Responsable del documento: Oscar Gutiérrez.

Control de versiones

Versión	Motivo	Realizado por	Fecha
0.1	Versión preliminar. (Borrador)	R.Sánchez (Milenium Solutions)	19-07-2017
1.0	Versión Inicial	O. Gutiérrez	24/01/2017
1.1	Actualización LOPDGDD	R.Sánchez	03/04/2019
1.2	Actualización responsable Sistemas y nueva Ley Prop. Intelectual	R.Sánchez	23/05/2019
1.3	Incluir terminología de género	O. Gutiérrez	27/08/2019
1.4	Revisión	O. Gutiérrez	28/08/2020
1.5	Revisión	O. Gutiérrez	22/07/2021

Índice

Aprobado por: 28/08/2020 Dirección Iscan Servicios Integrales

Introducción

Este documento expone la Política de Seguridad de la Información de Iscan Servicios Integrales S.L. (en adelante la empresa), como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de la Norma ISO 27001.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la empresa. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La seguridad de la información es la protección de este activo, con la finalidad de asegurar la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio. Es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

La dirección de la empresa, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

Definiciones

- **Disponibilidad:** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Integridad:** La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Confidencialidad:** La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

Propósito

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de la empresa, asegurando para ello la disponibilidad, integridad y confidencialidad de la información y de las instalaciones,

sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

Alcance

El alcance del Sistema de Gestión de Seguridad de la Información engloba los sistemas de información que soportan los servicios de Transporte Sanitario (urgente y no urgente), Gestión Sociosanitaria y servicios de consultoría de la empresa.

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la empresa para los procesos descritos.

El personal sujeto a esta política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de la empresa. Por lo tanto, también se aplica a los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la empresa.

El contenido de la Política de Seguridad de la Información, cuando así se requiera, será desarrollado en normas y procedimientos complementarios de seguridad.

Objetivos y Fundamentos de esta Política

- La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción.
- La confidencialidad de la información debe garantizarse de forma permanente, evitando el acceso y la difusión a toda persona o sistema no autorizado.
- La integridad de la información debe ser asegurada, evitando la manipulación, alteración o borrado accidentales o no autorizados.
- La disponibilidad de la información debe salvaguardarse de forma que los/as usuarios/as y sistemas que lo requieran puedan acceder a la misma de forma adecuada para el cumplimiento de sus tareas y siempre que ello sea necesario.

- Se establecerán planes de contingencia y continuidad para garantizar la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas y medios para su tratamiento.
- La Política de Seguridad de la Información es aprobada por la Dirección de la empresa y su contenido y el de las normas y procedimientos que la desarrollan es de obligado cumplimiento.
- Todos los/as usuarios/as con acceso a la información tratada, gestionada o propiedad de la empresa tienen la obligación y el deber de custodiarla y protegerla.
- La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas de la norma ISO/IEC 27001:2014.
- Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad y la empresa deberá establecer una planificación para su implantación y gestión.
- Las medidas de seguridad y los controles establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.
- Los/as usuarios/as que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con la empresa y con la legislación vigente y aplicable.

Requisitos Legales

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 Abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Clasificación de la Información

La información se clasificará de acuerdo a la sensibilidad requerida en su tratamiento y a los niveles de seguridad y protección exigibles.

Roles, Responsabilidades y Deberes

La dirección asigna y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información. También se asegurará de que los/as usuarios/as conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados.

Usuarios/as

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de la empresa se considerará un/a usuario/a. Los/as usuarios/as son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos de la empresa. El/La usuario/a es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los/as usuarios/as tienen la obligación de:

- Cumplir la Política de Seguridad de la Información y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información de la empresa, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de seguridad aplicables.

Dirección

La dirección de la empresa está profundamente comprometida con la política descrita en este documento y es consciente del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

La dirección asume las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información

- Asegurar que se establecen la política y los objetivos de seguridad de la información y que estos son compatibles con la dirección estratégica de la organización.
- Aprobar y comunicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los/as usuarios/as, internos o externos, a los clientes y a los proveedores.
- Fomentar una cultura corporativa de seguridad de la información.
- Apoyar la mejora continua de los procesos de seguridad de la información.
- Asegurar que están disponibles los recursos necesarios para el cumplimiento de la política de seguridad de la información, de las normas de uso de los sistemas y para el funcionamiento del sistema de gestión de seguridad de la información.
- Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos y asegurar la evaluación de los mismos al menos con una periodicidad anual.
- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.
- Definir y controlar el presupuesto para seguridad de la información.
- Aprobar los planes de formación y las mejoras y proyectos relacionados con la Seguridad de la Información.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.

Responsable de Seguridad

La persona con el cargo de Responsable de Seguridad Informática en el organigrama de la empresa asumirá las siguientes funciones:

- Definir las políticas, normas y procedimientos de seguridad de la información e implantarlas tras la aprobación de la Dirección.
- Controlar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.
- Gestionar y verificar los incidentes de seguridad y proponer medidas correctoras.
- Analizar y gestionar los riesgos relacionados con la seguridad de la información, determinar las vulnerabilidades y establecer las medidas

de salvaguarda que garanticen la confidencialidad, integridad y disponibilidad de la información de acuerdo a un riesgo residual asumido por la organización.

- Proponer medidas y proyectos de mejora relacionados con la Seguridad de la Información a la Dirección para su aprobación.
- Elaboración y mantenimiento de los planes de contingencia y/o continuidad.
- Gestionar y supervisar el cumplimiento de la legislación vigente en materia de seguridad de la información incluyendo protección de datos, propiedad intelectual y sociedad de la información.
- Promover planes de formación, divulgación y concienciación en materia de seguridad de la información en la organización.
- Respecto a la protección de datos personales, asumirá el rol de Delegado de Protección de Datos LOPD.

Responsable del Sistema.

Serán funciones del Responsable del Sistema las siguientes:

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y la Dirección.
- Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de

revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.

- Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).

Evaluación de Riesgos de seguridad

Conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para la empresa, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

Se utilizará la metodología Magerit para analizar los riesgos. Por ello, se realizará un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que quedará documentado en un documento de Análisis de Riesgos.

La entidad debe determinar los niveles de riesgo a partir de los cuales tomará acciones de tratamiento sobre los mismos. Un Riesgo se considera aceptable cuando implantar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección de la empresa será responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

Proyectos

Todos los proyectos relacionados o que afecten a los sistemas de información deberán incluir, en su proceso de análisis, una evaluación de los requisitos de seguridad y definir un modelo de seguridad consensuado con el responsable de seguridad de la información.

En el diseño, desarrollo, instalación y gestión de los sistemas de información y en los proyectos se tendrán en cuenta y aplicarán los conceptos de seguridad desde el diseño, codificación segura y los controles y medidas de seguridad que proceda según el documento de aplicabilidad aprobado por la empresa.

Contratación y adquisiciones

Todas las contrataciones y adquisiciones que supongan o requieran acceso o tratamiento de información clasificada como no pública, deberán realizarse amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de información.

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberá incluir en el contrato el clausulado requerido para el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal y sus desarrollos, así como el futuro desarrollo del Reglamento Europeo de Protección de Datos.

Las empresas y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información confidencial o de uso interno, deberán conocer la Política de Seguridad de la Información y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las empresas y personas externas que accedan a la información de la empresa deberán considerar dicha información, por defecto, como confidencial. La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

Concienciación, Divulgación y formación

La presente Política de Seguridad de la Información debe ser conocida por todos los usuarios internos y externos y por las empresas que accedan, gestionen o traten datos de la empresa.

El conjunto de Políticas, normas y procedimientos complementarios a esta Política de Seguridad de la Información y el Documento de Seguridad LOPD también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso.

Se definirán, periódicamente, programas de comunicación, concienciación y formación y se entregará copia de la normativa correspondiente a los usuarios.

Respuesta a incidentes de seguridad

Cualquier compromiso de la confidencialidad, integridad o disponibilidad de la información de la empresa se considera un incidente de seguridad. Esto incluye, entre otros, el acceso, la eliminación, la destrucción, la modificación o la interrupción de la disponibilidad no autorizadas. También se consideran incidentes de seguridad los meros intentos de compromiso de las condiciones anteriores, los de evitar, alterar o modificar las medidas de seguridad o las violaciones o incumplimientos de la Política de Seguridad de la Información o de las normas y procedimientos complementarios.

Los usuarios son responsables de informar, de forma inmediata, de cualquier incidente de seguridad, a través de los canales y procedimientos definidos en la organización para la comunicación de incidencias.

Revisión y Auditorías

El responsable de seguridad revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la dirección.

Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de seguridad se auditará completamente cada año, según un plan de auditorías desarrollado por el responsable de seguridad.