CONTENIDO

[1 OBJETIVO 2](#_Toc141215125)

[2 DESTINATARIOS 2](#_Toc141215126)

[3 GLOSARIO 2](#_Toc141215127)

[4 GENERALIDADES 7](#_Toc141215128)

[5 DESCRIPCION DE ACTIVIDADES 7](#_Toc141215129)

[5.1 REALIZAR LA RECEPCIÓN Y ESCALAMIENTO DEL INCIDENTE 7](#_Toc141215130)

[5.2 ANALISIS TECNICO DEL INCIDENTE 8](#_Toc141215131)

[5.2.1 Validación de Información RUES 8](#_Toc141215132)

[5.2.2 Validación de Información RNBD 10](#_Toc141215133)

[5.2.3 Validaciones en el sistema de trámites 12](#_Toc141215134)

[5.2.4 Validación de Vulnerabilidades WEB 14](#_Toc141215135)

[5.3 Identificar preguntas relacionadas con el incidente reportado 15](#_Toc141215136)

[5.4 CLASIFICACION MANUAL DEL INCIDENTE 16](#_Toc141215137)

[5.4.1 Severidad Baja 16](#_Toc141215138)

[5.4.2 Severidad Media 16](#_Toc141215139)

[5.4.3 Severidad Alta 17](#_Toc141215140)

[6 DOCUMENTOS RELACIONADOS 19](#_Toc141215141)

[7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN 19](#_Toc141215142)

# OBJETIVO

Describir los criterios y operatividad de la gestión para la Clasificación y tratamiento para los incidentes relacionados con las bases de datos personales reportadas a la Delegatura de protección de datos personales por los diferentes medios dispuestos por la entidad con este fin; a través del desarrollo de las actividades descritas en este documento, las cuales serán desarrolladas por los Servidores públicos y/o contratistas del Grupo de Trabajo de Investigaciones Administrativas encargados de realizar revisiones técnicas y jurídicas según sea cada caso.

# DESTINATARIOS

Este instructivo aplica para todos los Servidores públicos y/o contratistas del Grupo de Trabajo de Investigaciones Administrativas que tienen la función de clasificar, ordenar, analizar y evaluar técnicamente los incidentes relacionados con las bases de datos personales reportadas a la Delegatura de protección de datos personales por medio de Reporte físico, Reporte electrónico o de oficio.

# GLOSARIO

**Acceso** **no** **autorizado**: Se produce cuando un usuario, legítimo o no autorizado, tiene acceso a un recurso que no tiene permitido utilizar.

**Aceptación** **del** **riesgo**: Decisión informada para tomar un riesgo en particular.

**Activo**: Cualquier recurso o capacidad.

**Alcance**: Límite o extensión, a la que un proceso, procedimiento, certificación, contrato, entre otros aplica.

**Análisis**: La tercera fase del proceso de forense digital que implica el uso legal de métodos y técnicas justificables para obtener información útil que aborde las cuestiones que fueron el impulso para llevar a cabo la recopilación y examinación.

**Ataque**: Intento de destruir, exponer, modificar, inutilizar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

**Autenticación**: Garantía de que una característica reclamada por una entidad es correcta. Verificación de la identidad de un usuario, proceso o dispositivo, a menudo como requisito previo para permitir el acceso a los recursos en un sistema de información.

**Aviso** **de** **Privacidad**: Documento físico, electrónico o en cualquier otro formato (visual, sonoro, etc.) generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con lo que establece la Ley.

**Cadena** **de** **custodia**: Un proceso que sigue el movimiento de la evidencia a través de la recolección, preservación y el análisis mediante la documentación de cada persona que maneja la evidencia, la fecha y hora en la que fue recolecta o transferida, y el propósito de la transferencia.

**Categorías** **de** **seguridad**: La caracterización de la información o un sistema de información basado en una evaluación de los posibles efectos que la pérdida de confidencialidad, integridad o disponibilidad de dicha información o sistema de información podría tener en las operaciones, activos, o personal de la organización.

**Clasificación**: El acto de asignar automática o manual una categoría, en el caso de incidentes se refiere a MUY ALTO, ALTO, MEDIO O BAJO.

**Confidencialidad**: Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

**Consecuencia**: Resultado de un evento que afecta a los objetivos.

**Contramedida**: Acciones, dispositivos, procedimientos, técnicas u otras medidas que reduzcan la vulnerabilidad de un sistema de información. Sinónimo de controles de seguridad y salvaguardas.

**Control** **de** **seguridad**: Controles administrativos, operativos y técnicos prescritos para un sistema de información a fin de proteger la confidencialidad, integridad y disponibilidad del sistema y su información y o datos personales.

**Criterio**: Requisitos o reglas para tomar una decisión o resolución.

**Datos** **personales**: Cualquier información que refiera a una persona física que pueda ser identificada a través de los mismos, los cuales se pueden expresar en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

**Datos** **personales** **sensibles**: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que pueden revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, y preferencia sexual.

**De oficio**: El Despacho tiene conocimiento de la ocurrencia de un incidente a través de algún medio externo sin que la sociedad Responsable o Encargada hubiera reportado el mismo, en este caso se da apertura a la investigación de oficio.

**Disponibilidad**: Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. Garantizar el acceso oportuno y confiable, y el uso de información.

**Evidencia** **digital**: Información electrónica almacenada o transferida en formato digital.

**Gestión** **de** **incidentes**: Procesos para controlar y administrar las tareas asociadas a incidentes de seguridad; implica la gestión de un incidente e incluye todos los procesos de detección, triage y respuesta, así como los procesos de preparación y protección.

**Gestión** **de** **seguridad** **de** **la** **información**: Proceso que garantiza la confidencialidad, integridad y disponibilidad de los activos de una organización, información, datos personales y servicios de TI.

**Imagen** **forense**: Una copia bit a bit del medio original, incluyendo el espacio libre y espacio no asignado.

**Impacto**: Medida del efecto de un incidente, problema o cambio en los procesos del negocio. La magnitud del daño que se puede esperar resultado de las consecuencias de la divulgación, modificación o destrucción no autorizada de información, o pérdida de la disponibilidad del sistema de información o información.

**Incidente**: Una interrupción no planificada de un servicio de TI o reducción de la calidad de un servicio de TI. Una violación o la amenaza inminente de la violación de las políticas de seguridad, las políticas de uso aceptable o prácticas de seguridad estándar.

**Incidente** **de** **seguridad**: Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Integridad**: Propiedad de exactitud e integridad.

**Intrusión**: Acto no autorizado de eludir los mecanismos de seguridad de un sistema.

**Lecciones** **aprendidas**: Conocimiento que se gana o identifica después de una actividad completada.

**Manejo** **de** **incidentes**: Procesos utilizados para evitar un incidente, incluye los procesos de detección, notificación, triage, análisis y respuesta a incidentes de seguridad en cómputo.

**Mejores** **prácticas**: Actividades o procesos probados que se han utilizado con éxito por varias organizaciones.

**Monitoreo**: Observación repetida de un elemento de configuración, servicio de TI o proceso para detectar eventos y asegurar que el estado actual es conocido.

**Plan** **de** **respuesta** **a** **incidente**: La documentación de un conjunto predeterminado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de ataques cibernéticos maliciosos contra los sistemas de información de una organización.

**Políticas** **de** **seguridad** **de** **la** **información**: Conjunto de directivas, reglamentos, normas y prácticas que describe cómo una organización gestiona, protege y distribuye su información.

**Procedimiento**: Documento que contiene los pasos que especifican la forma de lograr una actividad.

**Proceso**: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados. Un programa en ejecución.

**Protocolo**: Conjunto de reglas y formatos, semánticas y sintácticas, que permite a los sistemas de información el intercambio de información.

**Pruebas** **de** **seguridad**: Proceso para determinar si un sistema de información protege los datos y mantiene la funcionalidad como se pretende.

**Recolección**: Primera fase del proceso de análisis forense digital que consiste en identificar, etiquetar, registrar y adquirir los datos de las posibles fuentes de datos relevantes, mientras que se siguen directrices y procedimientos que permitan preservar la integridad de los datos.

**Recuperación**: Regresar un elemento de configuración o un servicio de TI a su estado funcional.

**Registro** **Nacional** **de** **Base** **de** **Datos:** El Registro Nacional de Bases de Datos (RNBD) es un módulo vinculado al SISI, por medio del cual se da cumplimiento a la obligación incorporada en el artículo 25 de la Ley 1581 de 2012 y demás decretos reglamentarios, en virtud de la cual los responsables del Tratamiento deben inscribir las bases de datos sujetas a tratamiento, las políticas de tratamiento implementadas por la organización, el registro de incidentes relacionado con las bases de datos.

**Remediación**: El acto de corregir una vulnerabilidad o eliminar una amenaza. Existen tres posibles tipos de remediación: instalación de un parche, ajustes de configuración o desinstalación de una aplicación.

**Reporte físico**: ocurre cuando se radica directamente en la Superintendencia en soporte físico o a través del correo de la entidad [contactenos@sic.gov.co](mailto:contactenos@sic.gov.co).

**Reporte electrónico**: se realiza a través del enlace dispuesto en el Registro Nacional de Base de Datos – RNBD el cual se encuentra en la página web www.sic.gov.co.

**Respaldo** **(Backup)**: Copia de datos para protegerlos de la pérdida de integridad o disponibilidad de los datos originales.

**Respuesta** **a** **incidentes**: Una respuesta dada o una acción tomada por las personas designadas para reaccionar ante un incidente. Es el proceso que comprende la planificación, coordinación y ejecución de las estrategias y acciones de mitigación y recuperación.

**Riesgo**: Una medida del grado en el que una entidad se ve amenazada por una circunstancia potencial o evento, y por lo general una función de: (i) impactos adversos que surgirían si se produce la circunstancia o evento; y (ii) la probabilidad de ocurrencia.

**Triage**: El proceso de recepción, clasificación inicial, y priorización de la información para facilitar su manejo adecuado.

**Virus**: Un programa informático que puede copiarse a sí mismo e infectar una computadora sin el permiso o conocimiento del usuario. Un virus podría dañar o eliminar datos en la computadora, utilizar programas de correo electrónico para propagarse a otros equipos, o incluso borrar todo el contenido de un disco duro.

**Vulnerabilidad**: Una debilidad en un sistema, aplicación o red que está sujeta a la explotación o uso indebido.

# GENERALIDADES

Se debe llevar una ordenada clasificación de los incidentes relacionados con las bases de datos personales que son reportados a la Delegatura de protección de datos personales, la cual permita determinar si el tratamiento y la gestión de incidentes son adecuados según los niveles de criticidad determinados para cada caso y basados en la ley 1581 del 2012 y sus decretos reglamentarios.

# DESCRIPCION DE ACTIVIDADES

La gestión del análisis y clasificación manual de los incidentes de seguridad reportados a la Delegatura de Protección de Datos Personales se realizará siguiendo las fases y acciones que se describen a continuación:

## REALIZAR LA RECEPCIÓN Y ESCALAMIENTO DEL INCIDENTE

Inicialmente el Responsable y/o Encargados del Tratamiento, personas naturales o jurídicas generan el ***reporte físico*** de incidentes de seguridad a por medio de radicación directa en la Superintendencia en soporte físico, o por correo electrónico [contactenos@sic.gov.co](mailto:contactenos@sic.gov.co), de estos dos métodos se obtiene un número de radicado único. Esta radicación es entregada a la Dirección de Protección de datos personales, al Servidor Público y/o contratista que se encarga de avocar y es asignado al Servidor Público y/o contratista que se encarga de revisarlo y clasificarlo como incidente asignando el perfil de radicación (Trámite 424 “Incidentes” con Evento 0 y la Actuación 411“Presentación”), finalmente se asigna y notifica al Servidor Público del laboratorio forense para su análisis técnico a través del sistema de trámites con la tarea *“Para Estudio Técnico - 615”*.

El Responsable y/o Encargado tiene la opción a través del enlace dispuesto en el Registro Nacional de Base de Datos – RNBD el cual se encuentra en la página web [www.sic.gov.co](http://www.sic.gov.co), de realizar el ***reporte electrónico*** de los incidentes de seguridad, este automáticamente es clasificado en el sistema de tramites como incidente (Trámite 424 “Incidentes” con Evento 0 y la Actuación 411“Presentación”) estos incidentes se incluyen dentro de la gestión masiva de incidentes.

Para los incidentes ***de Oficio***, el Despacho tiene conocimiento de la ocurrencia de un incidente de seguridad a través de algún medio externo, por esto se da apertura a la investigación originada en la Dependencia 7100 dirigido a la Dependencia 7111 con trámite 384 evento 330 actuación 706, 654, con posterioridad a ello al determinar que en efecto la información corresponde a un incidente se procede a realizar cambio de trámite al 424, esto es realizado por el Servidor Público que se encarga de revisarlo, se asigna para dar inicio a la actuación preliminar con el envío de requerimiento a la sociedad con el fin de precisar ampliación de los hechos que originaron el incidente y la gestión dada al mismo.

## ANALISIS TECNICO DEL INCIDENTE

Los análisis técnicos de incidentes son solicitados por la Delegatura para la Protección de Datos Personales, la Dirección de Investigaciones Administrativas o el grupo de trabajo de Investigaciones Administrativas, al Servidor público y/o contratista del laboratorio forense, el designado radicara un informe técnico con la actuación 359 *“entrega de evaluación”* acompañado de los anexos necesarios, a continuación, se describen los pasos realizados.

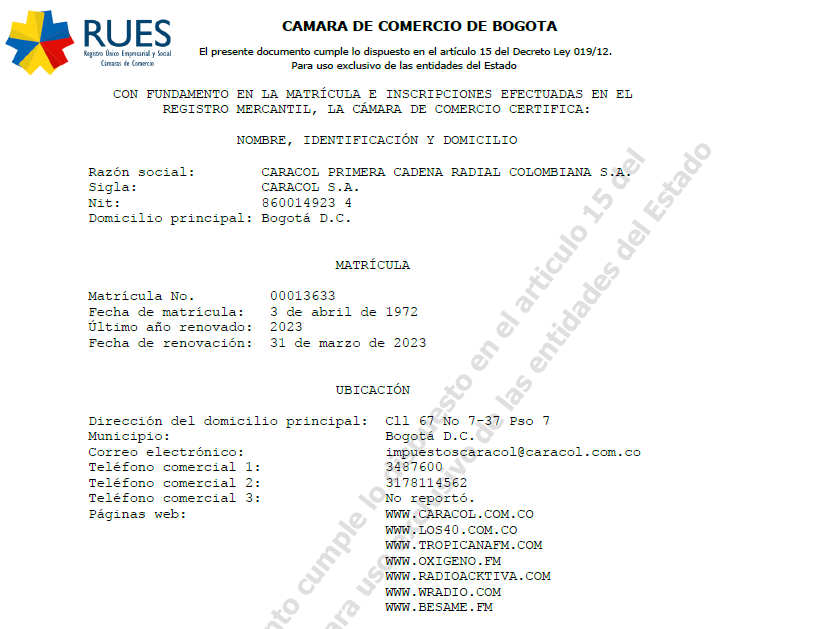
### Validación de Información RUES

El Servidor público y/o contratista al cual le fue asignado el análisis técnico del incidente, inicia validando la información de la sociedad consultando en el RUES y descargando el certificado mercantil si la sociedad se encuentre registrada.

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

* Ingresar a la plataforma RUES desde la página web https://[www.rues.org.co/,](http://www.rues.org.co/) el acceso se realiza mediante usuario y contraseña asignado por la Dirección, se ejecuta la búsqueda mediante el número de Identificación y/o el nombre de la razón social como se observa a continuación.
* La búsqueda arroja los datos de las empresas asociadas y se validan los resultados, se consulta el listado de sociedades se observa la información requerida de la razón social que reporta el incidente, este certificado se anexa al acta de análisis.

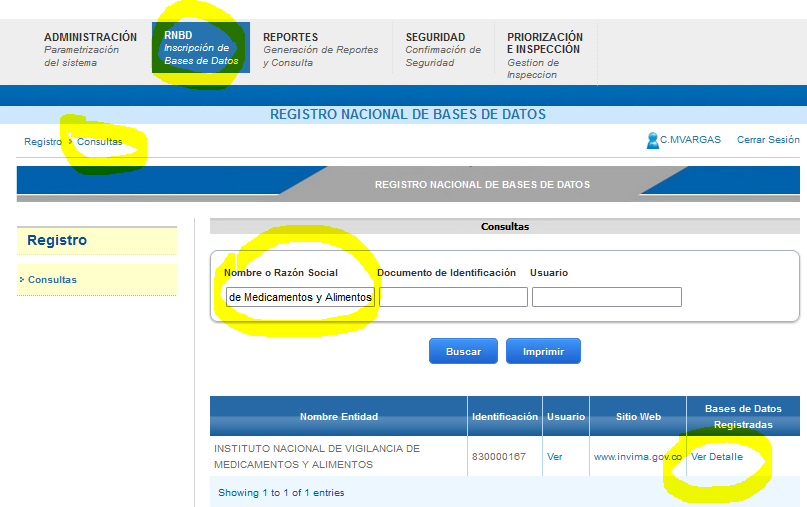


### Validación de Información RNBD

El Servidor público y/o contratista al cual le fue asignado el análisis técnico del incidente, inicia validando la información de la sociedad consultando en el RNBD este se accede por medio del enlace <https://rnbd.sic.gov.co/sisi/login> con un usuario de dominio y contraseña habilitados anteriormente en el sistema, con el fin de validar si la sociedad registro sus bases de datos, los datos contenidos y documentación complementaria relacionada con el incidente reportado.



* Cuando se inicia la sesión se debe dirigir al módulo RNBD Inscripción de Base de Datos, a la opción Consultas donde se podrá buscar por medio de los campos Nombre o Razón Social, Documento de identificación o por medio del Usuario.
* Con el resultado de búsqueda deberá seleccionar la opción Ver detalle para visualizar las Bases de Datos de la Razón Social Registrada y/o incidentes previos o el reportado, en este punto se deberá ir a la Base de Datos de interés del incidente y seleccionar la opción Consultar Registro, para observar toda la información de interés.



Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* Se realizan las capturas de pantallas que se consideren relacionadas con el incidente reportado y se anexa al acta de análisis, en el caso de que se encuentre algún documento adjunto al incidente este de igual manera se anexa al acta.

### Validaciones en el sistema de trámites

El Servidor público y/o contratista al cual le fue asignado el análisis técnico del incidente, realiza la validación de la información consultando el número de radicado del incidente en el sistema de tramites ([*http://10.20.100.5/~hmurillo/Tramites1/Ingreso.php*](http://10.20.100.5/~hmurillo/Tramites1/Ingreso.php)), este se accede por medio de un usuario de dominio y contraseña habilitados anteriormente en el sistema, con el fin de validar documentación complementaria relacionada con el incidente reportado, confirmar el canal de reporte del incidente, traslado o apertura de oficio y acceder al sistema para la descarga de la documentación aportada por la sociedad responsable y/o encargada, así mismo el estado del trámite.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Se verá reflejado el resultado de la búsqueda en sistema de trámites en donde se deberá dirigir al icono en forma de lupa, al seleccionarlo se visualizarán los documentos relacionados en el radicado.

Una captura de pantalla de una red social

Descripción generada automáticamente

* Cuando se observa que es requerido el acceso a documentos dispuestos en la nube mediante “One Drive, Google Drive, Share Point, entre otros” se debe Informar al servidor público y/o contratista abogado encargado del incidente para requerir el acceso en caso de encontrarse bloqueado y que esta información sea necesaria para determinar la gestión adecuada del incidente reportado.
* En caso de que se deban analizar documentos que no se encuentren en el sistema de trámites y estén disponibles en la nube externa de la entidad mediante “*One Drive, Google Drive, Share Point, entre otros*” y los mismos sean necesarios para determinar la gestión adecuada del incidente reportado se anexaran al acta.
* Se deben identificar radicados relacionados con el incidente reportado, en este caso se incluye en el informe un Cuadro resumen donde se indiquen los responsables, encargados, duplicados, entre otros y se procederá a solicitar la acumulación de estos al Servidor público encargado de esta actividad.

### Validación de Vulnerabilidades WEB

El escaneo de vulnerabilidades WEB, se ejecutan en el caso de los incidentes donde se identifique que los recursos web afectados realice tratamiento de Datos Personales, el escaneo se realiza por medio de una herramienta especializada para realizar la actividad, este efectúa un análisis técnico de vulnerabilidades técnicas presentes en los recursos publicados en la web.

En el caso que en el reporte del escaneo se puedan evidenciar vulnerabilidades técnicas Criticas (*Criticas, Altas y Medias*), se procede a anexar el reporte generado y se incluyen estos hallazgos de seguridad al informe de análisis del incidente.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

## Identificar preguntas relacionadas con el incidente reportado

Después de la lectura del incidente reportado y revisión de los documentos encontrados en las plataformas anteriormente descritas, se adjunta un listado básico de las preguntas que se deberían realizar a la razón social que reportó el incidente en caso de no tener claridad o presentar dudas adicionales que no se encuentren debidamente documentadas en el reporte inicial, estas pueden variar de acuerdo con el incidente.

* ¿Cuál es la Información relacionada con el tratamiento del incidente?
* ¿Cuáles son las Políticas de seguridad de la información?
* ¿Cuáles son las políticas de protección de datos?
* ¿Existen acuerdos de confidencialidad suscritos con los empleados?
* ¿Qué tipo de datos personales se vieron comprometidos en el incidente?
* Protocolos, mecanismos y medidas de seguridad establecidos;
* Medidas correctivas implementadas luego del incidente;
* Los reportes o inconformidad del titular y posibles otros titulares afectados por este incidente, informar si a la fecha se han presentado quejas o reclamos relacionados con el incidente y los canales por los que han sido recibidos y la gestión dada, Adjuntar los procedimientos de queja o reclamo que permitan el reporte.
* Auditorias, pruebas y demás métodos para comprobar el seguimiento, la remediación y efectividad de las acciones correctivas que se presentaron en el incidente reportado.
* Informar los medios por los cuales se les notifico a los titulares sobre el incidente.
* Teniendo en cuenta las oportunidades de mejora reportadas, informar cuales han sido implementadas y allegar información que soporte dicha implementación.
* Procedimiento para la generación de copias de respaldo de la información.
* Procedimiento para la gestión de contraseñas.
* Procedimiento para el cifrado de medios removibles.
* Gestión del incidente reportado, adjuntar todas las evidencias de la contención, tratamiento, planes de acción y lecciones aprendidas.
* Métodos de sensibilización de la Política tratamiento de datos personales o incidentes presentados.

## CLASIFICACION MANUAL DEL INCIDENTE

Se inicia el proceso de diligenciamiento de los formatos PD01-F07 *Informe* *De* *Análisis* *de* *Incidente* *de* *Seguridad* o *PD01-F08* *Informe* *de* *Seguimiento* *de* *Análisis* *de* *Incidente*, de esta manera se procede a la clasificación por severidad definido en tres niveles descrito a continuación:

### Severidad Baja

* En el incidente se identifica que no hay afectación de datos personales y no se encuentra en peligro la integridad, confidencialidad o disponibilidad de la información.
* Los datos afectados se clasifiquen como Públicos y/o pertenezcan a personas mayores de 18 años.
* El Informe se registra en el sistema de trámites y entrega copia digital del acta al Servidor Público Jurídico quien lo asigna en reparto para que se tome una decisión administrativa según su criterio y el documento técnico radicado.

### Severidad Media

* Se identifica la afectación de datos personales o se encuentra sin determinar.
* En el incidente se identifica afectación de la integridad o confidencialidad o disponibilidad de la información. (Sólo uno)
* La descripción del incidente y soluciones se encuentran completas y de conformidad con el análisis realizado por el encargado de la clasificación y tratamiento del caso.
* Los controles y las medidas aplicadas se encuentran completas y de conformidad con el análisis realizado por el encargado de la clasificación y del tratamiento del caso.
* Los datos afectados se clasifiquen como Públicos, semi-públicos y/o pertenezcan a personas mayores de 18 años.
* El Informe se registra en el sistema de trámites y entrega copia digital del acta al Servidor Público Jurídico quien lo asigna en reparto para que se tome una decisión administrativa según su criterio y el documento técnico radicado.

### Severidad Alta

* Se identifica la afectación de datos personales o se encuentra sin determinar.
* En el incidente se identifica afectación en la integridad, la confidencialidad o la disponibilidad de los datos personales (más de uno o los tres simultáneamente).
* La descripción del incidente y la gestión descrita en la documentación aportada no es de conformidad con el análisis técnico realizado por el Servidor Público.
* Los controles y las medidas aplicadas no se encuentran soportadas y/o no hay conformidad con el análisis técnico realizado por el Servidor Público.
* Los datos afectados son privados y/o sensibles y/o biométricos o de otras categorías especiales, que pertenezcan a personas mayores de 18 años y/o menores de 18 años.
* Se vean afectadas mas de una base de datos o más de una sociedad.
* Se tiene en cuenta si existen reincidencias relacionadas con el mismo tipo de incidente.
* Se tiene en cuenta si existen reincidencias con el reporte de incidentes por la misma sociedad.
* El Informe se registra en el sistema de trámites y entrega copia digital del acta al Servidor Público Jurídico quien lo asigna en reparto para que se tome una decisión administrativa según su criterio y el documento técnico radicado.

Según la tabla se puede observar la severidad de acuerdo con los criterios descritos en los puntos anteriores:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Clasificación** | **Afectación** **Datos** | **Tipos** **de** **Datos** **Afectados** | | |
| **Mayores** **de** **18** **Años**  **Datos** **Públicos** | **Mayores** **de** **18** **Años**  **Datos**  **Semi-** **Privados** | **Mayores** **de** **18** **Años** **Menores** **de** **18** **Años**  **Datos** **Privados**  **Datos** **Sensibles**  **Datos** **Biométricos**  **Datos Categorías Especiales** |
| **Severidad** **Baja** | ***Ninguna*** | ***Ninguna*** | ***Ninguna*** | ***Ninguna*** |
| **Severidad** **Media** | ***Afectación Pilares de Seguridad***  -Integridad  -Confidencialidad  -Disponibilidad  ***(Solo*** ***Uno).*** |  |  |  |
| **Severidad** **Alta** | ***Afectación Pilares de Seguridad***  -Integridad  -Confidencialidad  -Disponibilidad  ***(Varios*** ***Factores de*** ***Afectación simultáneos)*** |  |  |  |

***Tabla*** ***1 - Mapa*** ***de*** ***Calor*** ***Análisis*** ***de*** ***severidad*** ***de*** ***incidente*** ***de*** ***seguridad***

En el informe de análisis del incidente de seguridad se debe plasmar técnicamente los puntos:

* La explicación clara del incidente de seguridad reportado.
* Identificar la afectación en datos personales y detallarlo.
* Identificar y describir la estrategia para, contener y mitigar el incidente reportado.
* Identificar la relación con terceros y las responsabilidades sobre el incidente reportado, si aplica.
* Evaluación de la pertinencia de las acciones realizadas según el incidente reportado, en los roles de responsable y encargado.

Para determinar si las medidas de seguridad fueron apropiadas y la gestión del incidente de seguridad adecuada, se deben analizar las medidas técnicas, humanas o administrativas.

# DOCUMENTOS RELACIONADOS

* PD01-F07 Formato Informe De Análisis De Incidente De Seguridad
* PD01-F08 Formato Informe De Seguimiento De Análisis De Incidente
* PD01-P01 Procedimiento de Investigaciones Sobre Posibles Violaciones a las Normas Sobre Protección de Datos Personales.

# RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

|  |
| --- |
| Se incluye la validación de Vulnerabilidades WEB  Se modifican algunos ítems en la clasificación manual de la severidad de un incidente.  Se realiza la actualización de los métodos de recepción de incidentes. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Fin documento