Contenido

Elaborado: *Responsable del Sistema de Gestión (10/03/2022)*
Aprobado: ***Miguel Angel Camarero (****21/03/2022****)***

CONTROL DE VERSIONES

Versión	Fecha	Descripción
1.0	21/03/2022	Versión inicial

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 18 de Marzo del 2022 por la Dirección. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

KANBANLOG S.L. (KANBANLOG) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando de forma rápida y eficiente frente a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación y en la solicitud de ofertas.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de acuerdo al Artículo 7 del ENS.

2.1 PREVENCIÓN

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de y a todos los miembros de la organización, sin excepciones.

4. MISIÓN Y VISIÓN

Misión: Proveer de equipamiento y sistemas que ofrezcan soluciones logísticas en el entorno sanitario.

Visión: Ser líder reconocido en la implantación con éxito de soluciones innovadoras.

5. MARCO NORMATIVO

KANBANLOG se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

Normativa del Sector Público

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se trasponen al ordenamiento jurídico española las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 2/2015, de 2 de abril, de la Generalitat, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones

Normativa relativa a la Seguridad de la Información

- Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Otras Normativas

- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Ley 18/2018, de 13 de julio de la Generalitat Valenciana, para el fomento de la responsabilidad social.
- Los distintos convenios que sean de aplicación.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Gestión de la Seguridad de la Información estará formado por el Director de Operaciones y Seguridad de la Información, Responsable de TI, Responsable del Sistema de Gestión.

El Comité tendrá las siguientes funciones:

- Coordina todas las actividades relacionadas con la seguridad de las TIC.
- Es responsable de la redacción de la Política de Seguridad.
- Es responsable de la creación y aprobación de las normas que enmarcan el uso de los servicios TIC.
- Aprobará los procedimientos de actuación en lo relativo al uso de los servicios TIC.
- Aprobará los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en el documento de roles y responsabilidades de KANBANLOG.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

Los distintos cargos del Comité serán nombrados por la Dirección a propuesta del Comité de Gestión de la Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Gestión de la Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el mismo comité y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

KANBANLOG trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de KANBANLOG se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando cambie la información manejada.
- cuando cambien los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Gestión de la Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Gestión de la Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. GESTIÓN DOCUMENTAL

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en el procedimiento correspondiente: Elaboración y Control Documentos.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de KANBANLOG en diferentes materias:

- Aspectos organizativos de la seguridad de la información, que establece un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
- Seguridad física y ambiental, que establece las directrices para prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.
- Gestión de comunicaciones y operaciones, que define las pautas a seguir para asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información, así como de las redes.
- Control de acceso, que define cómo limitar el acceso a los recursos de tratamiento para prevenir el acceso no autorizado, garantiza el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.
- Adquisición, desarrollo y mantenimiento de los SSII, para garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida.
- Cumplimiento legal, para evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.
- Seguridad de los RRHH y Terceros, que asegura que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para desempeñar sus funciones.
- Cifrado, para garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
- Gestión de activos, que define como identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en una carpeta compartida accesible por parte de todos los usuarios.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de KANBANLOG tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Gestión de la Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de KANBANLOG asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de KANBANLOG, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. TERCERAS PARTES

Cuando preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando KANBANLOG utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

13. PRINCIPIOS SEGURIDAD DE LA INFORMACIÓN

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, KANBANLOG está altamente comprometida con mantener un servicio competitivo a través de ofrecer un modelo de negocio responsable, basado en la búsqueda permanente del equilibrio económico, social y ambiental, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad y legalidad de toda la información gestionada.

En consecuencia, KANBANLOG define los siguientes principios en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

- Confidencialidad: la información tratada por KANBANLOG será conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- Integridad: la información tratada por KANBANLOG será completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.

- Disponibilidad: la información tratada por KANBANLOG estará accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- Legalidad: KANBANLOG garantizará el cumplimiento de toda legislación o requisito contractual que sea de aplicación. Y en concreto, la normativa en vigor relacionada con el tratamiento de datos de carácter personal.

KANBANLOG para el correcto desempeño de sus funciones de negocio se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo estos, uno de los activos principales de KANBANLOG. De tal manera que el daño o pérdida de los mismos inciden en la realización de sus servicios 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 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 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 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 de cara a disponer de una profesionalidad en proceso de mejora continua en todos sus empleados.
- 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 activos de KANBANLOG.
- Proteger el capital intelectual de la organización para que no se divulgue ni se utilice ilícitamente.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la organización.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.

- Realizar una eficiente autorización y control de los accesos de la organización.
- Proteger adecuadamente las instalaciones.
- En el proceso de adquisición de productos aplicar controles de seguridad de la información, en función de la gestión del riesgo de la entidad.
- Aplicar el principio de seguridad por defecto
- Realizar una gestión adecuada al riesgo de la entidad en función de la integridad y actualización del sistema
- Realizar una eficiente protección de la información almacenada y en tránsito.
- Aplicar medidas de prevención ante otros sistemas de información interconectados.
- Realizar un adecuado registro de la actividad de los Sistemas de Información.
- Llevar a cabo acciones para garantizar la continuidad de la actividad de la organización ante posibles contingencias.
- Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y efectos.

La Dirección de KANBANLOG asume la responsabilidad de apoyar y promover el establecimiento de las medidas organizativas, técnicas de control necesarias para el cumplimiento de la presente Política de Seguridad de la Información. Así como, de proveer aquellos recursos que sean necesarios para resolver con la mayor rapidez y eficacia posible, las no conformidades e incidentes de seguridad de la información que pudiesen surgir, y la puesta en funcionamiento de las medidas necesarias para que estas no vuelvan a ocurrir.

Esta Política será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto se revisará de forma planificada o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia de tal forma que se aplique mejora continua en todo el proceso de seguridad de la información.

De igual forma, para gestionar los riesgos que afronta KANBANLOG se establece un procedimiento de evaluación de riesgos formalmente definido.

Por su parte, todas las políticas y procedimientos incluidos en el SGSI serán revisados, aprobados e impulsados por la Dirección de KANBANLOG.

Firmado Dirección:

Valencia a 21 de Marzo del 2022