POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Última actualización: 01 de agosto de 2022

1. **Introducción**

   Este documento resume la Política de Seguridad de la Información de **Ekinplace** 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 y Esquema Nacional de Seguridad.

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

   La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la continuidad del servicio y minimizar el riesgo.

   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.

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

   Esta política ha sido aprobada por la dirección de **Ekinplace**, la cual se revisará cada doce meses y se actualizará conforme sea necesario.

   Las **dimensiones** de la seguridad de la información son:

   1. **Autenticidad:** El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
   2. **Confidencialidad:** La información sólo ha de estar disponible para usuarios autorizados, especialmente conforme su categorización.
   3. **Disponibilidad:** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
   4. **Integridad:** La información del sistema ha de estar disponible tal y como se almacenó por un usuario.

   El **ciclo PDCA** es el que se utilizará durante todo el ciclo de vida del SGSI [Sistema de Gestión de la Seguridad de la Información].

   1. **P (Planificar):** en esta fase se establecen las actividades, responsabilidades y recursos además de los objetivos a cumplir y cómo se van a medir estos objetivos.

2. **D (Desarrollar):** se desarrollan los procesos y se implementan. Una vez implementados, hay que medir los resultados de la ejecución de dichos procesos.
3. **C (Comprobar):** se analizan los resultados para comprobar si se han alcanzado los objetivos y si no es así, identificar las causas.
4. **A (Actuar):** Se toman las acciones necesarias para corregir los fallos detectados en los procesos o para mejorarlos.

2. Normatividad, Proposito y Objetivo

Las **normas** de referencia para el desarrollo de la plataforma, así como su ámbito de aplicación son las siguientes:

1. Norma UNE-ISO/IEC 27001 Tecnología de la Información. Especificaciones para los Sistemas de Gestión de Seguridad de la Información, en la que se recogen los requisitos para establecer, implantar, documentar y evaluar un SGSI. Es la norma sobre la que se desarrolla el sistema y la que permite obtener la certificación de este por parte de un organismo certificador independiente.
2. Norma ISO/IEC 27002 Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información. Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad y constituir una práctica eficaz de la gestión.
3. Esquema Nacional de Seguridad. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.
    1. 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 Ekinplace. 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.

El objetivo de esta Politica de la Seguridad de la información es promover el uso extensivo y seguro de las Tecnologías de la Información y Comunicación (TIC), a través de la protección de las redes de datos, los sistemas de información e infraestructuras críticas operativas, fortaleciendo los niveles de confidencialidad, integridad y disponibilidad.

Es la política de Ekinplace asegurar que:

1. 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.
2. La confidencialidad de la información debe garantizarse de forma permanente, evitando el acceso y la difusión a toda persona o sistema no autorizado.
3. La integridad de la información debe ser asegurada, evitando la manipulación, alteración o borrado accidentales o no autorizados.
4. 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.

5. 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.
6. 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.
7. 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.
8. 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 y Esquema Nacional de Seguridad.
9. Se cumplen los requisitos legales aplicables.
10. Se cumplen los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.
11. La Dirección valora los activos de información con los que cuenta la plataforma del cual 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.
12. Por seguridad las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán internamente en el Documento de Aplicabilidad y la empresa deberá establecer una planificación para su implantación y gestión.
13. Las medidas de seguridad y los controles establecidos serán estandarizadas, sin importar su clasificación ya que establecimos la criticidad de toda la información a proteger.
14. 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 el apartado 8 de procedimiento disciplinario y con la legislación vigente y aplicable.
    1. Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
    2. Se establecen procedimientos para cumplir con la Política de Seguridad.
15. 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.

3. Requisitos

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

1. **Organización e implantación del proceso de seguridad:** La seguridad deberá comprometer a todos los miembros de la organización.
2. **Análisis y gestión** de los riesgos propio y proporcionado respecto a las medidas.
3. **Gestión de personal.**
    1. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.

2. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.
3. El personal relacionado con la información y los sistemas ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.
4. 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.

4. **Profesionalidad.** La seguridad de los sistemas estará atendida, revisada y auditada por personal calificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento
5. **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.
6. **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.
7. **Seguridad por defecto.** Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:
    1. El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
    2. 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.
    3. 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.
8. **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.
9. **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.
    1. 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.
    2. 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.
10. **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.

11. **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.
12. **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.

4. Estructuracion de la seguridad de la informacion

Ekinplace tiene la responsabilidad de gestión de la información de salud y personal. Para ello contamos con una gestión de infraestructura de seguridad de la información explícita.

Alojamos la información en los servidores de AWS. Estos servidores están certificados bajo los siguientes estándares globales:

1. SOC 1/ISAE 3402, SOC 2, SOC 3
2. FISMA, DIACAP, and FedRAMP
3. PCI DSS Level 1
4. ISO 9001, ISO 27001, ISO 27017, ISO 27018

AWS mantiene sus altos estándares de seguridad y regularmente hacen auditorias para mantener los niveles de seguridad y propia implementación de estos.

Internamente, también utilizamos protocolos de seguridad para asegurar la seguridad del Intercambio de Información y la información otorgada.

1. Tráfico cifrado ocupando certificado SSL.
2. Acceso al servidor por personal autorizado.
3. Contraseñas encriptadas.
4. AWS: Certificaciones, Leyes/Regulaciones, Frameworks y Privacidad. https://aws.amazon.com/compliance/programs/

Estructura diseñada y estructurada para facilitar el acceso de los sujetos de atención (por ejemplo, para hacer peticiones para obtener información personal de salud), para facilitar la presentación de informes dentro de la estructura de la organización y para garantizar la entrega oportuna de la información.

5. Derechos y responsabilidad de terceros

éticas del personal, según lo acordado en la ley, y aceptadas por los usuarios de la plataforma;

1. Requisitos legales, reglamentarios y contractuales, incluidas las relativas a la protección personal de información personal de salud y las responsabilidades legales y éticas de los profesionales de salud para proteger esta información;
2. Disposiciones para la notificación de incidentes de seguridad de la información, incluyendo un canal para levantar preocupaciones respecto a la confidencialidad, y sin temor a la culpa o recriminación. En la creación del documento de política de seguridad de la información, las organizaciones de salud deberán considerar específicamente los siguientes

factores, que son únicas al sector salud:

3. La amplitud de la información de salud;
4. Los derechos de los sujetos de atención, donde aplique, a la privacidad y el acceso a sus registros;
   Cuando la organización de salud obtiene apoyo de terceros o colabora con terceros y especialmente donde recibe servicios de otras jurisdicciones, el marco de la política deberá incluir una política documentada, controles y procedimientos que cubran estas interacciones y que especifican las responsabilidades de todas las partes. En los casos en que los datos personales cruzan las fronteras nacionales o jurisdiccionales, las disposiciones del ISO 22857 deberán ser aplicadas.
5. Las obligaciones de médicos con respecto al consentimiento de obtener información de sujetos de atención y mantener la confidencialidad de la información personal de salud;
6. Las necesidades legitimas de médicos y organizaciones de salud que sean capaces de superar los protocolos normales de seguridad cuando las prioridades de salud, a menudo involucrados a la incapacidad de ciertos temas de cuidado de expresar sus preferencias, requieren esas anulaciones, también los procedimientos a emplear para lograr esto;
7. Las obligaciones de las respectivas organizaciones de salud, y de sus sujetos de atención, donde los servicios de salud son entregados en un "cuidado compartido" o "extensión de cuidados básicos";
8. Los protocolos y procedimientos a ser aplicados para compartir información para los propósitos de investigación y ensayos médicos;
9. Las medidas adoptadas y los límites de la autoridad, empleados temporales, tales como estudiantes o personal de guardia;
10. Las medidas adoptadas y las limitaciones impuestas al acceso a la información médica personal por los voluntarios y el personal de apoyo, como el clero y personal de caridad.

Las organizaciones cuyo personal está involucrado en el proceso de información personal de salud deberán documentar cada participación en una descripción relevante de trabajo. Funciones y responsabilidades de seguridad, tal como se establece en la política de seguridad de la información de la organización, también deberán ser documentadas en las descripciones de trabajo relevante.

Especial atención debe ser puesta sobre las funciones y responsabilidades del personal temporal o de corto plazo, tales como estudiantes, pasantes, etc.

6. Acuerdos de confidencialidad

Es obligación de todo personal y usuario de Ekinplace mantener la confidencialidad e integridad de los datos a los cuales pueden estar expuestos. Toda informacion esta considerada como altamente confidencial y sensible por lo que no debe de ser copiada, clonada, descargada o similar. El objetivo de este acuerdo es el de proteger la informacion de los usuarios de la plataforma.

Los datos personales y medicos de los usuarios y potenciales usuarios, deberán recibir el mismo trato que la Información Confidencial descrita en la cláusula anterior.

Asegurar que las condiciones relativas a la confidencialidad de información personal de salud sobrevivan la terminación del empleo a perpetuidad.

En caso de que cualquiera de las partes, incluyendo a sus respectivos usuarios, empleados, asesores, socios o personas allegadas a estos, incumplan alguna de las estipulaciones de la presente politica podrá ser causa de terminación de la relacion y la parte que incumpla pagará a la otra parte los daños y perjuicios que tal incumplimiento ocasionare, sin perjuicio de las demás acciones legales que procedan, por violación a los derechos de propiedad intelectual o industrial, incluyendo el delito de revelación de secretos contemplado en el Código Penal Federal de los Estados Unidos Mexicanos y la Ley de la Propiedad Industrial de los Estados Unidos Mexicanos, de igual forma los delitos relacionados con la recopilación de datos personales establecidos en la LFPDPPP.

7. **Responsabilidad de los prestadores de servicio**

Los profesionales de la salud deben estar continuamente empeñados en la superación de la calidad de la atención. Esto se refiere no sólo a mantener sus competencias, sino también a la colaboración con otros profesionales para reducir el error médico, elevar los niveles de seguridad del paciente, minimizar la excesiva utilización de los recursos y optimizar el resultado final de la atención. Este propósito debe ser tanto una acción individual, como una acción colectiva a través de las asociaciones y sociedades profesionales y científicas.

Como miembros de una profesión, los profesionales de la salud deben trabajar en colaboración a fin de maximizar la calidad de la atención, respetarse los unos con los otros y participar en el proceso de autorregulación, el cual incluye aplicar medidas disciplinarias a quienes fallen en la observación de los estándares profesionales.

Ley de Portabilidad y Responsabilidad del Seguro Médico

Los profesionales de la salud tienen el deber de tomar medidas razonables para preservar la confidencialidad de la información médica y personal. A toda persona se le reconoce el derecho a la confidencialidad a menos que autorice revelar la información. Los profesionales de la salud deben dar a conocer regularmente de qué modo garantizan la confidencialidad de la información médica. Los profesionales de la salud pueden compartir la información médica de una persona, pero solo entre ellos mismos y en la medida en que sea preciso para proporcionar los cuidados necesarios o para la gestión del pago del tratamiento. La información médica personal no puede ser revelada con fines comerciales. Los profesionales de la salud deberán tomar las precauciones necesarias para garantizar la confidencialidad de sus comunicaciones con el paciente. Las personas pueden presentar denuncias sobre prácticas de privacidad de los profesionales de la salud (directamente al profesional de la salud o ante el organismo gubernamental correspondiente.

En algunos casos excepcionales los profesionales de la salud son requeridos por ley para desvelar cierta información, en general si la enfermedad puede representar un peligro para los demás. Por ejemplo, ciertas enfermedades infecciosas, tales como la causada por el virus de la COVID-19, la inmunodeficiencia humana (VIH), la sífilis y la tuberculosis, suelen ser de declaración obligatoria ante los organismos gubernamentales o sanitarios competentes. Los profesionales de la salud que detectan signos de maltrato, abusos o negligencia en niños, adultos o ancianos deben notificarlo de forma sistemática a los servicios de protección.

Con respecto al personal clínico, los términos y condiciones de empleo deberán especificar los derechos de acceso que dicho personal tendrá a los registros de los sujetos de atención y a los sistemas de información de salud asociados en caso de reclamaciones de terceros.

Profesionalismo

El profesionalismo de la salud esta basado en conocimiento especializado, autonomía en la toma de decisiones, compromiso de servicio a la sociedad y autorregulación. Por lo que en todo momento los profesionales de la salud tienen la obligación de servir los intereses del paciente, con altruismo en la construcción de la relación médico-paciente. Ni las fuerzas del mercado, ni las presiones sociales, ni las exigencias administrativas pueden interferir con la aplicación de este principio. Los profesionales de la saluddeben tener respeto por la autonomía del paciente, deben ser honestos y darle el poder para la toma de decisiones informadas sobre su tratamiento. Pero las decisiones del paciente no deben ir en contra de las prácticas éticas ni dar lugar a demandas por atención inadecuada. Los profesionales de la salud deben tener una disposición por la justicia en los sistemas de salud, incluyendo la adecuada distribución de los recursos. Los médicos deben esforzarse en eliminar la discriminación en los servicios de salud, sea por raza, género, estatus socioeconómico, etnia, religión o cualquier otra categoría social.

Información

Los profesionales de la salud tienen la obligación de proveer información completa y honesta al paciente antes de su consentimiento para iniciar tratamiento. Si un paciente resulta lesionado como consecuencia del tratamiento, él o ella deben ser prontamente informados. El reporte en el análisis de los errores médicos sirve para la prevención y la implementación de estrategias de compensación.

Los profesionales de la salud tienen el deber dehacer notas deberán expresarse en lenguaje técnico médico, sin abreviaturas, con letra legible, sin enmendaduras ni tachaduras y conservarlo en buen estado. Los diagnosticos seran basados en la lista oficial del CIE-10 para una clasificacion estandarizada y un mejor control de los pacientes.

Faltas y brechas de acuerdos de confidencialidad

El contrato mencionado anteriormente deberá incluir referencia a las faltas que son posibles cuando una brecha en la política de seguridad de la información es identificada.

Brechas

1. Acceso post terminacion de empleo.
2. Acceso a area no autorizada.
3. Filtracion de datos no autorizados
4. Filtracion de malware.

Faltas

1. Divulgar o revelar datos de otro usuario.
2. Vender datos de otros usuarios.
3. Copiar informacion.
4. Mal uso de la informacion.
5. Infiltracion de malware o randsomware.

6. Alteracion de datos.
7. Cualquier acto que casione la destrucción, pérdida o alteración accidental o ilícita de datos.

Es importante notar el énfasis especial que tiene que ser puesto sobre las preocupaciones de los sujetos de atención de que no desean que su información personal de salud sea vista por los trabajadores de la salud tales como, colegas o parientes. Tales preocupaciones a menudo constituyen un porcentaje grande de quejas de aquellos con temores sobre la confidencialidad de su información personal de salud. De la misma manera, los empleados a menudo no desean ser colocados innecesariamente en la posición de revisar la información sobre amigos, parientes o vecinos de los sujetos de atención.

¿Cuáles son mis derechos con respecto al tratamiento de mis datos?

Bajo la LFPDPPP tiene los siguientes derechos:

1. Derecho a ser informado sobre el tratamiento de sus datos personales (es decir, para qué fines, qué tipo de datos personales, a qué destinatarios se divulgan, períodos de almacenamiento, cualquier fuente de terceros a partir de la cual se obtuvo, constatación de decisiones automatizadas, incluida la elaboración de perfiles, y la lógica, la importancia y las consecuencias previstas). La consulta de esta Política de Privacidad forma parte de su derecho a estar informado.
2. Derecho a presentar una queja ante nosotros contacto@ekinplace.com o ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), https://home.inai.org.mx/, si considera que tratamos sus datos personales de manera ilegal.
3. Derecho a solicitar una copia de los datos personales que tratamos sobre usted.
4. Puede pedirnos que borremos (si considera que no tenemos derecho a retenerlo) o rectifiquemos (si cree que son inexactos) sus datos personales.
5. Puede oponerse al tratamiento de sus datos personales o (cuando dependamos de su consentimiento para el tratamiento) retirar su consentimiento.
6. Derecho a restringir el tratamiento de sus datos personales.
7. Puede solicitar que sus datos se proporcionen de forma portátil.
8. Puede ponerse en contacto con nosotros (consulte los datos de contacto al final de esta política) si desea hacer valer alguno de estos derechos. Cumpliremos con nuestras obligaciones legales en lo que respecta a sus derechos como interesado.

Cualquier solicitud de acceso a sus datos personales debe hacerse por escrito y le contestaremos en un periodo no mayor a 30 (treinta) días.

Nos reservamos el derecho de negarnos a responder cuando las solicitudes sean manifiestamente infundadas o excesivas: en este caso, le explicaremos la situación y le informaremos sobre sus derechos.

Nuestro objetivo es garantizar que la información que tenemos sobre usted sea precisa en todo momento.

Para ayudarnos a mantener su información actualizada, deberá indicarnos cualquier cambio en sus datos personales. Si lo solicita, tomaremos medidas razonables para garantizar que los datos sean precisos y rectificaremos cualquier dato personal incorrecto de inmediato o en un plazo no mayor a 30 (treinta) días.

8. **Procedimiento disciplinario**

En caso de que haya una brecha de seguridad de la informacion o violacion de los terminos y politicas de la plataforma por parte de un usuario se tomaran medidas disciplinarias y se estableceran sanciones conforme la gravedad de la situacion identtificada.

Procedimiento disciplinario:

En caso de que un usuario haya sido reportado o encontrado en conflicto de las politicas de seguridad asi como los terminos y condiciones de la plataforma, este sera sujeto a un procedimiento disciplinario con la Direccion de la empresa o departamento correspondiente. De ser necesario se involucrara a la autoridad correspondiente ya sea local, estatal o federal. En caso de que se encuentre algún incumplimiento a los principios puedes hacerte acreedor de sanciones, multas y en el peor de los casos prisión.

Algunos ejemplos ilustrativos de posibles violaciones de la politica de seguridad pero no limitativas son: divulgacion de datos, copiar informacion para uso personal o comercial, infiltracion de malware o randsomware al servidor o cualquier acto que casione la destrucción, pérdida o alteración accidental o ilícita de datos.

Una vez reconocido al usuario y la infraccion, se designara los participantes del comite disciplinario para la revision, evaluacion y sancion correspondiente. La participacion del usuario en cuestion, sera limitada a una declaracion explicativa o justificativa de sus actos.

Sanciones establecidas pero no limitadas a:

1. Expulsion de la plataforma.
2. Multas financieras correspondientes al dano realizado a la plataforma o a posibles victimas. la sanción es de 100 a 160,000 veces el valor de la UMA.
3. En infracciones graves por violentar los datos la sanción es de 3 meses hasta 3 años de prisión.

Los procesos disciplinarios de las organizaciones de salud con respecto a las violaciones de seguridad de la información deberán seguir los procedimientos que son reflejados en la política y por lo tanto conocido por el sujeto(s) del proceso disciplinario. Además de cumplir con las reglas aplicables, como procesos, deberán cumplir con los acuerdos alcanzados entre profesionales de la salud y organizaciones profesionales de salud.

Para mayor informacion consulte nuestros terminos y condiciones asi como nuestro aviso de privacidad.