Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

1. OBJETIVO

El objetivo de esta **Guía Técnica para la Gestión de Incidentes de Privacidad** es establecer un marco metodológico claro y efectivo para la identificación, clasificación, evaluación y resolución de incidentes relacionados con el tratamiento de datos personales. Esta guía asegura que los incidentes sean gestionados de manera adecuada, cumpliendo con las normativas legales vigentes y garantizando la protección de la confidencialidad, integridad y disponibilidad de la información personal de los titulares.

2. ALCANCE

Esta guía es aplicable a todos los procesos y actividades relacionados con la gestión de incidentes de privacidad dentro de la organización, desde la identificación hasta la resolución y documentación de los mismos. Establece los lineamientos que deben ser respetados y mantenidos en cualquier herramienta o mecanismo que utilice la organización para la identificación, evaluación y gestión de incidentes de privacidad.

Esta guía no reemplaza la gestión de incidentes de **TIC** o de **seguridad de la información**, sino que la complementa, centrándose en los incidentes que afectan específicamente la **privacidad** y el **tratamiento de datos personales**. Proporciona directrices para asegurar que la gestión de incidentes de privacidad se realice conforme a las mejores prácticas del mercado y en cumplimiento con las normativas aplicables, independientemente del sistema o herramienta utilizada

3. GENERALIDADES

3.1 Definiciones

Dentro de la gestión de incidentes de seguridad de datos personales es importante definir algunos conceptos que son mencionados dentro de la presente metodología de gestión de incidentes:

- **Confidencialidad**: La confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
- **Integridad**: La integridad es la propiedad de la información que busca mantener los datos libres de modificaciones no autorizadas.
- **Disponibilidad**: La disponibilidad es la propiedad de la información que busca que los datos o información puedan ser accedidos o consultados en el momento exacto en el que se requiere.
- **Gestión de incidentes de seguridad**: La gestión de incidentes de seguridad se refiere a la documentación de los pasos a seguir una vez se ha detectado un incidente de seguridad de datos personales.
- **Incidente de seguridad de datos personales:** Un incidente de seguridad datos personales se refiere a la violación de los códigos de seguridad que se han establecido velar por la confidencialidad, integridad y disponibilidad de la información.

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

- **Causales de incidentes de seguridad:** Un causal de incidente de seguridad se refiere a aquellas causas bajo los cuales se puede realizar la clasificación de un incidente de seguridad de datos personales.
- **Situaciones de riesgo**: Una situación de riesgo corresponde a un evento, comportamiento, falta de control o acción que puede dar lugar o la materialización de un incidente de seguridad de datos personales.
- **Valoración del incidente**: La valoración del incidente corresponde a la clasificación que se realiza sobre el incidente de acuerdo con los tipos de datos que se hayan visto comprometidos en el incidente.

4. FASES DE LA GESTIÓN DE INCIDENTES

La **gestión de incidentes de privacidad de datos personales** sigue un proceso estructurado por fases, alineado con las mejores prácticas del mercado para asegurar una adecuada respuesta ante incidentes que involucren datos personales de los titulares. Este proceso tiene como objetivo garantizar que todos los incidentes detectados sean identificados, clasificados y documentados, con el fin de crear una base de conocimiento que permita mejorar la respuesta ante futuros incidentes y gestionar aquellos que afecten la **confidencialidad**, **disponibilidad** e **integridad** de la información personal.

Para cumplir con este objetivo, se presentan las siguientes fases del proceso de gestión de incidentes:

Fase 0: Clasificación

El propósito de esta fase es determinar si la situación reportada constituye un incidente de privacidad. Cualquier reporte de situación, anomalía o eventualidad debe ser evaluado y clasificado. Una situación será considerada un **incidente de privacidad de datos personales** si afecta alguno de los siguientes principios: **Confidencialidad**, **Disponibilidad** o **Integridad** de los datos personales, o una combinación de estos.

A continuación, se describen los principios afectados:

Principio Afectado	Descripción
Confidencialidad de los datos personales	Este principio asegura que los datos personales sean accesibles únicamente para las personas o sistemas autorizados. Protege la privacidad y evita que la información personal sea divulgada o utilizada indebidamente, garantizando que solo aquellos con el permiso adecuado puedan acceder a ella.
Disponibilidad de los datos personales	Se refiere a la capacidad de garantizar que los datos personales estén siempre accesibles y disponibles para su uso cuando sean requeridos por las personas autorizadas. Esto implica proteger los sistemas de posibles fallos o ataques que puedan impedir el acceso a la información.

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

Integridad de los datos personales	La integridad garantiza que los datos personales permanezcan exactos, completos y no sean alterados de manera no autorizada o accidental. Este principio asegura que la información personal no sea modificada o corrompida durante su almacenamiento o transmisión
Confidencialidad y disponibilidad de los datos personales	Combina dos principios esenciales. Garantiza que los datos personales estén protegidos contra accesos no autorizados (confidencialidad) y que al mismo tiempo estén accesibles y disponibles para los usuarios o sistemas autorizados cuando sea necesario (disponibilidad).
Confidencialidad e Integridad de los datos personales	Esta combinación asegura que los datos personales solo puedan ser accedidos por personas autorizadas (confidencialidad) y que estos datos no sean modificados, alterados o corrompidos sin autorización (integridad), manteniéndose completos y precisos.
Disponibilidad e Integridad de los datos personales	Combina el acceso continuo y garantizado a los datos (disponibilidad) con la protección contra modificaciones o alteraciones no autorizadas (integridad), asegurando que la información esté siempre accesible y sin cambios indebidos.
Confidencialidad, Disponibilidad e Integridad de los datos personales	Es la integración de los tres principios clave de la seguridad de la información. Asegura que los datos personales estén protegidos contra accesos no autorizados (confidencialidad), que siempre estén disponibles para su uso (disponibilidad) y que se mantengan exactos y sin alteraciones no autorizadas (integridad). Estos principios en conjunto garantizan una gestión segura y confiable de los datos personales.

Tabla 1. Principios y sus combinaciones

Fase 1: Identificación

Una vez se determina que la situación reportada afecta al menos uno de los principios clave (Confidencialidad, Disponibilidad o Integridad), esta se clasifica como un incidente de privacidad. En esta fase, se recopila información detallada para asegurar una identificación clara del incidente. Las preguntas clave a responder en esta fase son:

1. **Descripción del incidente que se presentó:** Se debe proporcionar una descripción precisa del incidente, especificando lo que ocurrió y qué aspectos del sistema o proceso se vieron comprometidos.
2. **¿Cuándo se detectó el incidente?:** Es esencial registrar la fecha y hora exacta en que se detectó el incidente para garantizar una trazabilidad adecuada del evento y poder responder de manera oportuna.
3. **¿Cuál fue la situación que dio origen al incidente?:** Se debe identificar la causa subyacente del incidente, como un error humano, una falla en el sistema o un ataque externo, que generó la vulnerabilidad.
4. **¿Qué o quién identificó el incidente?:** Aquí se debe detallar si el incidente fue detectado por un sistema automatizado, un miembro del equipo, un cliente, o cualquier otra fuente interna o externa que dio aviso sobre el problema.

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

5. **¿De los titulares que tiene identificados, cuáles se vieron afectados?:** Es necesario identificar a las personas cuyos datos personales fueron afectados, diferenciando entre las distintas categorías de titulares (empleados, clientes, proveedores, etc.).
6. **¿De los tipos de datos que tiene identificados, cuáles se vieron afectados?:** Se debe especificar las categorías que clasifican o agrupan datos personales como nombres, direcciones, números de identificación, diplomas, certificados de estudio, etc.
7. **¿De los tipos de datos sensibles que tiene identificados, cuáles se vieron afectados?:** En caso de que se hayan comprometido datos sensibles, como información de salud, religiosa, política o relacionada con menores, es importante registrar qué tipos específicos de datos sensibles fueron afectados.

Toda esta información debe ser documentada y almacenada en un registro central de incidentes. Este proceso es esencial para formar una visión clara y precisa del incidente, lo que permitirá una respuesta informada y eficaz.

Fase 2: Impacto

En esta fase se busca evaluar las consecuencias del incidente en términos de la afectación a los datos personales y la organización. A través de una serie de preguntas clave, se determina el alcance del daño y se establece una base para priorizar las acciones correctivas y de mitigación. Las preguntas a responder en esta fase incluyen:

1. **¿El acceso NO autorizado a la información personal se detuvo en?:** Se debe documentar el tiempo en el que se logró contener el acceso no autorizado. Las posibles respuestas incluyen "de inmediato", "menos de una hora", "menos de un día", "menos de una semana", "menos de un mes" o "más de un mes". Este aspecto es crucial para determinar la gravedad del incidente y las acciones requeridas.
2. **¿Quién tuvo acceso a la información personal?:** Es importante identificar si el acceso fue realizado por personal interno no autorizado, terceros no autorizados, hackers maliciosos, o si el acceso no ha podido ser identificado. Esta información ayudará a evaluar el riesgo potencial para los titulares y la organización.
3. **¿Se afectaron datos de menores (niños, niñas o adolescentes) ?:** Es esencial determinar si el incidente involucró datos sensibles de menores de edad, ya que esto puede aumentar significativamente la gravedad y las repercusiones legales del incidente.
4. **¿El incidente es una situación recurrente o aislada?:** Aquí se busca establecer si este tipo de incidentes ha ocurrido anteriormente o si se trata de un evento único. Los incidentes recurrentes pueden indicar una vulnerabilidad o riesgo sistemático dentro de la organización que requiere atención prioritaria.
5. **¿Cuál es el porcentaje (%) de personas afectadas del total que podrían verse afectadas?:** Se debe calcular el porcentaje de titulares afectados por el incidente en relación con el número total de personas cuyos datos personales estaban en riesgo. Este porcentaje proporciona una medida cuantitativa del impacto.

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

6. **El impacto del incidente para la organización es:** Se evalúa el impacto del incidente en la operación, la reputación, las relaciones con los clientes, y las posibles consecuencias legales

o regulatorias. Esto incluye determinar si el incidente ha generado daños financieros, pérdidas de confianza o interrupciones significativas en los procesos internos. Un incidente de privacidad puede clasificarse entonces en cuatro (4) niveles de impacto:

Nivel de Impacto	Descripción o criterio
IMPACTO BAJO:	El acceso no autorizado fue detectado y detenido **de inmediato o en menos de una hora**. Los datos comprometidos no son sensibles ni incluyen información de menores. El incidente fue causado por **personal interno sin mala intención**, y el acceso fue limitado a un pequeño grupo de personas. El incidente es aislado, no recurrente, y solo afecta a un **porcentaje mínimo de titulares**. Las consecuencias para las personas afectadas son prácticamente nulas, ya que la información no fue usada de manera inapropiada ni expuesta de forma significativa.
IMPACTO MEDIO	El acceso no autorizado fue detenido en **menos de un día**, involucrando a **personal interno o terceros no maliciosos**. Los datos comprometidos incluyen información personal, pero no son extremadamente sensibles ni se han visto afectados datos de menores. El incidente es **aislado** y afectó a un porcentaje moderado de titulares, aunque la naturaleza del acceso no indica intenciones maliciosas. Las personas afectadas podrían experimentar consecuencias limitadas, como molestias o vulneraciones menores de su privacidad, pero no sufren daños significativos.
IMPACTO ALTO	El acceso no autorizado fue detectado y detenido en **menos de una semana**. El incidente involucra a **hackers maliciosos o terceros no autorizados con intención de comprometer la información**. Los datos comprometidos son sensibles y críticos, y **existe una alta probabilidad de que se vean comprometidos datos de menores**. El incidente podría ser **recurrente**, afectando a un porcentaje significativo de titulares. Las consecuencias para las personas afectadas son graves, ya que se expuso información crítica que puede ser utilizada para fines malintencionados, como fraudes, robo de identidad o daños reputacionales.
IMPACTO GRAVE	El acceso no autorizado fue contenido **después de más de una semana, más de un mes, o no pudo ser detenido**. Este incidente involucra a **hackers maliciosos o terceros con intenciones peligrosas**. Los datos comprometidos son extremadamente sensibles, incluyendo información personal crítica y **datos de menores**. El incidente afecta a **un alto porcentaje de los titulares** o a la mayoría de ellos, y puede ser recurrente o sistémico. Las repercusiones para los afectados son críticas y peligrosas, con consecuencias severas que incluyen fraudes masivos, daños financieros, uso indebido de la información y exposición a riesgos físicos o emocionales.

Tabla 2. Niveles de impacto establecidos para un incidente y su criterio

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

Este análisis detallado de la fase de impacto permite una comprensión clara del daño causado por el incidente, tanto en los titulares como en la organización, y facilita la priorización de las acciones de recuperación

Fase 3: Afectación

En esta fase se examinan los daños o afectaciones generadas por el incidente desde diferentes perspectivas: los titulares de los datos personales, la organización y el entorno en general. Esta evaluación integral es esencial para comprender el verdadero alcance del incidente y para planificar las acciones de mitigación correspondientes. Las preguntas clave a responder son:

1. **¿Qué daño o afectación generó el incidente sobre los titulares de datos personales?:** Se analiza cómo el incidente ha afectado directamente a las personas cuyos datos personales fueron comprometidos. Esto puede incluir daños financieros, como fraudes o robos de identidad, afectaciones emocionales o psicológicas, pérdida de confianza en la organización, o cualquier otra consecuencia negativa directa sobre los titulares. Además, se debe considerar si los datos sensibles, como los de menores o datos de salud, han amplificado el impacto.
2. **¿Qué daño o afectación generó el incidente para la organización?:** En esta parte se evalúa el impacto sobre la organización, que puede incluir daños reputacionales, pérdida de clientes, sanciones regulatorias, costos asociados a la contención y mitigación del incidente, así como posibles demandas legales. También se considera cómo el incidente ha afectado la operación diaria de la organización y si ha generado interrupciones significativas en los procesos internos.
3. **¿Qué daño o afectación generó el incidente para el público o el entorno?:** Se examina si el incidente ha tenido repercusiones más allá de los titulares de los datos y la organización, afectando a terceros o al público en general. Esto puede incluir la erosión de la confianza pública en la organización o en el sector al que pertenece, o impactos negativos en la comunidad, en los socios comerciales o en otras partes interesadas. En los casos más graves, el incidente puede tener repercusiones a nivel de la industria o incluso en la percepción pública sobre la seguridad de los datos personales.

Esta fase es fundamental para obtener una visión integral del daño causado, no solo a nivel interno de la organización, sino también en términos de las personas afectadas y el entorno más amplio.

Fase 4: Contención

En esta fase, el enfoque está en detener el avance del incidente y minimizar sus efectos. Una respuesta rápida y efectiva es esencial para evitar que el incidente cause mayores daños. Las preguntas clave que se deben responder en esta fase son:

1. **¿Qué acciones realizó para detener o contener el incidente o su propagación?:** Aquí se describen las acciones inmediatas que la organización tomó para frenar el incidente. Esto puede incluir la restricción de accesos, la desconexión de sistemas comprometidos, la

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

actualización de contraseñas, la revocación de permisos de usuarios, o cualquier medida técnica y operativa que haya sido implementada para contener la situación.

2. **Acciones adicionales que llevó a cabo para detener o contener el incidente:** En esta pregunta se documentan acciones complementarias o posteriores que se implementaron.

3. para reforzar la contención del incidente. Estas medidas pueden incluir la implementación de parches de seguridad, la reconfiguración de sistemas, la colaboración con equipos externos de ciberseguridad o la notificación a autoridades regulatorias. El objetivo es detener por completo cualquier riesgo residual que pudiera haber quedado sin atender tras las primeras medidas de contención.

Esta fase es crucial para asegurar que el incidente no siga propagándose y que la organización recupere el control de la situación, reduciendo al mínimo el impacto negativo sobre los datos personales y la operación

Fase 5: Prevención

Esta fase está enfocada en identificar e implementar medidas que eviten la recurrencia del incidente y fortalezcan la seguridad de los datos personales. Es esencial aprender del incidente para mejorar los controles y procesos de la organización. Las preguntas clave que se deben responder en esta fase son:

1. **¿Qué acciones realizará para evitar o prevenir que el incidente vuelva a ocurrir?:** Aquí se deben describir las medidas preventivas que la organización implementará para corregir las vulnerabilidades detectadas y asegurar que el mismo tipo de incidente no vuelva a ocurrir. Esto puede incluir la actualización de políticas internas, la implementación de nuevas herramientas de seguridad, la revisión de permisos de acceso, o la capacitación del personal.
2. **Acciones adicionales que llevará a cabo para prevenir y evitar que vuelva a ocurrir:** Esta pregunta aborda cualquier otra medida complementaria que la organización planea ejecutar para fortalecer su sistema de protección de datos. Estas acciones adicionales pueden incluir auditorías de seguridad, revisiones periódicas de los sistemas, mejoras en la infraestructura tecnológica, o la implementación de monitoreo continuo para detectar posibles incidentes de manera proactiva.

Esta fase es clave para asegurar que el aprendizaje del incidente se traduzca en mejoras concretas, minimizando la probabilidad de que el mismo tipo de incidente se repita en el futuro.

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

5. SEGUIMIENTO

El seguimiento es una etapa fundamental para comprobar que las acciones realizadas en las fases de contención y prevención han sido efectivas. El objetivo es garantizar que la organización ha restaurado la normalidad y ha fortalecido la seguridad para prevenir futuros incidentes.

La **organización** es responsable de llevar a cabo un seguimiento exhaustivo de todos los elementos que forman parte de la gestión de incidentes. Esto incluye la revisión de las acciones ejecutadas, la evaluación de su efectividad y la implementación de mejoras necesarias para reducir riesgos futuros. Los responsables dentro de la organización deben elaborar informes periódicos para el comité o la alta dirección, según la frecuencia de sus reuniones y la criticidad de los incidentes. La efectividad de la gestión se medirá mediante indicadores definidos previamente, que proporcionarán una visión clara del desempeño de las acciones tomadas.

La documentación de cada incidente se realizará utilizando un formato o sistema de información designado por la organización. El almacenamiento y la gestión de estos registros deberán realizarse de manera adecuada, asegurando que se cumplan los lineamientos establecidos para la administración técnica de los sistemas y la integridad de la información.

6. COMUNICACIÓN DE INCIDENTES

La comunicación en caso de incidentes debe ajustarse al nivel de impacto del incidente, asegurando que tanto las autoridades como los titulares de los datos sean informados de manera adecuada. A continuación, se detalla el plan de comunicación basado en los diferentes niveles de impacto.

1. Impacto Bajo

Criterio	El acceso no autorizado fue detectado y detenido **de inmediato o en menos de una hora**. Los datos comprometidos no son sensibles ni incluyen información de menores. El incidente fue causado por **personal interno sin mala intención**, y el acceso fue limitado a un pequeño grupo de personas. El incidente es aislado, no recurrente, y solo afecta a un **porcentaje mínimo de titulares**. Las consecuencias para las personas afectadas son prácticamente nulas, ya que la información no fue usada de manera inapropiada ni expuesta de forma significativa.
Acciones de Comunicación	• Reporte a las autoridades: Si la normativa lo exige específicamente, se debe reportar a través de los canales oficiales establecidos y de acuerdo con la información requerida por el ente regulador. • Comunicación a los Titulares: No es necesario comunicar el incidente a los titulares, ya que el impacto es mínimo. Solo se documentará internamente.

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

Medios de Comunicación	• Si se debe notificar a las autoridades, comunicación formal a través de los canales oficiales requeridos por la entidad reguladora. • No se requiere el uso de ningún medio para informar a los titulares.
Documentación	Se debe registrar el incidente internamente, asegurando que los detalles, evaluaciones y acciones tomadas queden documentadas para futuras revisiones o auditorías.

Tabla 3. Criterios para la comunicación de un incidente de impacto Bajo

2. Impacto Medio

Criterio	El acceso no autorizado fue detenido en **menos de un día**, involucrando a **personal interno o terceros no maliciosos**. Los datos comprometidos incluyen información personal, pero no son extremadamente sensibles ni se han visto afectados datos de menores. El incidente es **aislado** y afectó a un porcentaje moderado de titulares, aunque la naturaleza del acceso no indica intenciones maliciosas. Las personas afectadas podrían experimentar consecuencias limitadas, como molestias o vulneraciones menores de su privacidad, pero no sufren daños significativos.
Acciones de Comunicación	• Reporte a las autoridades: Si la normativa lo exije específicamente, se debe reportar a través de los canales oficiales establecidos y de acuerdo con la información requerida por el ente regulador. • Comunicación a los Titulares: La comunicación a los titulares es opcional y depende de la decisión de la organización. Si se decide notificar, debe incluir una explicación clara del incidente y las medidas preventivas que los titulares pueden tomar.
Medios de Comunicación	• Si se debe notificar a las autoridades, comunicación formal a través de los canales oficiales requeridos por la entidad reguladora. • Si se notifica a los titulares, el canal puede ser correo electrónico general o personalizado, según la magnitud del incidente.
Documentación	Registrar el análisis del incidente, la decisión de notificación (si aplica), y la información proporcionada a las autoridades y/o titulares. Todo el proceso debe ser documentado como párte de la gestión de incidentes.

Tabla 4. Criterios para la comunicación de un incidente de impacto Medio

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

3. Impacto Alto

Criterio	El acceso no autorizado fue detectado y detenido en **menos de una semana**. El incidente involucra a **hackers maliciosos o terceros no autorizados con intención de comprometer la información**. Los datos comprometidos son sensibles y críticos, y **existe una alta probabilidad de que se vean comprometidos datos de menores**. El incidente podría ser **recurrente**, afectando a un porcentaje significativo de titulares. Las consecuencias para las personas afectadas son graves, ya que se expuso información crítica que puede ser utilizada para fines malintencionados, como fraudes, robo de identidad o daños reputacionales.

Acciones de Comunicación	• Reporte a las autoridades: Si la normativa lo exije específicamente, se debe reportar a través de los canales oficiales establecidos y contar con por lo menos
	  ○ Descripción del incidente.
	  ○ Categorías de datos comprometidos.
	  ○ Número estimado de personas afectadas.
	  ○ Medidas adoptadas para contener y mitigar el incidente.
	  ○ Otros datos que pueda requerir la autoridad de vigilancia y control
	• Comunicación a los Titulares: La comunicación es obligatoria a los titulares, informando como minimo:
	  ○ La naturaleza del incidente.
	  ○ Los datos comprometidos.
	  ○ Consejos para que los titulares se protejan (cambio de contraseñas, monitoreo financiero, etc.).
	  ○ Acciones que la organización ha tomado para mitigar el daño.

Medios de Comunicación	• Si se debe notificar a las autoridades, comunicación formal a través de los canales oficiales requeridos por la entidad reguladora. • Notificación directa a los titulares mediante correo electrónico, llamadas telefónicas, msg u otros canales que aseguren que la comunicación y la información a compartir llegue rápidamente.
Documentación	Se debe mantener un registro detallado de las comunicaciones con las autoridades y titulares, incluyendo los informes enviados, los tiempos de notificación y las respuestas recibidas. Esta documentación debe ser accesible para auditorías y revisiones regulatorias.

Tabla 5. Criterios para la comunicación de un incidente de impacto Alto

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

4. Impacto Grave

Criterio	El acceso no autorizado fue contenido **después de más de una semana, más de un mes, o no pudo ser detenido**. Este incidente involucra a **hackers maliciosos o terceros con intenciones peligrosas**. Los datos comprometidos son extremadamente sensibles, incluyendo información personal crítica y **datos de menores**. El incidente afecta a **un alto porcentaje de los titulares** o a la mayoría de ellos, y puede ser recurrente o sistémico. Las repercusiones para los afectados son críticas y peligrosas, con consecuencias severas que incluyen fraudes masivos, daños financieros, uso indebido de la información y exposición a riesgos físicos o emocionales

Acciones de Comunicación	• Reporte a las Autoridades: Si la normativa lo exije específicamente, se debe realizar una notificación urgente a las autoridades de control, proporcionando un informe detallado que incluya:
	  ○ La descripción completa del incidente.
	  ○ Las acciones inmediatas de contención.
	  ○ El número y tipo de datos comprometidos.
	  ○ El plan de mitigación y prevención de futuros incidentes.
	  ○ Otros datos que pueda requerir la autoridad de vigilancia y control
	• Titulares: Notificación inmediata a los titulares afectados, proporcionando:
	  ○ Información clara sobre los datos comprometidos.
	  ○ Riesgos potenciales para los titulares.
	  ○ Acciones preventivas que los titulares deben tomar.
	  ○ Medidas que la organización ha tomado para controlar el incidente.

Medios de Comunicación	• Si se debe notificar a las autoridades, comunicación formal a través de los canales oficiales requeridos por la entidad reguladora. • Se deben emplear múltiples medios de comunicación para asegurar que todos los titulares afectados reciban la información. Estos pueden incluir correos electrónicos, llamadas telefónicas, publicaciones en el sitio web de la organización o notas de prensa si el incidente afecta a un gran número de personas.
Documentación	Toda la documentación relacionada con la comunicación debe ser precisa y completa, incluyendo: • Los informes enviados a las autoridades. • Las notificaciones a los titulares. • Las acciones y respuestas recibidas de ambas partes. • Los plazos y fechas clave en todo el proceso

Tabla 6. Criterios para la comunicación de un incidente de impacto Alto

Cra. 13 #N° 51-25 Oficina 312, (Bogotá - Colombia)
3112754665 - 3203602262
l.leguizamon@leguizamonasesorias.com

Este enfoque estructurado permite abordar la comunicación de incidentes en función del nivel de impacto, garantizando que las acciones sean proporcionales al daño potencial y que se cumplan las obligaciones legales y operativas.