POLÍTICA INTERNA DE TRATAMIENTO DE DATOS PERSONALES

Tabla de contenido

1. INTRODUCCIÓN

I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S, domiciliada en Bogotá D.C., Colombia e identificada con NIT 830.110.405 - 2 (en adelante, la "Sociedad"), dando cumplimiento a las normas contenidas en la Ley Estatutaria 1581 de 2012, el Decreto 1074 de 2015 y las demás normas concordantes, por las cuales se dictan disposiciones generales para la protección de datos personales, en su calidad de Responsable del Tratamiento de Datos Personales, se permite implementar la presente Política Interna de Tratamiento de Datos Personales (en adelante la "Política") para adoptar un conjunto de medidas destinadas a proteger aquella información que se reciba de los titulares de datos personales o de terceros a través de los diferentes canales de recolección de datos que ha dispuesto en el desarrollo de sus actividades.

2. OBJETIVO

El objetivo principal de la presente Política es definir los principios y las reglas básicas para la gestión de la protección de los datos personales, para de esta forma lograr que I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S, dé cumplimiento de la ley, políticas y procedimientos de atención de derechos de los titulares, criterios de recolección, almacenamiento, uso, circulación y supresión que se dará a los datos personales.

3. ALCANCE

Dar cumplimiento a las exigencias de la normatividad vigente en materia de Protección de Datos Personales, así como a cualquier exigencia originada en el principio de *responsabilidad demostrada.*

Brindar la debida protección a los intereses y necesidades de los titulares de la Información personal tratada por I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S**.**

El alcance de la presente Política abarca toda la información personal que recolecte la Sociedad con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente. La Política deberá estar y ser accesible por todos los trabajadores de la Sociedad.

4. PRINCIPIOS DE LA POLÍTICA

La presente Política responde al cumplimiento de la legislación vigente en materia de protección de datos personales. Además, la Sociedad establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de datos personales:

Principio de Legalidad en Materia de Tratamiento de Datos: El Tratamiento es una actividad reglada que debe sujetarse a lo establecido en la Ley 1581 del 17 de octubre de 2012, decretos reglamentarios y demás disposiciones que la desarrollen.

Principio de Finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Principio de Libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de Veracidad o Calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de Datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de Transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de Acceso y Circulación Restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley.
Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados

Principio de Seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de Confidencialidad: Todos los funcionarios y contratistas que intervengan en el Tratamiento de Datos Personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma. **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** se compromete a tratar los datos personales de los titulares tal y como lo define el literal g) del artículo 3 de la Ley 1581 de 2012 de forma absolutamente confidencial haciendo uso de estos, exclusivamente, para las finalidades indicadas en el apartado anterior, siempre que el titular no se haya opuesto a dicho tratamiento. **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** informa que tiene implantadas las medidas de

seguridad de índole técnica y organizativas necesarias que garanticen la seguridad de sus datos personales y eviten su alteración, pérdida, tratamiento y/o acceso no autorizado.

Principio de temporalidad: Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Una vez cumplida la finalidad del tratamiento y los términos establecidos anteriormente, se procederá a la supresión de los datos.

Interpretación integral de los derechos constitucionales: Los derechos se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los derechos constitucionales aplicables.

Principio de Necesidad: Los datos personales tratados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos.

Conocimiento: Esta Política deberá ser conocida, comprendida y asumida por todos los empleados de la Sociedad.

5. CATEGORÍAS ESPECIALES DE DATOS

5.1. Datos sensibles: 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.

5.2. Tratamiento de datos sensibles: Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
c) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
d) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

5.3. Autorización especial de datos personales sensibles: I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S informará a través de los diversos medios de obtención de la autorización a todos sus titulares, que en virtud de la ley 1581 del 2012 y normas reglamentarias estos no están obligados a otorgar la autorización para el tratamiento de datos sensibles.

En caso de tratamiento de datos relativos a la salud, I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S, implementará las medidas necesarias para proteger la confidencialidad de la información.

6. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S podrá transferir y transmitir los datos personales a terceros con quienes tenga relación operativa que le provean de servicios necesarios para su debida operación, o de conformidad con las funciones establecidas a su cargo en las leyes. En dichos supuestos, se adoptarán las medidas necesarias para que las personas que tengan acceso a sus datos personales cumplan con la presente Política y con los principios de protección de datos personales y obligaciones establecidas en la Ley.
En todo caso, cuando **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** transmita los datos a uno o varios encargados ubicados dentro o fuera del territorio de la República de Colombia, establecerá cláusulas contractuales o celebrará un contrato de transmisión de datos personales en el que indicará:

1. Alcances del tratamiento,
2. Las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y,
3. Las obligaciones del Encargado para con el titular y el responsable.

Mediante dicho contrato el Encargado se comprometerá a dar aplicación a las obligaciones del responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables vigentes.
Además de las obligaciones que impongan normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado:

1. Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
3. Guardar confidencialidad respecto del tratamiento de los datos personales.

En caso de transferencia se dará cumplimiento a las obligaciones estipuladas en la Ley 1581 de 2012 y normas reglamentarias.

7. DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

7.1. Derechos de los titulares

En el Tratamiento de Datos Personales por parte de I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S se respetarán en todo momento los derechos de los titulares de Datos Personales que son:

a) Conocer, actualizar y rectificar los Datos frente a él o los Encargados del Tratamiento de datos.

b) Solicitar prueba de la autorización otorgada, o cualquier otra que suscriba el titular de los Datos Personales para el efecto, salvo cuando expresamente se exceptúe como requisito para el Tratamiento de datos de conformidad con la ley.

c) Ser informado por la Sociedad o el Encargado del Tratamiento, previa solicitud, respecto del uso que se les ha dado a los datos.

d) Presentar ante la Autoridad Competente quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, sustituyan o adicionen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Autoridad Competente haya determinado que, en el Tratamiento **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** o Encargados del Tratamiento de Datos Personales, han incurrido en conductas contrarias a la ley y a la Constitución. La revocatoria procederá siempre y cuando no exista la obligación legal o contractual de conservar el dato personal.

f) Acceder en forma gratuita a los Datos Personales que hayan sido objeto de Tratamiento.

7.2. Autorización del titular

Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización, como cuando, por ejemplo, se remite a la Sociedad una hoja de vida para participar en procesos de selección.

7.2.1. Casos en que no es necesaria la autorización

La autorización del Titular no será necesaria cuando se trate de:

a) Información requerida por la Sociedad, en ejercicio de sus funciones legales o por orden judicial.

b) Datos de naturaleza pública.
c) Casos de urgencia médica o sanitaria.
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
e) Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la Ley 1581 de 2012 y demás normas concordantes y vigentes.

7.3. Suministro de la información

La información solicitada por los Titulares de información personal será suministrada principalmente por medios electrónicos, o por cualquier otro solo si así lo requiere el Titular.

La información suministrada por I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S será entregada sin barreras técnicas que impidan su acceso; su contenido será de fácil lectura, acceso y tendrá que corresponder en un todo a aquella que repose en la base de datos.

7.4. Deber de informar al titular

I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
c) Los derechos que le asisten como Titular.
d) La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento.

I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S como responsable del Tratamiento, deberá conservar prueba del cumplimiento de lo previsto en el presente numeral y, cuando el Titular lo solicite, entregarle copia de esta.

7.4.1. Personas a quienes se les puede suministrar la información: La información que reúna las condiciones establecidas en la ley podrá ser suministrada a las siguientes personas:

a) A los Titulares, sus causahabientes o sus representantes legales.
b) A las Sociedades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
c) A los terceros autorizados por el Titular o por la ley.

8. GESTIÓN DE LA SEGURIDAD DE PERSONAL AUTORIZADO

El Personal Autorizado deberá realizar su gestión teniendo en cuenta los criterios de seguridad establecidos en esta Política, siendo este un punto clave para asegurar su cumplimiento. Se deberán salvaguardar los requisitos establecidos en la presente Política en todo momento.

9. CONTROL DE SEGURIDAD EN PUESTOS DE TRABAJO

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.
- Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Esto incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, guardando bajo llave los que por su clasificación sean confidenciales o secretos.
- Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.
- Se establece de manera estricta la prohibición del consumo de alimentos y/o bebidas en el área designada como puesto de trabajo. Esta medida se implementa con el propósito de preservar la integridad de los equipos electrónicos y documentos sensibles, reducir el riesgo de posibles derrames que puedan comprometer la seguridad de la información, y mantener un entorno laboral ordenado y propicio para la eficiencia y la seguridad en el manejo de datos confidenciales.
- Clasificación de la información. Se deberá asignar un responsable encargado de realizar la gestión propia de los activos de información durante todo el ciclo de vida. El responsable deberá mantener un registro formal de los usuarios con acceso autorizado a dicho activo. Además, para cada activo o elemento de información deberá existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido.
- Queda estrictamente prohibido intentar corregir posibles situaciones de peligro en los puestos de trabajo, así como manipular elementos de los cuales se desconozca su funcionamiento o no se cuente con la autorización correspondiente para operarlos. Esta medida se implementa con el objetivo de salvaguardar la seguridad de los empleados y proteger la integridad de los equipos y sistemas, evitando acciones no autorizadas que puedan poner en riesgo la salud, la integridad física o la eficiencia operativa en el entorno laboral.
- Se establece como obligación del usuario el mantener exclusivamente los implementos dotados para llevar a cabo sus funciones en el puesto de trabajo, del mismo modo no mantener información que ya ha sido procesada por el trabajador.

10. CONTROL DE SEGURIDAD EN DISPOSITIVOS PERSONALES

Con el objetivo de asegurar la integridad y confidencialidad de la información de la sociedad, se establecen los siguientes requisitos en relación con el control de seguridad en dispositivos personales:

La Sociedad autoriza el uso de dispositivos personales que permitan a los empleados utilizar sus propios recursos o dispositivos móviles. Sin embargo, se establece que dichos dispositivos no estarán habilitados para acceder a recursos o información de la Sociedad. Esta medida busca conciliar la flexibilidad y comodidad para los empleados, al tiempo que se resguarda la seguridad y confidencialidad de los datos y activos de la organización, asegurando el cumplimiento de las políticas internas de seguridad de la información.

11. GESTIÓN DE LAS COPIAS DE SEGURIDAD

Con el objetivo de mitigar el riesgo de pérdida de información, la sociedad implementará las siguientes condiciones en relación con la gestión de respaldos de información:

- El usuario asume la total responsabilidad de la información almacenada en el o los PC's asignados para su uso. Se espera que el usuario evalúe la importancia de los datos y determine el período de retención necesario para la información que requiera respaldos. Estos respaldos deberán ser almacenados en los distintos drives asociados a la cuenta del usuario. Esta medida busca empoderar al usuario en la gestión y protección de su propia información, garantizando que se realicen copias de seguridad de manera acorde a sus necesidades y criterios.
- Es imperativo realizar copias de seguridad de la información en los sistemas críticos de la sociedad, las cuales deben ser verificadas periódicamente. Con el propósito de asegurar la integridad y disponibilidad de los datos, se establece la realización de backups mensuales. Estas medidas son fundamentales para garantizar la continuidad operativa y mitigar posibles pérdidas de información crítica en el entorno empresarial.
- Las copias de seguridad deberán recibir idénticas protecciones de seguridad que los datos originales, garantizando su correcta conservación y aplicando los controles de acceso apropiados. Con el objetivo de asegurar la eficacia de los procesos, se llevarán a cabo pruebas regulares de restauración tanto de las copias de seguridad como de los procedimientos definidos. Estas pruebas se realizarán periódicamente y se documentarán detalladamente, asegurando así la fiabilidad y la capacidad de recuperación de los datos en caso de eventualidades.

12. CONTROL Y MONITOREO DE ACCESO

Todos los sistemas de información de la Sociedad deberán contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas y monitoreo de consultas.

La Sociedad deberá asumir una serie de requisitos de negocio para el control de acceso, que serán, al menos, los siguientes:

- Los usuarios deberán ser únicos y no podrán ser compartidos.
- La Sociedad deberá implementar controles de acceso que garanticen que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.

La Sociedad deberá gestionar adecuadamente los controles de seguridad de la información personal para los trabajadores antes de la vinculación y una vez finalizado el contrato laboral, de manera que se puedan evitar fugas de información.

13. TRATAMIENTO DE LA INFORMACIÓN PERSONAL EN SU CICLO DE VIDA

La Sociedad deberá gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases.

El ciclo de vida de un activo de información consta de las siguientes fases:

- Creación o recolección: Esta fase se ocupa de los registros en su punto de origen. Esto podría incluir su creación por un miembro la Sociedad o la recepción de información desde una fuente externa. Incluye correspondencia, formularios, informes, dibujos, entrada/salida del ordenador u otras fuentes.
- Circulación: Es el proceso de gestión de la información una vez que se ha creado o recibido. Esto incluye tanto la distribución interna como externa, ya que la información que sale de la Sociedad se convierte en un registro de una transacción con terceros.
- Uso o acceso: se lleva a cabo después de que la información se distribuya internamente, y puede generar decisiones de negocio, generar nueva información, o servir para otros fines. Detalla el conjunto de usuarios autorizados por la Sociedad a acceder a la información.
- Almacenamiento: Es el proceso de organizar la información en una secuencia predeterminada y la creación de un sistema de gestión para garantizar su utilidad dentro la Sociedad.
- Disposición final: Establece las prácticas para la eliminación de la información que ha cumplido los periodos de retención definidos y la información personal que ha dejado de ser útil para la Sociedad, conforme su Política de tratamientos de Datos Personales. La Sociedad implementará las medidas de seguridad desarrolladas en esta Política para asegurar la correcta gestión del ciclo de vida de la información.

14. AUDITORÍAS DE SEGURIDAD Y GESTIÓN DE VULNERABILIDADES

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la Sociedad, de acuerdo con su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado. Una vez identificadas las vulnerabilidades, la Sociedad deberá aplicar las medidas correctoras

necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

15. ÁREA RESPONSABLE DE LA ATENCIÓN A PETICIONES, CONSULTAS Y RECLAMOS POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

Las peticiones, consultas y reclamos formulados por los titulares de Datos Personales bajo Tratamiento de I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S para ejercer sus derechos a conocer, actualizar, rectificar y suprimir datos, o revocar la autorización deberán ser dirigidas a:

Oficial de Protección de Datos Personales: Walter Anderson Murcia – Seguridad de la Información
Dirección: Calle 110 # 9-25 Oficina 713, Bogotá D.C.
Teléfono: (57) 320 3918396
Correo electrónico: contacto@ikm.com.co

16. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES CON DATOS PERSONALES

Se entiende por incidencia cualquier anomalía, evento o circunstancia que comprometa o pueda comprometer la seguridad, integridad, disponibilidad o confidencialidad de las bases de datos o la información alojada en ellas. Esto puede incluir, entre otros, intrusiones no autorizadas, pérdida de datos, fallos en la protección de datos, intentos de acceso no autorizado, y cualquier otro evento que represente una amenaza para la seguridad de los datos almacenados.

16.1. Notificación de Incidentes:

Todos los colaboradores, funcionarios y terceros están obligados a informar cualquier evento o incidente relacionado con la seguridad de la información. Esto incluye, pero no se limita a, intrusiones, pérdida de datos, intentos de acceso no autorizado y cualquier otra actividad sospechosa que comprometa la integridad de los datos.

Los canales disponibles para reportar estos eventos son los siguientes:

- Oficinas IKM ubicadas en Calle 110 # 9-25, Oficina 713, Torre Empresarial Pacific.
- Correo electrónico: mesa.servicio@ikm.com.co
- Línea de atención telefónica: 320 3918396

Es importante destacar que, sin excepción, independientemente del medio utilizado para reportar el evento o incidente de seguridad de la información, se debe registrar el incidente en la herramienta de solicitudes Freshdesk. Este registro asegura que se documente adecuadamente el evento, facilitando su seguimiento y gestión por parte del equipo de seguridad de la información de la organización.

16.2. Categorizar y Registrar

Una vez que el Ingeniero de Servicio y Mesa de Ayuda recibe el reporte, su primera tarea es identificar y comprender la naturaleza del incidente. Luego, procede a registrar el incidente de manera detallada, incluyendo información relevante como la hora y fecha del evento, la descripción del incidente, los posibles impactos y cualquier otra información pertinente.
Posteriormente, el Ingeniero clasifica el incidente según su gravedad y naturaleza, determinando la prioridad y la urgencia de la respuesta requerida. Esta categorización es crucial para asignar los recursos adecuados y tomar las medidas apropiadas de manera oportuna.

Una vez clasificado, el Ingeniero de Servicio y Mesa de Ayuda escala inmediatamente el incidente al Especialista de Seguridad Informática.

16.3. Recolectar Información

El Especialista de Seguridad lleva a cabo la evaluación inicial del reporte, analizando la información proporcionada y cualquier documento adjunto, si los hay. En caso necesario, se comunica con el personal relevante para recabar detalles adicionales. La clasificación del reporte puede ser una de las siguientes:

- Evento de seguridad de la información.
- Incidente de seguridad de la información.
- Falsa alarma.

Se consideran incidentes de seguridad de la información aquellos que se relacionan con:

- Denegación de Servicio.
- Hacking.
- Pruebas Maliciosas o Escaneos de Red.
- Compromiso de contraseñas.
- Compromiso de llaves de cifrado.
- Phishing (suplantación de sitios web).
- Suplantación de identidad de funcionarios.
- Eavesdropping: Escuchar Secretamente y sin autorización llamadas o comunicaciones.
- Introducción de código malicioso (Virus, gusanos, troyanos)
- Ingeniería social.
- Distribución de spam.
- Acceso no autorizado a sistemas de información o redes.
- Cambio de privilegios sobre sistemas de información sin autorización.
- Modificación o inserción de transacciones, archivos o bases de datos sin autorización.
- Descarga o envió de contenido inapropiado.
- Divulgación no autorizada de información del negocio.
- Piratería de software.
- Robo de información de negocio.

- Robo de información personal de clientes y/o funcionarios (ej.: Phishing). • Pérdida o hurto de equipo de cómputo.
- Robo de software.
- Robo de información de autenticación.
- Daño o pérdida de los servicios o enlaces de comunicaciones.
- Pérdida de energía.
- Daño o pérdida de los equipos del Centro Alterno de Datos.

Si el reporte corresponde a una falsa alarma, se debe documentar en el sistema la justificación de la decisión y posteriormente se debe cerrar y notificar a los interesados.
Si el evento o incidente de seguridad de la información, atenta contra los sistemas de información o bases de datos que contienen datos personales y es catalogado como crítico entrañando un alto riesgo para los derechos y libertades de los titulares de la información se procederá sin dilación a realizar las actividades desde el punto 16.8 en adelante.

16.4. Análisis y Evaluación del Impacto

El Especialista de Seguridad Informática de la Información tiene la responsabilidad de llevar a cabo las siguientes acciones:

- Valorar el Impacto en términos de Confidencialidad e Integridad.
- Evaluar la Urgencia, considerando la Disponibilidad.
- Determinar la Prioridad, calculada como el producto del Impacto por la Urgencia.
- Analizar la Afectación y las posibles Causas o Tipo de Ataque.

Además, el Especialista de Seguridad Informática debe informar al Especialista de Seguridad Informática para coordinar las actividades necesarias para contener, controlar y restaurar las operaciones afectadas por el incidente. Estas actividades deben ser debidamente documentadas en el sistema e incluir:

Clasificación de la criticidad del incidente, categorizándolo en función de su impacto y estableciendo el nivel de prioridad para su resolución. Las categorías son: Crítica, Grave, Moderada y Leve.

- Acciones de contención, si son necesarias.
- Acciones complementarias, si son necesarias.

16.5. Aplicar acciones de contención

El Especialista de Seguridad Informática, en colaboración con el equipo especializado del sistema de información, identifica las acciones de respuesta inmediata (contención) para abordar el incidente. Estas acciones pueden resultar en la implementación de controles de emergencia y/o controles permanentes adicionales.

El plan de acción puede incluir actividades como:

- Activación de Contingencias.

- Desconexión.
- Copia/Clonación de datos.
- Registro de posibles evidencias.
- Establecimiento de posibles causas.
- Notificación a las partes interesadas.

Si la acción de contención requiere un cambio de emergencia, se activa el proceso de Gestión de Cambios de Emergencia.

El Especialista de Seguridad Informática coordina la ejecución de las actividades del plan de acción centradas en la recuperación de la operación. Estas actividades pueden incluir:

- Ejecución de acciones de restauración.
- Implementación de medidas de remediación.
- Pruebas.
- Ejecución del plan de retorno.

Independientemente del resultado de las acciones realizadas, el Especialista de Seguridad Informática realiza un seguimiento verificando la documentación y evidencias registradas. Una vez finalizadas las acciones de contención, el Especialista de Seguridad Informática determina si el incidente de seguridad de la información está bajo control.

16.6. Aplicar acciones Complementarias

El Especialista de Seguridad Informática, junto con el equipo especializado del sistema de información, evalúa si se necesitan actividades adicionales para abordar los incidentes de seguridad de la información. Esto podría implicar la restauración de los sistemas, servicios y/o redes de información a su estado normal.
Si las acciones complementarias requieren cambios normales en el entorno, se activa el proceso de Gestión de Cambios de TI para garantizar que estos cambios se realicen de manera controlada y documentada.

16.7. Notificar

El Especialista de Seguridad Informática procede a almacenar una copia de las evidencias recopiladas y a documentar el incidente utilizando el sistema correspondiente. La información mínima que debe incluir es la siguiente:

- Fecha de solicitud.
- Nombre de la persona que diligencia el informe.
- Ubicación del incidente.
- Descripción detallada del incidente, presentada de manera cronológica para comprender los acontecimientos.
- Clasificación del incidente según el procedimiento establecido (en caso de que el evento sea considerado un incidente).

- Posibles impactos del incidente.
- Partes involucradas, con especial énfasis en la especificación de terceros, si los hay.
- Acciones realizadas hasta el momento, tanto medidas de contención como de recuperación implementadas.

16.8. Reporte en el Registro Nacional de Base de Datos RNBD

En la Plataforma tecnológica de la Superintendencia de Industria y Comercio, se debe reportar el incidente de seguridad dentro de los quince (15) días hábiles siguientes al registro del incidente o evento de seguridad.

16.9. Comunicación a los afectados

Una vez que se haya identificado el incidente de seguridad y se hayan completado todas las actividades descritas en este procedimiento, la Oficina de Seguridad de la Información comunicará al interesado de manera clara y sencilla la violación de seguridad detectada.

Además, se informarán las medidas correctivas adoptadas por la organización y se proporcionarán recomendaciones de seguridad que deben seguir los interesados.

16.10. Documentar Lecciones Aprendidas

El Especialista de Seguridad, junto con el equipo encargado de abordar el incidente, tiene la responsabilidad de identificar las lecciones aprendidas para prevenir la reincidencia de incidentes y eliminar las debilidades que fueron explotadas por la amenaza que causó el incidente de seguridad. Además, el Especialista de Seguridad es responsable de evaluar si se requieren nuevos controles o modificaciones a los existentes en la Universidad, con el fin de mejorar el proceso y la seguridad de la información de IKM.

16.11. Cerrar el Incidente

El Especialista de Seguridad informa al Ingeniero de Servicios y Mesa de Ayuda para proceder con el cierre del incidente en la herramienta de gestión correspondiente. Además, se encarga de notificar a todas las partes interesadas sobre el cierre del incidente y cualquier información relevante relacionada con el mismo.

17. PROCEDIMIENTO PARA ATENDER LOS DERECHOS DE LOS TITULARES

Los titulares de Datos Personales, sin importar el tipo de vinculación que tengan con **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S**, pueden ejercer sus derechos a conocer, actualizar, rectificar y suprimir información y/o revocar la autorización otorgada.

17.1. Procedimiento de Consultas

I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S y/o los Encargados, garantizan a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes o personas autorizadas, el derecho de consultar toda la información contenida en su registro individual o toda aquella que esté vinculada con su identificación conforme se establece en la presente Política de Tratamiento de Datos Personales.

Responsable de atención de consultas

El **Oficial de Protección de Datos Personales** de **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S**, será el responsable de recibir y dar trámite a las solicitudes remitidas, en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en las presentes políticas.

Las consultas dirigidas a **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** deberán contener como mínimo la siguiente información:

a) Nombres y apellidos del Titular y/o su representante y/o causahabientes;
b) Lo que se pretende consultar
c) Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
d) Firma, número de identificación o procedimiento de validación correspondiente.
e) Haber sido presentada por los medios de consulta habilitados por **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S**

Una vez sea recibida la solicitud de CONSULTA de información por parte del Titular de los datos o su representante o tercero debidamente autorizado, a través de los canales establecidos por **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S**, el Oficial de Protección de Datos Personales procederá a verificar que la solicitud contenga todas las especificaciones requeridas a efectos de poder valorar que el derecho se ejerza por un interesado o por un representante de éste, acreditando con ello, que se cuenta con la legitimidad legal para hacerlo.

Plazos de Respuesta a consultas
Las solicitudes recibidas mediante los anteriores medios serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo.

Prórroga del plazo de Respuesta
En caso de imposibilidad de atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

17.2 Procedimiento de Reclamos

Derechos Garantizados mediante el procedimiento de reclamos

a) **Corrección o Actualización: I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** y/o los Encargados, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de corregir o actualizar los datos personales que reposen en sus bases de datos, mediante presentación de reclamación, cuando consideren que se cumplen los parámetros

establecidos por la ley o los señalados en la presente Política de Tratamiento de Datos Personales para que sea procedente la solicitud de Corrección o Actualización.

b) **Revocatoria de la autorización o Supresión de los datos Personales: I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** y/o los Encargados, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de Solicitar la Revocatoria de la autorización o solicitar la supresión de la información contenida en su registro individual o toda aquella que esté vinculada con su identificación cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente Política de Tratamiento de Datos Personales. Así mismo se garantiza el derecho de presentar reclamos cuando adviertan el presunto incumplimiento de la Ley 1581 de 2012 o de la presente Política de tratamiento de datos personales.

Responsable de atención de Reclamos

El **Oficial de Protección de Datos Personales** de **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S**, será el responsable de recibir y dar trámite a las solicitudes remitidas, en los términos, plazos y condiciones establecidos en la Ley 1581 de 2012 y en las presentes políticas.

Las reclamaciones presentadas deberán contener como mínimo la siguiente información:

a. Nombres y apellidos del Titular y/o su representante y/o causahabientes;
b. Lo que se pretende consultar
c. Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
d. Firma, número de identificación o procedimiento de validación correspondiente.
e. Haber sido presentada por los medios de consulta habilitados por **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S**

Una vez sea recibida la solicitud de ACTUALIZACIÓN o de RECTIFICACIÓN de información por parte del Titular de los datos o su representante o tercero debidamente autorizado, a través de los canales establecidos **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** el Oficial de Protección de Datos Personales procederá a verificar que la solicitud contenga todas las especificaciones requeridas a efectos de poder valorar que el derecho se ejerza por un interesado o por un representante de éste, acreditando con ello, que se cuenta con la legitimidad legal para hacerlo.

Reclamaciones sin cumplimiento de Requisitos legales
En caso de que la reclamación se presente sin el cumplimiento de los anteriores requisitos legales, se solicitará al reclamante dentro de los cinco (5) días siguientes a la recepción del reclamo, para que subsane las fallas y presente la información o documentos faltantes.
Desistimiento del Reclamo

Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Recepción de reclamos que no correspondan a la Entidad
En caso de que **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** reciba un reclamo dirigido a otra organización, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al reclamante.

Inclusión de leyenda en la base de datos:
Recibida la reclamación de forma completa, en un término máximo de dos (2) días hábiles contados desde la recepción, **I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S** Incluirán en la base de datos donde se encuentren los datos personales del Titular, una leyenda que diga "*reclamo en trámite*" y el motivo del mismo. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

Plazos de Respuesta a los Reclamo
El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

Prórroga del plazo de Respuesta
Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Procedimiento de Supresión de Datos Personales
En caso de resultar procedente la Supresión de los datos personales del titular de la base de datos conforme a la reclamación presentada, I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S, deberá realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información, sin embargo, el Titular deberá tener en cuenta que en algunos casos cierta información deberá permanecer en registros históricos por cumplimiento de deberes legales de la organización por lo que su supresión versará frente al tratamiento activo de los mismos y de acuerdo a la solicitud del titular.

18. CAPACITACIÓN DE COLABORADORES Y CONTRATISTAS

I K M INFORMATION AND KNOWLEDGE MANAGEMENT S.A.S debe poner en conocimiento estas políticas por el medio que considere adecuado y con ello, capacitar a sus colaboradores y contratistas en la administración de los datos personales con una periodicidad al menos anual, con el fin de medir sus conocimientos sobre el particular.
Los nuevos colaboradores y contratistas, al momento de vincularse con la Sociedad, deben recibir capacitación sobre Protección de datos personales y seguridad de la información dejando constancia de su asistencia y conocimiento.

19. MODIFICACIONES A LA POLÍTICA

La Sociedad podrá modificar o enmendar esta Política de forma discrecional. Cuando se realicen modificaciones o cambios a ésta, se actualizará la fecha de la misma, y esa modificación o enmienda será efectiva a partir de la fecha de actualización. Se recomienda revisar periódicamente esta Política para estar informado acerca de las modificaciones que se puedan presentar.

20. VIGENCIA DE LA POLÍTICA

Esta Política entrará en vigencia a partir de su publicación. Tanto la Política como las Bases de Datos contentivas de la información suministrada podrá permanecer vigente hasta por el término de duración de La Sociedad, sin perjuicio de que esta política pueda ser modificada en cualquier momento y de forma unilateral por parte de la Sociedad.

HUGO HERNANDO HIGUERA
Representante Legal