación.

ISOIN velará por la protección de la información, independientemente de la forma en la que esta se comunique, comparta, proyecte o almacene (en adelante, la "Información"). Esta protección afecta tanto a la información existente dentro de la organización como a la información compartida con terceros. En este sentido, se entiende por Seguridad de la Información, la salvaguarda y protección de (i) la Información titularidad de la Compañía, con independencia de que se encuentre en sistemas propios o de terceros; y (ii) la información titularidad de terceros, que se encuentre en sistemas de la organización.

A los efectos de la presente Política, se entiende por Sistemas de Información el conjunto de tecnologías o medios tecnológicos que gestionen, almacenen o transmitan Información (incluyendo tecnologías en la nube o similares) necesarios para que la compañía pueda desempeñar sus funciones y logro de sus objetivos.

3. ALCANCE

La presente Política se aplicará a los sistemas de información que dan soporte a la prestación de servicios de consultoría y ejecución de proyectos en los ámbitos de las TIC, la logística y el transporte de acuerdo con los sistemas de aplicabilidad vigente y, vinculará a todo su personal, independientemente de la posición y función que desempeñe.

La aplicación de la Política podrá hacerse extensiva, total o parcialmente, a cualquier otra persona física y/o jurídica vinculada con la organización por una relación distinta de la laboral cuando ello sea posible por la naturaleza de la relación y resulte conveniente para el cumplimiento de la finalidad de aquella.

De conformidad con la presente Política, ISOIN podrá desarrollar procedimientos e instrucciones para implementar y dar cumplimiento a las obligaciones asumidas, así como para adaptar la misma a las diversas legislaciones locales aplicables a la organización.

4. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

La presente Política establece, define y revisa los objetivos encaminados a mejorar la seguridad, entendiéndola como la conservación de la confidencialidad, integridad y disponibilidad de todos los activos de la información, así como de los sistemas que la soportan, que respaldan la consecución de los objetivos del negocio. Estos objetivos se consiguen mediante la aplicación de estándares y buenas prácticas.

ISOIN toma como marco de referencia para sus objetivos de la seguridad de la información:

- Proteger la información, evitando el acceso a personas no autorizadas.
- Cumplir con los objetivos del negocio, legales o reglamentarios y las obligaciones contractuales que sean de aplicación.
- Evaluar los activos de la información para aplicar las medidas técnicas y organizativas adecuadas según los riesgos analizados.
- Promover una cultura de seguridad mediante la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.
- Establecer que todo el personal es responsable de reportar las vulnerabilidades y amenazas a la seguridad, preservar la confidencialidad, integridad y disponibilidad de la información y cumplir con la presente política y demás normativa que la desarrolla.
- Establecer los medios necesarios para garantizar la continuidad de las actividades de la compañía.

5. PRINCIPIOS GENERALES

La consecución de los objetivos descritos en el apartado 4 se articula a través de los siguientes principios generales:

- Clasificación de la Información. La Información se clasificará en función a su valor, importancia y criticidad para el negocio, de forma que las medidas de protección se adecúen al nivel de clasificación de cada activo de información. Del mismo modo, la clasificación de los activos de Información se realizará tomando en consideración los requisitos legales, operacionales y las buenas prácticas y estándares al respecto.

- Uso de los Sistemas de Información. El uso de los Sistemas estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

- Segregación de funciones. Se deberán evitar las concentraciones de riesgos derivados de la ausencia de segregación de funciones y la dependencia unipersonal de funciones críticas para el negocio. En este sentido, se deberán establecer procedimientos formales para controlar la asignación de privilegios a los Sistemas de Información, de forma que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

- Retención de la Información. Se establecerán, cuando resulte necesario o conveniente, períodos de retención de la Información por categorías atendiendo a las necesidades operativas o de cumplimiento regulatorio, así como los correspondientes procedimientos de destrucción de la Información.

- Acceso a la Información por parte de terceros. Se desarrollarán los procedimientos de control de la puesta a disposición y acceso por terceros a la Información relativa a ISOIN o de cualesquiera otros terceros relacionados con la Compañía.

- Seguridad de la Información en los Sistemas. Los entornos de desarrollo y producción se mantendrán en Sistemas independientes. Igualmente, el desarrollo y mantenimiento de los Sistemas de Información deben incluir los controles y registros necesarios para garantizar la correcta implementación de las especificaciones de seguridad.

- Continuidad. Se establecerá un proceso de gestión de continuidad que permita garantizar la recuperación de la Información crítica para la Compañía en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables.

- Cumplimiento. Los Sistemas de Información y comunicaciones de la Compañía deberán estar adecuados de forma permanente a las exigencias de la legislación vigente en todas las jurisdicciones en las que opera, así como a la normativa interna de desarrollo que resulte de aplicación.

6. RESPONSABILIDADES

La responsabilidad de la protección de la Información y de los Sistemas que la tratan, almacenan o transmiten se extiende a todos los niveles organizativos y funcionales de ISOIN, cada uno en la medida que le corresponda, como se detalla a continuación:

6.1. Responsabilidades de los empleados

- Todos los empleados deberán conocer, asumir y cumplir la Política, así como la normativa interna de seguridad y uso de los Sistemas vigentes, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su entorno laboral y debiendo comunicar, con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.

- El uso de los Sistemas o servicios digitales por parte de los empleados, incluyendo expresamente el correo electrónico y los servicios de mensajería instantánea, estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

6.2. Responsabilidades en relación con proveedores y otros terceros

- Los contratos con terceros que impliquen el uso o acceso de estos últimos a la Información, entre los que se encuentran los de prestación de servicios o contratos de externalización, incluirán requerimientos específicos de seguridad relativos a la tecnología y las actividades de aquellos que llevan a cabo dichos servicios.

- En este sentido, los proveedores, el personal subcontratado o cualquier empresa externa que utilice o acceda, de manera potencial o real, a la Información (a través de los Sistemas o de cualquier otro medio, como se expone en el apartado 1), deberán conocer y cumplir la Política en lo que les sea de aplicación, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su relación con la Compañía.

6.3. Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información ejercitará su función de control de manera independiente y es su responsabilidad implementar esta Política y monitorizar su cumplimiento, así como el de todos los requerimientos

derivados de las leyes, normas y buenas prácticas en materia de seguridad de la Información que sean de aplicación. Por ello, es responsable de:

- Implementar una estrategia de seguridad de la Información que vele por el cumplimiento de los principios básicos de esta Política, y en particular que dé cobertura a los siguientes aspectos:
    - un adecuado acceso a la Información, basado en el principio de mínimo privilegio y la aprobación del dueño del activo de Información;
    - una segregación adecuada de roles y funciones en los Sistemas de Información; o una correcta configuración, administración y operación de la infraestructura, servicios y/o del software utilizado en los distintos procesos de negocio desde el punto de vista de la seguridad;
    - una correcta implementación de los requisitos de seguridad durante el ciclo de vida de los Sistemas de Información que dan soporte a los procesos de la Compañía.
    - una adecuada protección de los Sistemas y la Información que soportan frente a amenazas físicas o ambientales, en atención a su criticidad, que permita identificar, evaluar, prevenir y responder a cualquier riesgo que pueda comprometer su seguridad.

- Establecer y revisar los controles correspondientes para asegurar el cumplimiento de esta Política y su normativa de desarrollo, incluyendo los mecanismos organizativos y tecnológicos necesarios para facilitar la monitorización continua de las actividades del acceso y uso de los Sistemas, servicios o Información gestionados por la Compañía.
- Prevenir, detectar y responder ante cualquier incidente en materia de Seguridad de la Información y actuar de acuerdo con lo establecido en el “Procedimiento Notificación Incidentes de Seguridad”.
- Impulsar el desarrollo normativo de la presente Política, mediante los procedimientos o instrucciones que sean necesarios para definir un marco global de actuación de la seguridad de la Información en todos sus ámbitos. Igualmente, deberá revisar, actualizar y comunicar cualquier cambio que derive en variaciones de esta Política.
- Realizar actividades de formación y concienciación en materia de los procesos de Seguridad de la Información.
- Establecer un enfoque de mejora continua.
- Velar por el cumplimiento con la legislación vigente en el ámbito de las competencias que le atribuye la presente Política.

6.4. Comité de Seguridad de la Información

ISOIN cuenta con un Comité de Seguridad de la Información integrado por los Responsables de Seguridad de la Información, RRHH, Administración, Infraestructura y Calidad que tiene por objetivo asegurar que las buenas prácticas sobre la gestión de la seguridad se apliquen de manera efectiva y consistente en la Compañía.

Entre otras funciones, asume la responsabilidad de supervisar la estrategia de seguridad de la Información, incluyendo los planes de gasto, inversión y recursos en seguridad, y coordinar las necesidades de seguridad de la dirección y del negocio.

También deberá informar a través del Responsable de Seguridad de la Información, al menos anualmente, al Director Gerente de ISOIN, sobre el estado de la seguridad, la evolución de las amenazas y el apetito de riesgo, la asignación de los recursos destinados a la seguridad y sobre los incidentes significativos.

7. LIDERAZGO Y COMPROMISO

La Dirección de ISOIN, como Responsable de la Información, se compromete a dotar de aquellos medios y recursos que sean necesarios para dar cumplimiento a los objetivos de seguridad definidos en la presente Política e instando a todo el personal para que asuma este compromiso. Para ello, ISOIN implantará las medidas requeridas para la formación y concienciación del personal con la seguridad de la información.

8. APLICABILIDAD DE LA POLÍTICA Y MARCO NORMATIVO

Todo el personal interno, proveedores, colaboradores y, en general, todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de ISOIN, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

El marco normativo sobre el que se sustenta la presente política está definido por:

- Legislación relacionada con la Protección de Datos de Carácter Personal (LOPD, GDPR).
- Legislación sobre Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Legislación sobre protección legal para las obras de Propiedad Intelectual (LPI).
- Demás normativa y legislación aplicable a la actividad de la organización.

9. INCUMPLIMIENTO DE LA POLÍTICA Y PROCESO DISCIPLINARIO

ISOIN se someterá a revisiones y controles periódicos, así como a auditorías internas y externas para evaluar el cumplimiento general de esta Política.

El incumplimiento de la presente Política y de la normativa y procedimientos de seguridad de la información que la desarrollan, puede resultar en una acción disciplinaria dentro del marco legal aplicable, y dimensionadas al impacto que tengan sobre la organización.

10. REVISIONES Y DIVULGACIÓN

La presente Política de Seguridad será revisada y actualizada cuando proceda con el fin de adaptarla a los cambios que puedan surgir, garantizando su implantación en todo momento.

Esta Política de Seguridad y la normativa que la desarrolla, será difundida por los canales adecuados a todas las partes interesadas en base a la necesidad de su conocimiento. La presente Política estará disponible en la web corporativa y en el Portal del Empleado de ISOIN.

La Dirección de ISOIN