TABLA DE CONTENIDO

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

1. OBJETIVO ALCANCE Y USUARIOS

Este documento resume la Política de Seguridad de la Información de **KRATA** como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de las Norma ISO 27001.

OBJETO

Establecer las directrices y principios que regirán el modo en que KRATA gestionará y protegerá su información y sus servicios, a través de la implantación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) aplicando los requisitos de la Norma UNE ISO/IEC 27001 y de sus partes interesadas, dentro del marco regulatorio legal y vigente.

La Dirección de KRATA, considera la Seguridad de la Información y la de los datos personales como un aspecto vital para garantizar la consecución de los objetivos de negocio. Manteniendo la obligación de garantizar la máxima seguridad de los servicios que se prestan, es decir, la confidencialidad, integridad y disponibilidad de los datos, sistemas y/o comunicaciones gestionadas por KRATA se compromete a liderar y fomentar a todos los niveles la seguridad de acuerdo a la Política de Seguridad y los objetivos que en la misma se defina y apruebe, tanto en el ámbito general como en el particular, y a la implantación y mantenimiento de un Sistema de Gestión para la Seguridad de la Información (SGSI) que se articule de forma que cumpla los requisitos legales o reglamentarios, gestione la protección y distribución de los activos de la organización, y se encuentre distribuido y publicado en la red corporativa para un mejor conocimiento por parte de todos los empleados.

La Dirección de KRATA se compromete igualmente a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI de la entidad, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Calidad y Seguridad de la Información.

FINALIDAD

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la organización. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle,

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

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.

ÁMBITO DE APLICACIÓN

Esta política es de obligado cumplimiento para todo el personal de KRATA, así como para todas aquellas personas físicas, profesionales u organizaciones que pudieran tener acceso a los sistemas de información corporativos, englobándose dentro del concepto de usuarios de los sistemas de información, debiéndose respetar y seguir cada una de las medidas que se indican en esta Política.

La seguridad de la información 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.

DIFUSIÓN/COMUNICACIÓN

La presente política plantea una serie de prácticas que regulan el adecuado uso y disponibilidad de los recursos informáticos, comprometiéndose KRATA a su difusión hacia todo el personal laboral y los otros posibles usuarios de los sistemas corporativos

Esta política ha sido aprobada por la dirección de **KRATA.** y se revisará cada doce meses. No obstante, si tuvieran lugar cambios relevantes para la Organización, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento.

2. Documentos de referencia

- UNE-EN-ISO 27001: 2013 Sistema de gestión de la seguridad de la información
- UNE-EN-ISO 27001: 2022 Sistema de gestión de la seguridad de la información

3. Descripción

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

3.1. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANIFICACIÓN PARA SU EJECUCIÓN

La presente Política pretende establecer las directrices necesarias en cuanto a Seguridad de la Información, las cuales son consideradas por la Dirección de KRATA como un requisito imprescindible para la consecución de los objetivos estratégicos y operativos

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.

- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.

- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.

- Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.

- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos, se realizará tomando en cuenta los siguientes elementos:

- Lo que se va hacer.
- Los recursos necesarios.
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

3.2. PROPÓSITO, OBJETIVOS Y REQUISITOS MÍNIMOS DE LA POLÍTICA DE SEGURIDAD.

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de **KRATA.** Para ello se asegura 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.

Es la política de KRATA asegurar que:

- 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 usuarios 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.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

- Todos los usuarios 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 las normas ISO 27001.

- Se cumplen los requisitos legales aplicables.

- Se cumplen los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.

- La Dirección valora los activos de información con los que cuenta KRATA derivará el análisis de riesgos y posteriormente la gestión de riesgos, tanto el análisis como la gestión de riesgos serán revisados anualmente por la Dirección, la cual decidirá si se efectúa un nuevo análisis y gestión de riesgos. Los riesgos a tratarse se verán reflejados en el Plan de Seguridad.

- 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 usuarios 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.

- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.

- Se establecen procedimientos para cumplir con la Política de Seguridad.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

- El responsable de Seguridad será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación. Además de supervisar y comprobar que se cumpla el Plan de Seguridad que corresponda a ese año.

La conformidad con las políticas de seguridad se justifica mediante la realización de auditorías internas según el procedimiento correspondiente

Esta política de seguridad, se desarrollará aplicando los siguientes **requisitos mínimos**:

- **Organización e implantación del proceso de seguridad**: La seguridad deberá comprometer a todos los miembros de la organización.

- **Análisis y gestión de los riesgos** propio y proporcionado respecto a las medidas.

- **Gestión de personal**.

    - Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.

    - Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

    - El personal relacionado con la información y los sistemas ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

    - El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.

    - Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

- **Profesionalidad**. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento

- **Autorización y control de los accesos**. El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

- **Protección de las instalaciones**. Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

- **Adquisición y contratación de productos de seguridad**. En la adquisición o contratación de productos de seguridad de las tecnologías de la información y comunicaciones se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

- **Seguridad por defecto**. Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

    - El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos

    - Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

    - En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

- **Integridad y actualización del sistema**. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

- **Protección de la información almacenada y en tránsito**. En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros.

  - Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

  - Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica deberá estar protegida con el mismo grado de seguridad que ésta

- **Prevención ante otros sistemas de información interconectados**. El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas.

- **Registro de actividad**. Con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

- **Incidentes de seguridad**. Se establecerá un sistema de detección y reacción frente a código dañino. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

- **Continuidad de la actividad**. Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

- **Mejora continua del proceso de seguridad**. El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

3.3. APROBACIÓN, DIFUSIÓN Y APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Corresponde a Dirección General la aprobación de la Política de Seguridad de conformidad con el procedimiento de información documentada. Esta política es de obligado cumplimiento para el personal de KRATA, así como para todas aquellas personas físicas, profesionales u organizaciones que pudieran tener acceso a los sistemas de información corporativos, englobándose dentro del concepto de usuarios de los sistemas de información, debiéndose respetar y seguir cada una de las medidas que se indican en esta Política de uso de los SI, así como todas aquellas medidas adicionales que pueda comunicar KRATA como de obligado cumplimiento. Por tanto, todo el personal de KRATA, manifiesta estar de acuerdo en el establecimiento de las normas que deben regir su utilización, tomar todas las medidas que correspondan y someterse a su cumplimiento.

La presente política plantea una serie de prácticas que regulan el adecuado uso y disponibilidad de los recursos informáticos, comprometiéndose KRATA a su difusión hacia todo el personal laboral y los otros posibles usuarios de los sistemas corporativos.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

En cumplimiento de los requisitos del SGSI, la legislación aplicable y los requisitos de seguridad de la información del sector farmacéutico, la política de Seguridad de KRATA será objeto de desarrollo de forma que se especifiquen las distintas medidas de seguridad que específicas para todos los ámbitos de aplicación dentro de la organización y sus actividades. Esto dará como resultado distintas normativas y regulaciones específicas que permiten el cumplimiento de los objetivos planteados en la política de seguridad de KRATA.

En relación a lo expuesto, KRATA establecerá un marco normativo en materia de Seguridad de la información, el cual se estructurará en varios niveles:

- Política de Seguridad de la Información.

- Normativas generales de seguridad de la información que se derivan de la Política de Seguridad de la Información.

- Normativas de uso o buenas prácticas en seguridad de la información, documentos donde se especifica el uso apropiado de los sistemas de información, describiendo los requisitos de seguridad de la información de los activos, instalaciones etc. y que se comunicarán a los empleados y terceras partes afectados para evitar el uso indebido.

- Instrucciones técnicas sobre procedimientos de seguridad, documentos que describen paso a paso cómo realizar una cierta actividad.

- Documentación sobre cursos de formación, sensibilización y concienciación del personal, presentaciones, etc. sobre seguridad de la información.

Como parte de esta política se generará la documentación que hace referencia a Normativas y Procedimientos que aplican a los procesos descritos en el alcance del SGSI. Las normas aquí establecidas deben interpretarse como complementarias a las normas

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

legales comúnmente aplicables. Dicha documentación, así como los controles establecidos se comunicarán, por los canales adecuados y en base a la necesidad del conocimiento a todas las partes interesadas.

Los usuarios que, de forma reiterada, deliberada o por negligencia, los infrinjan, quedarán sujetos a las actuaciones técnicas o disciplinarias que se estimen oportunas. Los usuarios se comprometen a colaborar con el Administrador de sistemas corporativos de KRATA para llevar a cabo toda investigación que tenga por objeto encontrar las posibles causas derivadas del mal uso de los recursos tecnológicos.

La información documentada será clasificada en: pública, interna y confidencial, dando el uso adecuado de acuerdo a dicha clasificación y según el criterio que se establezca en el Procedimiento de Clasificación, Etiquetado y Protección de la Información.

3.4. FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Gestión de Seguridad de la Información formado por:

Director General
Director General de Regulación y Seguimiento Normativo
Director Financiero
Director de Calidad, Protección de Datos Y Corporate Compliance

Como responsable de la información asume las siguientes funciones:

- Aprobación de la Política de Seguridad
- Revisión de la Política de Seguridad y aprobación de sus modificaciones
- Difusión y Comunicación de la Política de Seguridad
- Aprobación y difusión de toda la información documentada, así como sus revisiones y modificaciones
- Coordinación de las acciones de implantación, mantenimiento y mejora del Sistema y sus auditorías.
- Concienciación y Formación en Seguridad de la Información

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

- Nombramiento y designación del Responsable de Seguridad de la Información.

- Las que se especifiquen en las Políticas y Procedimientos del SGSI

CDO Responsable de Protección de Datos:

Se encarga de la gestión de los datos y de asesorar a la empresa para el cumplimiento del reglamento RGPD.

CSO Responsable de Seguridad de la Información

- Tener una visión de negocio que comprenda los riesgos que afronta la organización y cómo tratarlos.

- Entender la misión y los objetivos de la empresa y asegurarse de que todas las actividades son planificadas y ejecutadas para satisfacer dichos objetivos.

- Comprender las necesidades normativas, la gestión de la reputación de la organización.

- Establecer los planes de continuidad de negocio y recuperación de desastres en el ámbito de las tecnologías de la información.

- Estar al tanto de los cambios normativos, debiendo informarse de las consecuencias para las actividades de la organización y proponiendo las medidas oportunas para adecuarse al nuevo marco normativo.

IT Tecnología de Información.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

El Comité de Calidad y Seguridad de la Información delega en el proveedor externo de IT de KRATA, la gestión de los requisitos técnicos de Seguridad de los Sistemas de Información de KRATA y ejercerá las funciones de Administrador de Sistemas y las que se especifiquen en las Políticas y Procedimientos del SGSI.

Entre otras desarrollará las siguientes funciones:

- Analizar las necesidades informativas de tecnología
- Desarrollar y probar software,
- Realizar tareas de mantenimiento
- Solucionar problemas informáticos

Usuarios

Serán responsable de cumplir la presente política dentro de su área de trabajo, así como de aplicar toda la información documentada del SGSI de la entidad en sus actividades laborales que afecta a su desempeño en seguridad de la información.

Todos los miembros de KRATA, y terceros que realicen servicios de cualquier clase, contratados por la organización, tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas y procedimientos de seguridad que les sean aplicables, siendo responsabilidad del Comité de Seguridad, disponer de los medios necesarios para que la información llegue a los afectados.

La organización dispone de un plan de formación y concienciación del personal (incluido en el plan de acogida para nuevas incorporaciones). Las personas con responsabilidad en el uso, operación o administración de sistemas TIC reciben la formación adecuada para realizar esta tarea de manera eficiente y segura.

Terceras partes.

Cuando KRATA utilice servicios de terceros o ceda información a los mismos, se les hará partícipes de esta Política de Seguridad y de las normas y procedimientos de seguridad que conciernan a estos servicios o información. La tercera parte quedará sujeta a las obligaciones establecidas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. 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.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, el Comité de Seguridad hará un estudio que precise los riesgos incurridos y la forma de tratarlos, para garantizar que el contrato final del servicio garantice el nivel de seguridad requerido, o cuando menos, la organización sea consciente del riesgo asumido por esta carencia.

El detalle de las responsabilidades antes indicadas, así como los roles y autoridades en materia de seguridad de la información, se detallarán en la Normativa de Organización de la Seguridad de la Información

3.5. RESPONSABILIDADES DERIVADAS DEL INCUMPLIMIENTO DE LA POLÍTICA

El presente documento estará regulado por las leyes y normativa española, así como las que dimanen de la Unión Europea y de las comunidades autónomas en relación con la protección de datos de carácter personal, propiedad intelectual y uso de herramientas telemáticas, así como la normativa aplicable dentro del ámbito laboral y toda la que pueda aparecer en un futuro.

El incumplimiento de las disposiciones contenidas en la presente Política, de las Normativas de Seguridad de la Información derivadas de la misma así como de las contenidas en los procedimientos e instrucciones técnicas de seguridad, está catalogado como una falta grave o muy grave de los procedimientos de KRATA y puede provocar la formación de un expediente disciplinario a cargo de Recursos Humanos, así como la puesta en marcha de un procedimiento interno de investigación y respuesta frente a posibles incidencias en relación con el Código de Ético de KRATA.

Será considerada una falta "Grave" aquella que afecte al incumplimiento de las obligaciones y responsabilidades del personal y como "Muy grave" aquella, que además de eso, comporte un agravio para la organización o las personas que forman parte de ella, ya sea por temas de secreto profesional, pérdidas económicas o daños morales o reputación de KRATA o de las personas que forman parte de KRATA.

Los usuarios que, de forma reiterada, deliberada o por negligencia, los infrinjan, quedarán sujetos a las actuaciones técnicas o disciplinarias que se deriven del incumplimiento de los términos y condiciones que emanen de la relación laboral, además de las sanciones legales establecidas en la normativa vigente aplicable.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

Cuando los incumplimientos los realizaran terceros, sobre los que recaiga la obligación de cumplimiento en virtud de un contrato o cualquier otro tipo de relación acordada, la responsabilidad les será exigida en los términos previstos en los instrumentos que regulen estas relaciones (contratos) y por la normativa legal que pueda resultar de aplicación.

Toda incidencia detectada en los equipos informáticos, así como en los sistemas de información, podrán derivar en la suspensión o restricción del acceso o uso de los servicios al usuario, así como la aplicación de las medidas que la dirección de **KRATA** considere oportunas por el incumplimiento de lo establecido en el presente documento.

Los usuarios se comprometen a colaborar con el Administrador de sistemas corporativos de KRATA para llevar a cabo toda investigación que tenga por objeto encontrar las posibles causas derivadas del mal uso de los recursos tecnológicos**.**

3.6. CUMPLIMIENTO LEGAL Y ESTATUTARIO

La presente Política establece la necesidad de cumplir con todos aquellos requerimientos legislativos, normativos y contractuales que le sean de aplicación a KRATA y los activos de información gestionados. En este sentido, la Dirección de KRATA se compromete a dotar los recursos necesarios para dar cumplimiento a toda legislación y regulación aplicable a la actividad de Lleida.net y establece la responsabilidad de dicho cumplimiento sobre todos sus miembros.

En este sentido, se velará por el cumplimiento de toda legislación y regulación aplicable, la cual contempla principalmente los siguientes aspectos:

• Legislación relacionada con la protección de datos de carácter personal: o Reglamento (UE) 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 (GDPR)

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

o Ley Orgánica 3/2018, de 5 de diciembre, protección de datos personales y garantía de los derechos digitales. o Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

• Ley de Servicios de la Sociedad de la Información (LSSI): o Ley 34/ 2002 de 11 de julio de servicios de la sociedad de la información y comercio electrónico

• Legislación relacionada con la firma electrónica: o Reglamento (UE) n o 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE o Ley 59/2003, de 19 de diciembre, de firma electrónica

• Legislación relacionada con las telecomunicaciones: o Ley 9/2014 de 9 de mayo de Telecomunicaciones

Asimismo, se deberá asegurar el cumplimiento de cualquier otra legislación o normativa aplicable.

3.7. CONCIENCIACIÓN Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Todos los miembros de KRATA deberán disponer de la formación adecuada para el desempeño de sus funciones. Asimismo, deberá asegurarse la adecuada concienciación de los miembros de KRATA en términos de Seguridad de la Información y buenas prácticas.

Igualmente, los miembros de KRATA deberán disponer de acceso y conocimiento de las actualizaciones regulares de la presente Política y el resto del Cuerpo Normativo y Documental del SGSI.

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

3.8. INCIDENTES DE SEGURIDAD

Un incidente de seguridad consiste en cualquier evento que pudiera comprometer la confidencialidad, integridad y/o disponibilidad de la información, así como afectar a la consecución de los objetivos de KRATA.

La presente Política establece la obligación y responsabilidad de todos los miembros de KRATA, así como terceras partes incluidas en el alcance del SGSI, de la identificación y notificación a los gestores de KRATA de cualquier incidente que pudiera comprometer la seguridad de los activos de información de KRATA, así como de cualquier situación que pudiera suponer una no conformidad con los procedimientos del SGSI y el estándar ISO/IEC 27001.

El compromiso con la privacidad de los datos que deba tratar KRATA se refleja en la Política de Privacidad disponible para su conocimiento y consulta a través de la web corporativa

4. Registros

N/A

5. Formatos

N/A

6. Validez y gestión de documentos

Esta Política será revisada anualmente.

7. Control de Cambios

Edición	fecha	Apartado	Modificación
1	15/04/2020	Inicial	
2	18/03/2024	Legislativo	

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema

El presente documento es propiedad exclusiva de KRATA, S.A. quedando prohibida su reproducción sin el consentimiento del Responsable del Sistema