KEDRION
BIOPHARMA

POLÍTICA DE SEGURIDAD Y PRIVACIDAD PARA EL TRATAMIENTO DE LA INFORMACIÓIN

Tabla de Contenido

1. INTRODUCCIÓN

KEDRIÓN DE COLOMBIA S.A.S (en adelante **KEDRIÓN**) ha implementado una Política de Seguridad de la Información, en atención a la identificación de responsabilidades y objetivos que se debe trazar una organización como Responsable del Tratamiento de Datos Personales, con la finalidad de brindar una protección adecuada de los activos de la información, y de reducir los riesgos que puedan conllevar a la divulgación, modificación, destrucción o utilización de forma indebida de estos.

La presente Política de Seguridad de la Información, está conformada por estándares, procedimientos y herramientas de verificación y control, con el propósito de orientar y robustecer las medidas humanas, técnicas y administrativas que permitan a **KEDRIÓN,** administrar la información bajo el principio de seguridad, y criterios orientadores en la identificación y gestión de los riesgos de seguridad y privacidad.

2. OBJETO

Este documento establece los lineamientos para velar por el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, finalidad, libertad, veracidad y/o calidad, seguridad, transparencia, acceso y circulación de la información[1] para el Tratamiento de datos personales y gestión de la información que lleva a cabo **KEDRIÓN,** de tal manera que permita a la organización mantener y robustecer la postura de seguridad de la información.

3. ALCANCE

Los presentes lineamientos aplican a todos los colaboradores, proveedores y/o terceros, que tengan acceso a los activos de la información de **KEDRIÓN.**

4. MARCO NORMATIVO

Artículo 15 de la Constitución Política de Colombia – ““Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar”. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”.
b
Ley Estatutaria 1581 de 2012 - Dicta disposiciones para la protección de datos personales, la cual tiene por objeto “desarrollar el derecho constitucional que tiene todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos (…)”.

Ley 1273 de 2009 – Modifica el Código Penal y crea un nuevo bien jurídico tutelado que se denomina “protección de la información y de los datos”.

[1] Ley 1581 de 2012, artículo 4°.

Ley Estatutaria 1266 de 2008 - Dicta disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Ley 1032 de 2006 (derechos de autor y conexos) - Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).

Ley 527 de 1999 (Acceso y Uso de Mensajes de datos) - Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Decreto 1074 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1377 de 2013 - Por el cual se reglamenta parcialmente la Ley 1581 de 2012 que constituye el marco general de la protección de los datos personales en Colombia.

CONPES 3701 de 2011 - "Lineamientos de Política Nacional para Ciberseguridad y Ciberdefensa".

CONPES 3854 de 2016 - "Política Nacional de Seguridad Digital".

ISO/IEC 27001 – Estándar Internacional aplicable a sistemas de gestión de la seguridad de la información.

ISO/IEC 27002 – Estándar Internacional que condensa buenas prácticas en gestión de la seguridad de la información.

5. GLOSARIO

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la organización[2].

Activo de la información: recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso, o que tiene relación directa o indirecta con las actividades de la empresa: software hardware, personas (roles), físicos (instalaciones, área de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación)[3].

[2] ISO 27000
[3] ISO 27001

Amenaza: causa potencial de un incidente no deseado que pueda provocar daños a un sistema o a la organización[4].

Amenaza informática: toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio[5].

Antivirus: ccategoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus[6].

Análisis de riesgos: proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo[7].

Anonimización del dato: eliminar o sustituir algunos nombres de personas (naturales o jurídicas), direcciones, información de contacto, números identificativos, apodos o cargo por otros datos para evitar la identificación de personas y preservar la confidencialidad de la información[8].

Autenticación: mecanismo técnico que permite garantizar que una persona o entidad es la correcta[9].

Autenticidad: Propiedad de que una entidad es lo que afirma ser[10].

Back up: se refiere a una copia de respaldo de información.

Buzón: espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros.

Canal de comunicación: medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.

Centro de cómputo: espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado también data center por su término anglosajón.

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética[11].

---

[4] ISO 27000
[5] Ministerio de las Tecnologías y Comunicaciones - Guía para la Implementación de Seguridad de la Información.
[6] Ministerio de las Tecnologías y Comunicaciones - Guía para la Implementación de Seguridad de la Información.
[7] ISO 27000
[8] http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estandares-Proteccion-Datos-Personales espanol.pdf
[9] ISO 27001
[10] ISO 27001
[11] CONPES 3701

Ciberespacio: ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.[12].

Confiabilidad: persona o cosa en la que se puede confiar.

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados[13].

Control informático: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento[14].

Criterios para adquisición de tecnología: condiciones o requisitos mínimos para tener en cuenta al momento de implementar y/o adquirir tecnología.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz)[15].

Datos personales sensibles: aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos[16].

Dato privado: dato que por su naturaleza íntima o reservada sólo es relevante para el titular[17].

Dato público: dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas[18].

[12] Resolución CRC 2258 de 2009
[13] NTC-ISO/IEC 27001
[14] ISO 27000
[15] Ley 1581 de 2012
[16] Decreto 1377 de 2013.
[17] Ley 1266 de 2008.
[18] Ley 1266 de 2008.

Dato semiprivado: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios[19].

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[20].

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información[21].

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas[22].

Gestión de incidentes de seguridad de la información: proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información[23].

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, comprende la identificación, evaluación y el tratamiento de riesgos[24].

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos[25].

Infraestructura tecnológica: elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros.

Impacto: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.[26]

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[27].

[19] Ley 1266 de 2008.
[20] NTC-ISO/IEC 27001
[21] ISO 27001
[22] ISO 27000
[23] ISO 27001
[24] NTC-ISO/IEC 27001
[25] Constitución Política de Colombia, artículo 15
[26]ISO 27000
[27] ISO 27000

Integridad: la propiedad de salvaguardar la exactitud y completitud de la información[28].

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos[29].

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro[30].

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma[31].

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas[32].

Responsable de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado encargado de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados, quien puede designar custodios del activo de información y autorizar a los usuarios para el acceso al activo de información.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones[33].

Responsable del tratamiento: persona natural o jurídica, pública o privada que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos[34].

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información[35].

Titular de la información: persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley[36].

[28] NTC-ISO/IEC 27001
[29] ISO 27000
[30] ISO 27000
[31] ISO 27000
[32] ISO 27000.
[33] ISO Guía 73:2002
[34] Ley 1581 de 2012
[35] NTC-ISO/IEC 27001
[36] Ley 1266 de 2008

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad[37].

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas[38].

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

KEDRIÓN entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y no repudio de la información, mediante una gestión integral de riesgos, implementación de controles físicos y digitales, con la finalidad de prevenir incidentes, y dando cumplimiento a los requerimientos legales. Por tal motivo, **KEDRIÓN** ha definido e implementado una Política de Seguridad y Privacidad de la Información, teniendo en cuenta los siguientes aspectos:

6.1. Proteger los activos de la información, mediante políticas, procedimientos e instructivos en materia de seguridad de la información, teniendo en cuenta el ciclo de vida útil del dato.
6.2. Aplicar controles de acceso a la información creada, procesada, transmitida o resguardada por los procesos propios del negocio, con la finalidad de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, teniendo en cuenta la clasificación de la información a la cual se le hace Tratamiento.
6.3. Mitigar el riesgo de vulnerabilidad en la seguridad de la información, en la ejecución de los procesos y actividades propias de **KEDRIÓN**, a través de una adecuada gestión de eventos de seguridad y riesgos asociados al Tratamiento de datos personales y gestión de la información.
6.4. Cumplir con los principios (Disponibilidad, Integridad y Confidencialidad) de seguridad de la información.
6.5. Fortalecer la cultura de seguridad de la información al interior de la organización.
6.6. Verificar de manera periódica el cumplimiento de las políticas de seguridad de la información.
6.7. Cumplir las obligaciones legales, regulatorias y contractuales establecidas.

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1. ROLES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

[37] ISO 27000
[38] ISO 27000

En atención a la estructura organizacional de **KEDRIÓN,** el encargado de efectuar la verificación del cumplimiento y respectivo seguimiento de las medidas establecidas en la Política de Seguridad y Seguridad de la Información será el Representante Legal.

7.2. GESTIÓN DE ACTIVOS

7.2.1. Responsabilidad frente a los activos de información:

7.2.1.1. Propender por la seguridad y la calidad de la información, siguiendo criterios de confidencialidad, integridad, disponibilidad, efectividad, eficiencia, confiabilidad y cumplimiento, en calidad de colaboradores, proveedores y/o terceros con quienes **KEDRIÓN** tenga relación en el giro ordinario de los negocios.
7.2.1.2. Cumplir las políticas y los controles de seguridad de la información definidos, para garantizar la preservación de la confidencialidad, integridad, disponibilidad de los activos de la información de la organización, y recuperación de la información.
7.2.1.3. Está prohibido hacer modificaciones a los activos de la información, sin contar con autorización previa, expresa y por escrito para ello.
7.2.1.4. Está prohibido hacer uso de los activos de la información de **KEDRIÓN**, para fines diferentes al cumplimiento de las actividades propias de la organización.
7.2.1.5. Hacer el inventario de todos los activos de la información, los cuales deben estar asignados a un responsable,
7.2.1.6. Actualizar de manera periódica todos los activos de la información, con los lineamientos relacionados con las restricciones de acceso a la misma.
7.2.1.7. Ser el responsable del uso y protección de los activos de la información, en calidad de encargado de esta, mientras se encuentre en su custodia física o digital.
7.2.1.8. Informar cualquier incidente de seguridad que pueda presentarse, tales como: uso indebido, alteración y/o divulgación no autorizada.

7.2.2. Identificación de activos

Los activos de la información con que cuenta **KEDRIÓN** están conformados por: información relativa a la constitución y composición de la organización, y tres (3) bases de datos denominadas: “clientes kedrión”, “proveedores kedrión” y “nómina kedrión”.

La identificación de los activos de la información con los que cuenta **KEDRIÓN**, se lleva a cabo de forma manual dado al tamaño de la organización.

7.2.3. Etiquetado de la información

Con la finalidad de identificar la naturaleza y tipo de datos personales y en general, información, respecto de la cual se lleva a cabo Tratamiento; se debe tener en cuenta la siguiente clasificación:

7.2.3.1. **Información Pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. Literal b) del Artículo 6 de la Ley 1712 de 2014.

7.2.3.2. **Información Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

7.2.3.3. **Información sensible:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

7.2.3.4. **Información Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

El responsable de verificar el entendimiento y la debida clasificación de la información será el Representante Legal de **KEDRIÓN.**

7.2.4. Disposición de los activos

Con el objetivo de establecer reglas para el uso aceptable de los activos información identificados y la infraestructura destinada al procesamiento de la información, se documentarán las restricciones necesarias en la gestión de la información, de acuerdo con los requisitos de protección determinado por el tipo de información y su clasificación.

Se registrarán los colaboradores autorizados de **KEDRIÓN** que intervienen en los procesos que gestionan y procesan los activos de información.

Los lineamientos y procedimientos de operación de TI en **KEDRIÓN** establecerán las acciones en el manejo de cualquier medio móvil y reusable que vaya a ser transportado o dado de baja de la organización. Una vez removidos los medios, se tomarán las medidas para garantizar que la información no sea recuperable, estas actividades deberán ser registradas, documentadas e informadas a los responsables de los procesos de respaldo y recuperación de información.

El transporte de medios con información misional o asociada al objeto contractual de la organización deberá ser a través de proveedores de servicio especializado debidamente certificados. Las autorizaciones previas de traslado o eliminación de medios deberán contar con el registro y la disponibilidad para su posterior consulta. Los formatos utilizados para el almacenamiento de la información de acuerdo con su clasificación y valoración de riesgo deberán ser estándares vigentes en el mercado tanto en el cifrado como en la locación de la información, esto con el fin de facilitar su recuperación, por lo tanto, el seguimiento a los ejercicios periódicos de recuperación de copias de seguridad evaluará la efectividad de la restauración y la vigencia tecnológica a la infraestructura de "*BackUp*".

7.3. POLÍTICA DE CONTROL DE ACCESO

7.3.1. Objetivo

Establecer las definiciones de acceso a los usuarios autorizados a los sistemas, aplicaciones y demás recursos tecnológicos, ejerciendo, la asignación, modificación, revocación y gestión de permisos bajo los siguientes lineamientos:

7.3.1.1. Mínimo privilegio.
7.3.1.2. La necesidad estricta de cumplir las funciones asignadas.
7.3.1.3. Control dual establecido en los flujos de roles y perfiles.
7.3.1.4. La coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes.
7.3.1.5. Los requerimientos de seguridad de cada una de las aplicaciones.
7.3.1.6. Toda la información relacionada con las aplicaciones.
7.3.1.7. La legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
7.3.1.8. Los perfiles de acceso de usuarios base, comunes a cada categoría de puestos de trabajo.
7.3.1.9. La administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
7.3.1.10. La revisión periódica de los derechos de acceso.

7.3.2. Asignación de Permisos y/o asignación de contraseñas

Los permisos concretarán que acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el mínimo privilegio en el establecimiento de los permisos.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el siguiente flujo:

7.3.2.1. Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto.

7.3.2.2. Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.

7.3.2.3. Generar contraseñas provisionales para iniciar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.

7.3.3. Creación/modificación/borrado de cuentas de usuario

Para permitir el acceso a los sistemas de información de **KEDRIÓN** deberá seguirse el procedimiento que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios indicando quién debe autorizarlo. Detallar los datos identificadores de las mismas, las acciones que se permiten y dotándolas de las credenciales de acceso correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán asimismo parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales, así como de la Política de contraseñas.

7.3.4. Cuentas privilegiadas

El Responsable de la Información limitará y controlará la asignación y uso de privilegios. Los sistemas multiusuario que requieren protección contra accesos no autorizados deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

Se deben tener en cuenta los siguientes pasos:

7.3.4.1. Identificar los privilegios asociados a cada activo que requiera el acceso de usuarios, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

7.3.4.2. Asignar los privilegios a usuarios sobre la base de la necesidad de uso y evento por evento.

7.3.4.3. Mantener un proceso de autorización y un registro de todos los privilegios asignados. (Nota: Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización).

7.3.4.4. Establecer un periodo de vigencia para el mantenimiento de los privilegios, luego del cual los mismos serán revocados. (Nota: NO deben existir usuarios sin fecha de vigencia)

7.3.4.5. Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

7.3.5. Mecanismos de autenticación

Para establecer los mecanismos de autenticación adecuados para permitir el acceso a la información de la organización, se tendrán en cuenta aspectos como los siguientes:

7.3.5.1. Utilización mecanismos de autenticación internos o basados en servicios de autenticación de terceros
7.3.5.2. Tecnologías que pueden usarse: autenticación vía web, servicios de directorio, LDAP.
7.3.5.3. Factores de los mecanismos de autenticación (uno o varios): *(i)* algo que somos (a través de técnicas biométricas), *(ii)* algo que sabemos (a través de contraseñas), *(iii)* algo que tenemos (a través de dispositivos personales, *tokens* criptográficos).

7.3.6. Registro de eventos

Se deberán establecer los mecanismos necesarios para registrar los eventos relevantes garantizando su conservación y acceso autorizado en el manejo de la información de la organización. Asimismo, se registrará convenientemente quién accede a la información, cuándo, cómo y con qué finalidad.

7.3.7. Revisión de permisos

Los dueños de los activos de información que corresponde a los servicios de aplicación establecerán los requerimientos periódicos para la evaluación de los permisos, incluyendo los usuarios privilegiados.

7.3.8. Revocación de permisos

En cumplimiento de los procedimientos de gestión de usuarios a partir de las solicitudes de los dueños de los activos, se tomarán las acciones suficientes y necesarias para revocar los privilegios, permisos y accesos de cualquier usuario, que por motivos de traslados o desvinculación requiera dicha revocación. Se deberán ofrecer los mecanismos técnicos para su cumplimiento registro y seguimiento.

7.4. CONTROLES CONTRA SOFTWARE MALICIOSO

KEDRIÓN deberá establecer los controles de detección y prevención para la protección contra software malicioso, estableciendo y ejecutando los procedimientos adecuados de concientización de usuarios en materia de seguridad y controles de acceso al sistema.

Se aplicarán controles tales como:

7.4.1. Prohibir el uso de software no autorizado.
7.4.2. Evaluar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.

7.4.3. Instalar el software de detección y reparación de virus con sus componentes avanzados disponibles en el mercado para examinar los activos de información y medios informáticos, de forma permanente, por parte de toda estación de trabajo, servidor o infraestructura
7.4.4. Mantener los sistemas actualizados de acuerdo con las liberaciones generadas por sus fabricantes.
7.4.5. Establecer procedimientos para verificar toda la información relativa a software malicioso emitida por canales y entidades validadas.

7.5. ESCRITORIO LIMPIO

Esta política tiene por objetivo salvaguardar los activos de información asociados a los puestos de trabajo y equipos de cómputo a través de las acciones de mantener un puesto de trabajo limpio y datos de procesamiento de información no expuestos, para reducir los riesgos de acceso no autorizado, fuga o daño de la información durante y después de la jornada laboral.

Se debe configurar las estaciones de trabajo el bloqueo de sesión, el cual debe activarse automáticamente máximo después de ciento ochenta segundos o tres minutos de inactividad y será necesario para ingresar a la sesión, escribir la contraseña del usuario.

Siempre que un usuario se ausente de su computador de trabajo, debe realizar el bloqueo de la sesión oprimiendo la tecla de **Windows + la tecla L** para evitar riesgos de acceso no autorizado.

No se deben escribir las contraseñas en notas adhesivas en el escritorio o cualquier otro medio visual, o mantenerlas a la vista de las demás personas.

Cuando se envíe documentos a imprimir, el documento impreso debe retirarse inmediatamente de la impresora.

Al finalizar la jornada de trabajo se debe guardar en un lugar seguro bajo llave, los documentos y medios que contengan información de cumplimiento misional de **KEDRIÓN.**

7.6. ACCESO REMOTO

Los usuarios podrán acceder en forma remota a los activos de información a través de una plataforma de conexiones de VPN. Para el acceso deberá solicitarse la correspondiente autorización. En cualquier situación, dicho acceso será gestionado por el personal asignado para ello, y solo podrá tener por finalidad dar soporte a equipos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de seguridad y/o monitoreo.

Se debe mantener un registro de los accesos que se han realizado a través de la VPN para efectos de trazabilidad y posterior revisión en caso de ser requerido.

El acceso por VPN debe estar asociado a la gestión de usuarios y seguir los mismos lineamientos de creación, modificación, revocación, cambio y monitoreo.

7.7. NO REPUDIO

La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción. Se deberán incluir como mínimo los siguientes aspectos:

7.7.1. Trazabilidad: La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
7.7.2. Retención: La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la organización.
7.7.3. Auditoría: La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
7.7.4. Intercambio electrónico de información: La política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

7.8. POLÍTICA DE PRIVACIDAD Y CONFIDENCIALIDAD

7.8.1. Objetivo

Describir las políticas de Tratamiento y Protección de datos personales que deberán aplicarse, conforme a la normatividad vigente.

7.8.2. Principios del Tratamiento de Datos Personales[39]

7.8.2.1. Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
7.8.2.2. Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
7.8.2.3. Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
7.8.2.4. Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
7.8.2.5. Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
7.8.2.6. Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.

[39] Ley Estatutaria 1581 de 2012 “Régimen General de Protección de Datos Personales”.

7.8.2.7. Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
7.8.2.8. Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información

7.8.3. Acuerdo de Confidencialidad

Con la finalidad de preservar la confidencialidad y privacidad de la información que se maneja en **KEDRIÓN**, se hará uso del acuerdo de confidencialidad implementado con colaboradores, contratistas y/o terceras personas, en aquellos eventos en que la información que se esté tratando lo amerite.

7.9. POLITICA DE DISPONIBILIDAD DE LA INFORMACIÓN

7.9.1. Planes de recuperación

Con el objetivo de garantizar la continuidad de los servicios ante posibles eventos no deseados que interrumpan la operación de los procesos de **KEDRIÓN**, se debe identificar aquellos que puedan ocasionar interrupciones en los procesos operaciones de TI, por ejemplo, fallas en el equipamiento, interrupción de energía eléctrica, inundación de instalaciones, y demás que afecten los activos de información de **KEDRIÓN**. Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del periodo de recuperación, se deben identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

7.9.2. Acuerdos de nivel de servicio

El área de TI y el área Legal revisarán los contratos o acuerdos existentes con los proveedores de servicio, teniendo en cuenta los siguientes lineamientos:

7.9.2.1. Cumplir con la Política de Seguridad de la Información.
7.9.2.2. Acuerdo de confidencialidad de la información que sea compartida transmitida o gestionada.
7.9.2.3. Descripción de los servicios contratados Nivel de servicio esperado de acuerdo a la naturaleza del servicio contratados con las debidas multas ante el incumplimiento de los niveles pactados.

7.9.3. Segregación de ambientes

Los ambientes de desarrollo, prueba y operaciones estarán separados siguiendo las siguientes definiciones:

7.9.3.1. Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos o directorios.
7.9.3.2. Separar las actividades de desarrollo y prueba, en entornos diferentes.
7.9.3.3. Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo.
7.9.3.4. Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
7.9.3.5. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificaran claramente a qué instancia se está realizando la conexión.
7.9.3.6. Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
7.9.3.7. El personal de desarrollo NO tendrá acceso al ambiente operativo.

7.9.4. Gestión de cambios

Se deben definir los procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos de riesgos técnicos y de seguridad. Se deberá controlar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de estos ni de la información que soportan.

Los procedimientos de cambio evaluarán el posible impacto operativo de los cambios previstos y verificará su correcta implementación. El Responsable del Sistema de Información mantendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios deberán contemplar los siguientes puntos:

7.9.4.1. Evaluación de riesgos del posible impacto de dichos cambios.
7.9.4.2. Aprobación formal de los cambios propuestos.
7.9.4.3. Planificación del proceso de cambio – Ingeniería del detalle.
7.9.4.4. Prueba del nuevo escenario.
7.9.4.5. Comunicación de detalles de cambios a todas las personas pertinentes.
7.9.4.6. Identificación de las responsabilidades.
7.9.4.7. Actividades de retorno ante imprevistos.

7.10. REGISTRO Y AUDITORIA

El responsable de efectuar la auditoría y registro de los hallazgos evidenciados será el Representante Legal de **KEDRIÓN** o su delegado formalmente designado.

La auditoría será llevada a cabo semestralmente, debiéndose levantar un acta de los hallazgos que se evidencien, de tal manera que se administre un registro consecutivo del cumplimiento de esta obligación.

7.11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

7.11.1. Nivel de riesgo del incidente de seguridad[40]

El nivel de riesgo habrá de calcularse en relación con el riesgo que representa el incidente de seguridad para los Titulares de la información, de la siguiente manera:

BAJO RIESGO: es improbable que el incidente de seguridad tenga un impacto en las personas, y de generarlo, este sería mínimo.
RIESGO MEDIO: el incidente de seguridad puede tener un impacto en las personas, pero es poco probable que el impacto sea sustancial
RIESGO ALTO: el incidente de seguridad puede tener un impacto considerable en las personas afectadas.
RIESGO GRAVE: el incidente de seguridad puede tener un impacto crítico, extenso o peligroso en las personas afectadas.

7.11.2. Protocolo de respuesta en el manejo de violaciones o incidentes de seguridad

Con el presente protocolo se busca disponer de un lineamiento estructurado y planificado que permita manejar adecuadamente los incidentes de seguridad asociados al tratamiento de Datos Personales en **KEDRION** para:

7.11.2.1. Administrar adecuadamente los eventos tecnológicos asociados al tratamiento de Datos Personales
7.11.2.2. Gestionar los incidentes de seguridad asociados al tratamiento de Datos Personales
7.11.2.3. Integrar los procedimientos de atención de los eventos asociados al tratamiento de Datos Personales

Los eventos e incidentes asociados al tratamiento de Datos Personales pueden ocurrir en cualquier etapa del ciclo de vida del dato de **KEDRIÓN**. Es importante considerar que "la probabilidad de que se materialice una brecha de seguridad nunca es cero, y cuanto más tiempo transcurre, mayor es la probabilidad de que ocurra un incidente"[41].

El protocolo de gestión de incidentes de seguridad asociados al tratamiento de Datos Personales se desarrollará de acuerdo a las siguientes fases de manera cíclica, tal como lo muestra la imagen y se desarrolla en el cuadro[42]:

[40] Superintendencia de Industria y Comercio, Guía Gestión de Incidentes de Seguridad, 2020.
[41] Agencia Española de Protección de Datos Personales. *"Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"*. Madrid, 2021. Página 46.
[42] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf, página 2.

Ciclo de vida de la gestión de incidentes

ETAPA	DESCRIPCIÓN
Preparación, Reporte y Registro de eventos e incidentes de seguridad asociados al tratamiento de datos personales	Permite a **KEDRIÓN** estar en capacidad de responder ante los incidentes asociados al tratamiento de Datos Personales y, además, desarrollar una forma en que las vulnerabilidades puedan ser detectadas, evaluadas y gestionadas, es decir, medidas técnicas y organizativas para poder afrontar un incidente asociado al tratamiento de Datos Personales, con el fin de mitigar los riesgos.
Detección, Evaluación y Análisis	La **detección** se encarga de la identificación y gestión de elementos que alertan sobre un incidente, provee información sobre la futura ocurrencia del mismo e incide en la preparación de procedimientos para mitigar su impacto. Para ello**, KEDRIÓN** debe: i) definirse un listado de fuentes generadoras de eventos que permita la identificación de un incidente de seguridad asociado al Tratamiento de datos personales, ii) buscar estrategias con el fin de que el incidente no se propague y genere más daños. Las estrategias varían según el tipo de incidente asociado al Tratamiento de datos personales, iii) definir el nivel de prioridad, la criticidad de impacto -el impacto actual y el impacto futuro-, con el fin de implementar una atención adecuada a los incidentes de seguridad asociados al tratamiento de datos personales. En lo referente a la **evaluación** de un incidente se debe tener en cuenta el nivel de impacto según el análisis de riegos y la clasificación de

ETAPA	DESCRIPCIÓN
	activos de información de **KEDRIÓN**, dependiendo de su infraestructura, riesgos y criticidad de sus activos. Por último, para determinar con mayor precisión la clasificación del incidente en el análisis de las brechas de seguridad, debe tenerse en cuenta: (i) El componente tecnológico enfocado a los controles y medidas de seguridad, (ii) La valoración de los riesgos a los derechos y libertades de las personas.
Contención, Erradicación, Recuperación y Respuesta	La **contención** permite tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad asociado al Tratamiento de datos personales. La **erradicación** es la etapa en la que deben eliminarse los rastros que hubiera podido dejar la causa del incidente y que entrañan la ocurrencia de uno nuevo si se mantienen activos. Es indispensable contar con los recursos técnicos y humanos para preservar correctamente las posibles evidencias que sirvan para ubicar al responsable del incidente, si lo hay. Por último, la **recuperación** es la eliminación de rastros dejado por el incidente asociado al Tratamiento de datos personales y la posterior restauración del sistema y/o servicios afectados. Es importante tener en cuenta que en caso de que un incidente afecte gravemente puede activarse el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastre).
Actividades Post Incidente	Las actividades post incidentes se componen del reporte del Incidente asociado al Tratamiento de datos personales, de la verificación de las lecciones aprendidas, del diseño e implementación de medidas tecnológicas, disciplinarias y penales de ser necesarias así como el registro en la base de conocimiento para

ETAPA	DESCRIPCIÓN
	alimentar los indicadores.

7.11.3. Puntos o personas de contacto

En el evento de considerar que la seguridad y/o privacidad de la información que administra **KEDRIÓN** se encuentre en riesgo de ocurrencia de un incidente de seguridad, se deberá contactar de manera inmediata con el Representante Legal de la organización:

Representante Legal: Juan Carlos Beltrán Gonzalez

Número Contacto: +57 3173657453

Correo electrónico: j.beltran@kedrion.com

7.11.4. Reporte del incidente

KEDRIÓN como Responsable del Tratamiento de Datos Personales, está obligado a adoptar las medidas de seguridad necesarias y a su alcance para impedir el acceso no autorizado y la alteración de los Datos Personales. No obstante, en caso de que ocurra una violación a los códigos de seguridad, informará de dicha circunstancia a la SIC, de conformidad con los lineamientos establecidos al interior de la organización.

Para esto, el personal encargado de efectuar el reporte ante la SIC será el Representante Legal de **KEDRIÓN.**

7.11.5. Documentación y/o registro interno del incidente

En el evento que se llegase a presentar un incidente de seguridad y/o privacidad de la información de **KEDRIÓN,** el Representante Legal deberá llevar un registro documental, con la siguiente información:

7.11.5.1. Descripción general de las circunstancias del incidente de seguridad
7.11.5.2. Información y/o datos comprometidos
7.11.5.3. Categoría de los titulares de la información
7.11.5.4. Fecha y hora del incidente de seguridad y/o del descubrimiento de este
7.11.5.5. Investigaciones adelantadas por el encargado
7.11.5.6. Medidas correctivas implementadas
7.11.5.7. Prueba del reporte efectuado ante la SIC, cuando fuese necesario
7.11.5.8. Prueba de la comunicación realizada a los titulares de la Información, si aplica
7.11.5.9. Evaluación del nivel del riesgo

7.12. Capacitación y sensibilización en seguridad de la información

KEDRIÓN a través de su Representante Legal, deberá poner en conocimiento de los demás miembros de la organización la presente Política de Seguridad y Privacidad de la Información, efectuando periódicamente sensibilizaciones sobre la importancia del principio de seguridad en el Tratamiento de la información que se efectúa por parte de la organización, y las implicaciones que traería el incumplimiento del mismo.

De las sensibilizaciones que se hagan al interior de la organización, se levantará un acta donde conste: fecha de realización, tema y participantes.

8. VIGENCIA

La presente política rige a partir de la fecha de su aprobación. Las modificaciones que se den a las políticas acá descritas darán origen a una nueva versión del documento.

Dada en Bogotá D.C. a los veintidós (22) días del mes de agosto de dos mil veintidós (2022).

JUAN CARLOS BELTRÁN GONZALEZ
Representante Legal