CONTENIDO

1 OBJETIVO 2
2 DESTINATARIOS 2
3 GLOSARIO 2
4 GENERALIDADES 10
5 DESCRIPCION DE ACTIVIDADES 10
5.1 Realizar la recepción y escalamiento del incidente 10
5.2 Realizar análisis del incidente 11
5.2.1 Validar la información 11
5.2.2 Validar registro de la Razón Social 13
5.2.3 Verificar el sistema de trámites para validar la documentación relacionada al incidente. 17
5.3 Identificar preguntas relacionadas con el incidente reportado (si aplica). 19
5.4 Clasificar y dar tratamiento 20
5.4.1 Severidad Baja 20
5.4.2 Severidad Media 21
5.4.3 Severidad Alta 22
6 DOCUMENTOS RELACIONADOS 23
7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN 24

COPIA NO CONTROLADA

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: María Isabel Vargas Pérez Cargo: Contratista	Nombre: Carlos Enrique Muñoz Salazar Cargo: Director de Investigación de Protección de Datos Personales	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2019-07-31

Cualquier copia impresa, electrónica o de reproducción de este documento sin la marca de agua o el sello de control de documentos, se constituye en copia no controlada.

1 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 y / o por medio del RNBD; a través del desarrollo de las actividades descritas en este documento, las cuales serán desarrolladas por los funcionarios y/o contratistas del Grupo de Trabajo de Investigaciones Administrativas

2 DESTINATARIOS

Este instructivo aplica para todos los servidores públicos y contratistas que tienen la función de clasificación y tratamiento para los incidentes relacionados con las bases de datos personales reportadas a la Delegatura de protección de datos personales y/o por medio del RNBD.

3 GLOSARIO

Acceso: Capacidad para hacer uso de cualquier recurso de sistema de información.

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

Aceptación: Acuerdo formal en el que un servicio de TI, proceso, plan o cualquier otra prestación, esté completo, sea preciso, confiable y cumple con requisitos específicos.

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

Actividad: Conjunto de acciones destinadas a lograr un resultado particular.

Activo: Cualquier recurso o capacidad.

Alcance: Límite o extensión, a la que un proceso, procedimiento, certificación, contrato, etc. 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.

COPIA NO CONTROLADA

Archivo: Conjunto de información lógicamente agrupada en una sola entidad y referenciada por un único nombre, como el nombre de archivo.

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 una categoría a algo.

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.

Contraseña: Cadena de caracteres (letras, números y otros símbolos) utilizada para autenticar la identidad o verificar la autorización de acceso.

Control: Un medio de la gestión de riesgos, para asegurar que se cumple un objetivo de negocio o se sigue un proceso.

Control de seguridad: Controles administrativos, operativos y técnicos (por ejemplo, salvaguardas y contramedidas) prescritos para un sistema de información

COPIA NO CONTROLADA

a fin de proteger la confidencialidad, integridad y disponibilidad del sistema y su información.

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

Criticidad: Una medida del grado en el que una organización depende del sistema de información o información para el éxito de una misión o función de negocio.

Cumplimiento: Asegurar que una norma o conjunto de directrices se siguen o se están utilizando otras prácticas adecuadas.

Dato: Un subconjunto de la información en un formato electrónico que le permite ser recuperado o transmitido.

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.

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

Documento: Información en forma legible. El documento puede estar en papel o electrónico.

Escalamiento: Una actividad que obtiene recursos adicionales cuando éstas sean necesarias para cumplir los objetivos de nivel de servicio o las expectativas del cliente.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

Evento de seguridad de la información: Ocurrencia identificada de un sistema, servicio o estado de la red que indica un posible incumplimiento de la política de seguridad o la falla de controles, o una situación previamente desconocida que puede ser relevante en términos de seguridad.

COPIA NO CONTROLADA

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

Falla: Pérdida de la capacidad para operar según las especificaciones, o para entregar la salida requerida.

Firma digital: Una operación de clave asimétrica, donde se utiliza la clave privada para firmar digitalmente los datos y la clave pública para verificar la firma. Las firmas digitales proporcionan protección de autenticidad, integridad y no repudio.

Función: Equipo o grupo de personas y las herramientas utilizadas para llevar a cabo uno o más procesos o actividades.

Gestión de incidentes: Procesos para controlar y administrar las tareas asociadas a incidentes de seguridad en cómputo; 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 y servicios de TI.

Identificación: El proceso de verificación de la identidad de un usuario, proceso o dispositivo, por lo general, como requisito previo para conceder el acceso a los recursos en un sistema 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

COPIA NO CONTROLADA

de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Infraestructura de TI: Todo el hardware, software, redes, instalaciones, etc., que son necesarios para desarrollar, probar, entregar, supervisar, controlar o apoyar los servicios de TI.

Ingeniería social: Un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que se puede utilizar para atacar sistemas o redes.

Integridad: Propiedad de exactitud e integridad.

Interrupción: Un acontecimiento imprevisto que provoca que un sistema de información sea inoperable durante un periodo de tiempo.

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.

Lista de control de acceso (ACL): Una lista de los permisos asociados a un objeto. La lista específica de quién o qué tiene permitido acceder al objeto y qué operaciones puede llevar a cabo en el objeto.

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.

Mecanismo: Un objeto de evaluación que incluye temas específicos relacionados con la protección (por ejemplo, el hardware, software o firmware) empleados dentro o en los límites de un sistema de información.

Mejora: Cambios o avances deseables en la calidad de algo.

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

Metadato: Datos sobre los datos.

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

COPIA NO CONTROLADA

No conformidad: Incumplimiento de un requisito.

No repudio: Capacidad de probar la ocurrencia de un evento o una acción solicitada y sus entidades de origen. Garantía de que el remitente de la información cuenta con la prueba de la entrega y el destinatario cuenta con la prueba de la identidad del emisor, por lo que no puede negar haber procesado dicha información.

Perímetro de seguridad: Un límite físico o lógico que se define para un sistema, dominio o enclave, en el que se aplica una política de seguridad o arquitectura de seguridad en particular.

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.

Probabilidad: Posibilidad de que algo suceda.

Problema: La causa de uno o más incidentes.

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

Procedimientos de recuperación: Acciones necesarias para restaurar los archivos de un sistema de información y la capacidad de cómputo después de un fallo en el sistema.

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.

Prueba: Actividad que verifica que un elemento de configuración, servicio de TI, proceso, etc. cumple con las especificaciones y requisitos acordados.

COPIA NO CONTROLADA

Prueba de penetración: Una metodología de prueba en la que los evaluadores, utilizan toda la documentación disponible (por ejemplo, el diseño del sistema, código fuente, manuales) y trabajan bajo restricciones específicas, intentando eludir las características de seguridad de un sistema de información.

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

Punto de recuperación objetivo (RPO): Recovery Point Objective. Es el punto en el tiempo en el cual los datos deben ser recuperados después de una interrupción.

Punto único de fallo: Cualquier elemento de configuración que puede causar un incidente cuando falla, y para el cual no se ha aplicado una contramedida.

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: Documento que contiene los resultados o salidas de un proceso o actividad y puede ser en papel o electrónico.

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 etc., y su principal objetivo es conformar un directorio público de bases de datos que operan en el país

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.

Requisito: Necesidad o expectativa establecida, generalmente implícita u obligatoria.

Resolución: Acción tomada para reparar la causa raíz de un incidente o problema, o la implementación de una solución.

COPIA NO CONTROLADA

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.

Revisión: Actividad emprendida para asegurar la conveniencia, adecuación y efectividad del tema en cuestión para alcanzar los objetivos establecidos.

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.

Salvaguarda: Medidas de protección prescritos para cumplir con los requisitos de seguridad (es decir, la confidencialidad, integridad y disponibilidad) especificado para un sistema de información.

Sector: La unidad más pequeña que se puede acceder en los medios.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema: Un número de cosas relacionadas que trabajan en conjunto para lograr un objetivo en general.

Sistema de archivos: Un método para nombrar, almacenar, organizar y acceder a los archivos en volúmenes lógicos.

Sistema de información: Aplicaciones, servicios, activos de tecnología de información u otros componentes para el manejo de información.

Solución: Reducir o eliminar el impacto de un incidente o problema para los que una solución completa no está disponible todavía.

Spam: Correo no deseado. El abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.

SSL: Secure Socket Layer. Protocolo utilizado para proteger información sensible durante la transmisión vía internet.

COPIA NO CONTROLADA

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

Usuario: Individuo o proceso (sistema) autorizado a acceder a un sistema de información.

Validación: Confirmación a través de la aportación de evidencia objetiva, de que los requisitos para un uso o aplicación específica se han cumplido.

Verificación: Confirmación a través de la presentación de pruebas objetivas, en el que los requisitos específicos han sido cumplidos.

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.

4 GENERALIDADES

Se debe llevar una ordenada clasificación de los incidentes relacionados con las bases de datos personales reportadas a la Delegatura de protección de datos personales y / o por medio del RNBD, la cual permita determinar si el tratamiento y la gestión de incidentes son adecuados según los niveles de criticidad determinados por cada caso y basados en la ley 1581 del 2012.

5 DESCRIPCION DE ACTIVIDADES

La gestión de clasificación y de tratamiento de los incidentes de seguridad reportados en el registro nacional de bases de datos RNBD y/o a la Delegatura de protección de datos personales, se realizará siguiendo las fases y acciones que se describen a continuación:

5.1 Realizar la recepción y escalamiento del incidente

Inicialmente la empresa, o una persona natural genera un reporte de incidente de seguridad por medio de correo electrónico contactenos@sic.gov.co, o por medio físico, el cual se realiza en la oficina de radicación, de estos dos métodos se obtiene un número de radicado único. Esta radicación es entregada a la Dirección de Protección de datos personales, al funcionario y/o contratista que se encarga

COPIA NO CONTROLADA

de abocar clasificando como incidente, y al mismo tiempo asigna el perfil de radicación (***Tramite 424, Evento 0, Actuación 411***).

Finalmente se Asigna y notifica al funcionario y/o contratista asignados para su análisis correspondiente.

5.2 Realizar análisis del incidente

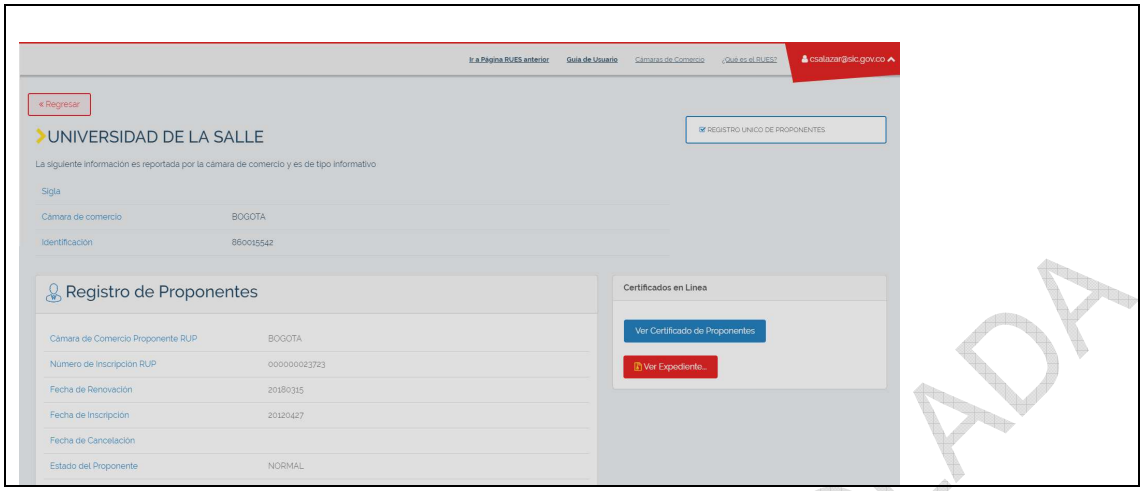
5.2.1 Validar la información

El funcionario o contratista encargado del incidente de la base de datos que la razón social reportó en el RNBD y/o a la Delegatura de Protección de Datos Personales, mediante el RUES, debe realizar las siguientes actividades:

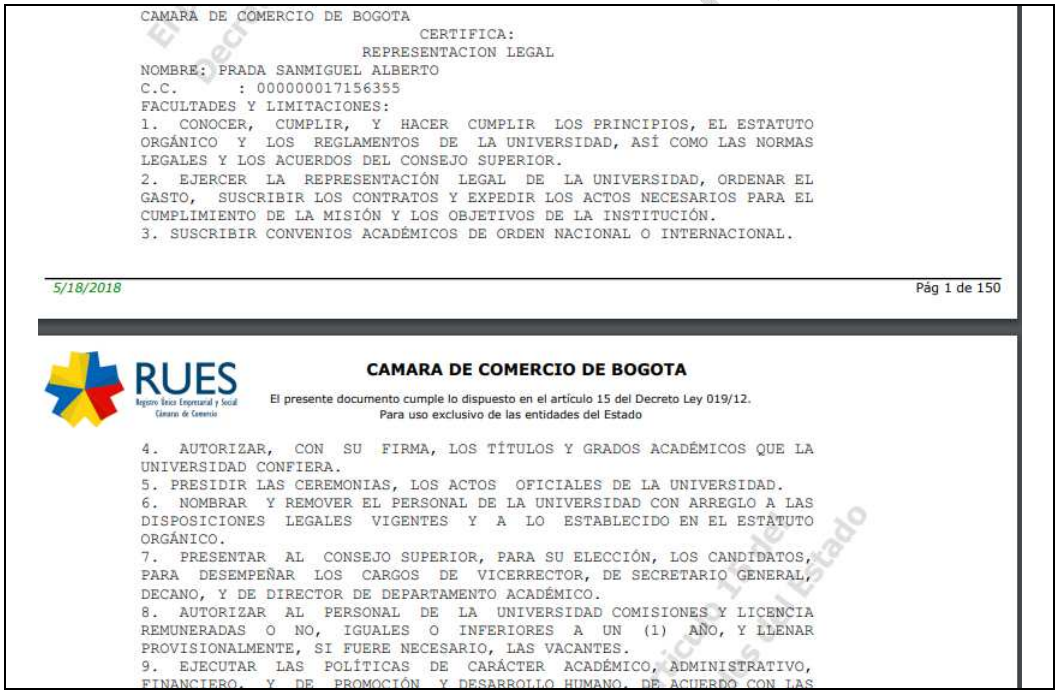
- Ingresar a la plataforma RUES desde la página web https://www.rues.org.co/,

- Efectuar la búsqueda por medio de dos opciones que el RUES ofrece, mediante el número de Identificación y el nombre de la razón social.

- Diligenciar la información requerida, este muestra en una pantalla los datos de las empresas asociadas.



- Posteriormente, se procede a descargar el Certificado Mercantil donde esta especificada toda la información requerida de la razón social que reporta el incidente, este Certificado debe ser anexado al análisis del incidente.



CAMARA DE COMERCIO DE BOGOTA

CERTIFICA:

REPRESENTACION LEGAL

NOMBRE: PRADA SANMIGUEL ALBERTO
C.C. : 000000017156355
FACULTADES Y LIMITACIONES:
1. CONOCER, CUMPLIR, Y HACER CUMPLIR LOS PRINCIPIOS, EL ESTATUTO ORGÁNICO Y LOS REGLAMENTOS DE LA UNIVERSIDAD, ASÍ COMO LAS NORMAS LEGALES Y LOS ACUERDOS DEL CONSEJO SUPERIOR.
2. EJERCER LA REPRESENTACIÓN LEGAL DE LA UNIVERSIDAD, ORDENAR EL GASTO, SUSCRIBIR LOS CONTRATOS Y EXPEDIR LOS ACTOS NECESARIOS PARA EL CUMPLIMIENTO DE LA MISIÓN Y LOS OBJETIVOS DE LA INSTITUCIÓN.
3. SUSCRIBIR CONVENIOS ACADÉMICOS DE ORDEN NACIONAL O INTERNACIONAL.

5/18/2018 Pág 1 de 150

RUES Registro Único Empresarial y Social Cámaras de Comercio

CAMARA DE COMERCIO DE BOGOTA

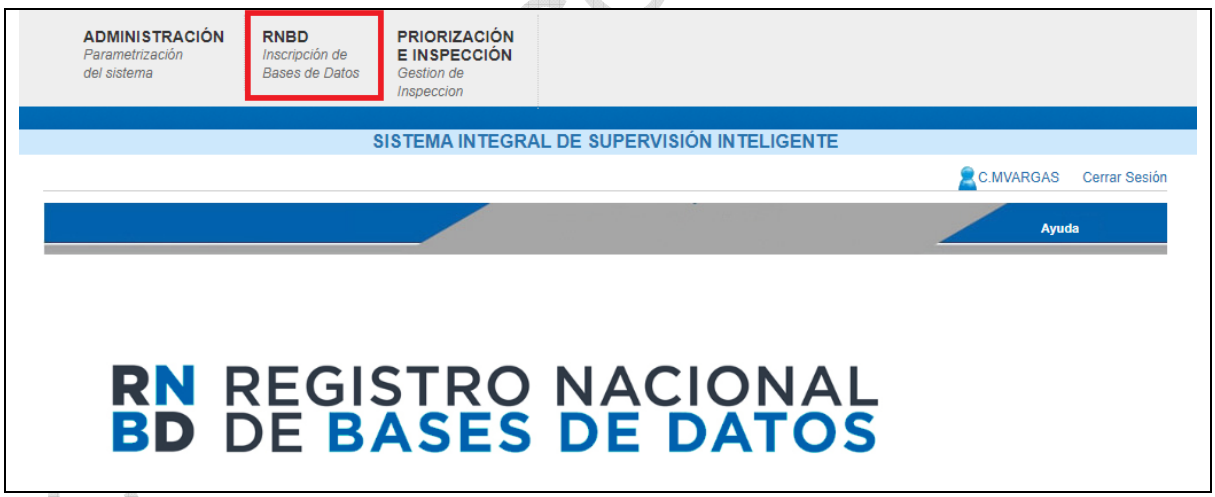
El presente documento cumple lo dispuesto en el artículo 15 del Decreto Ley 019/12.
Para uso exclusivo de las entidades del Estado

4. AUTORIZAR, CON SU FIRMA, LOS TÍTULOS Y GRADOS ACADÉMICOS QUE LA UNIVERSIDAD CONFIERA.
5. PRESIDIR LAS CEREMONIAS, LOS ACTOS OFICIALES DE LA UNIVERSIDAD.
6. NOMBRAR Y REMOVER EL PERSONAL DE LA UNIVERSIDAD CON ARREGLO A LAS DISPOSICIONES LEGALES VIGENTES Y A LO ESTABLECIDO EN EL ESTATUTO ORGÁNICO.
7. PRESENTAR AL CONSEJO SUPERIOR, PARA SU ELECCIÓN, LOS CANDIDATOS, PARA DESEMPEÑAR LOS CARGOS DE VICERRECTOR, DE SECRETARIO GENERAL, DECANO, Y DE DIRECTOR DE DEPARTAMENTO ACADÉMICO.
8. AUTORIZAR AL PERSONAL DE LA UNIVERSIDAD COMISIONES Y LICENCIA REMUNERADAS O NO, IGUALES O INFERIORES A UN (1) AÑO, Y LLENAR PROVISIONALMENTE, SI FUERE NECESARIO, LAS VACANTES.
9. EJECUTAR LAS POLÍTICAS DE CARÁCTER ACADÉMICO, ADMINISTRATIVO, FINANCIERO, Y DE PROMOCIÓN Y DESARROLLO HUMANO, DE ACUERDO CON LAS

5.2.2 Validar registro de la Razón Social

El funcionario o contratista encargado realiza esta verificación por medio del Ingreso al RNBD por medio del enlace https://rnbd.sic.gov.co/sisi/login, este se accede por medio de un usuario de dominio y contraseña habilitados anteriormente en el sistema.

Cuando se inicia la sesión se debe dirigir al módulo RNBD Inscripción de Base de Datos



En el módulo el funcionario o contratista encargado deberá dirigir a la opción Consultas donde se podrá hacer la buscar la Razón Social por medio de los campos Nombre o Razón Social, Documento de identificación o por medio del Usuario.

CONTROLADA

Opción 1: Búsqueda por medio de Nombre o Razón Social.

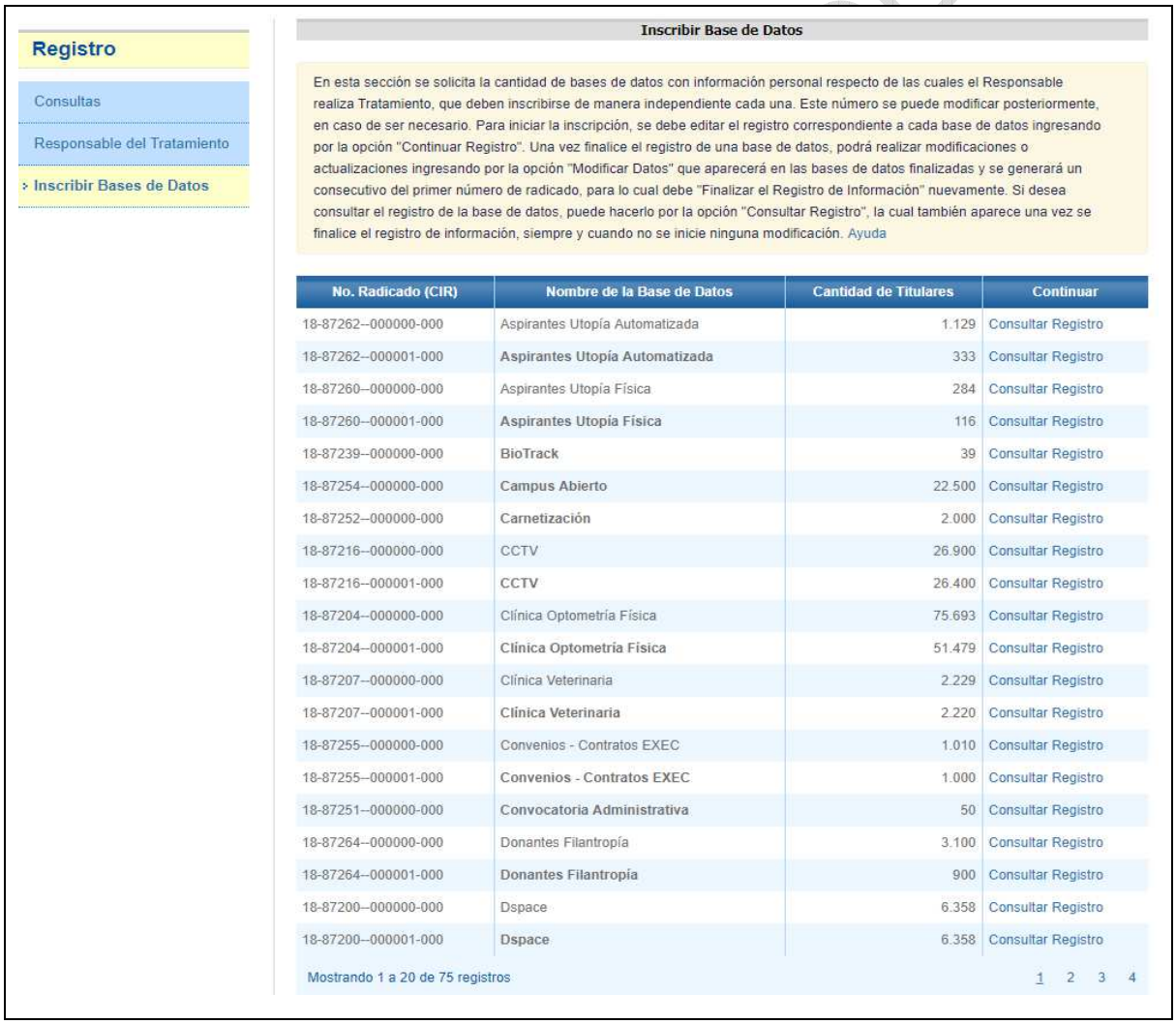
Opción 2: Búsqueda por medio de Documento de identificación.

Con el resultado de búsqueda deberá dar click en la opción Ver detalle para visualizar a detalle lo que la Razón Social ha Registrado a la fecha.

Nombre Entidad	Identificación	Usuario	Sitio Web	Bases de Datos Registradas
UNIVERSIDAD DE LA SALLE	860015542	Ver	www.lasalle.edu.co	Ver Detalle

Mostrando 1 a 1 de 1 registros

La visualización de las Bases de Datos de la Razón Social Registrada, en este punto el usuario deberá ir a la Base de Datos de interés del incidente y dará click en la opción Consultar Registro.



Registro

- Consultas
- Responsable del Tratamiento
- Inscribir Bases de Datos

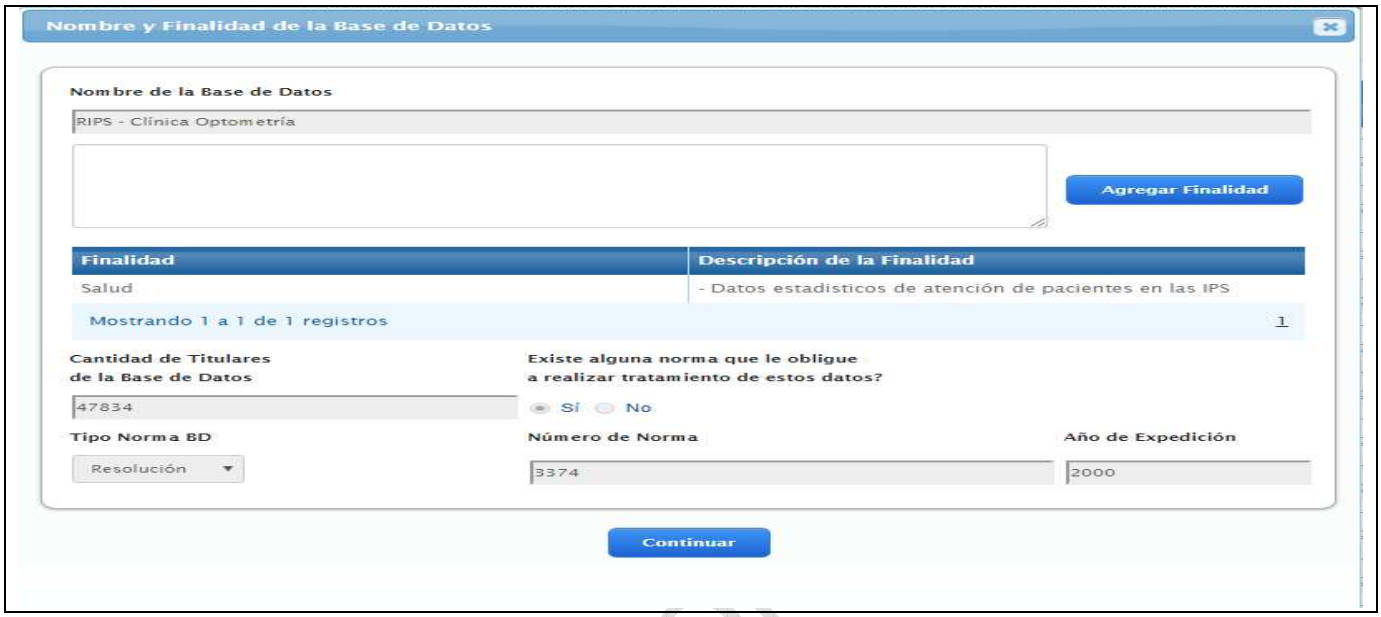
Inscribir Base de Datos

En esta sección se solicita la cantidad de bases de datos con información personal respecto de las cuales el Responsable realiza Tratamiento, que deben inscribirse de manera independiente cada una. Este número se puede modificar posteriormente, en caso de ser necesario. Para iniciar la inscripción, se debe editar el registro correspondiente a cada base de datos ingresando por la opción "Continuar Registro". Una vez finalice el registro de una base de datos, podrá realizar modificaciones o actualizaciones ingresando por la opción "Modificar Datos" que aparecerá en las bases de datos finalizadas y se generará un consecutivo del primer número de radicado, para lo cual debe "Finalizar el Registro de Información" nuevamente. Si desea consultar el registro de la base de datos, puede hacerlo por la opción "Consultar Registro", la cual también aparece una vez se finalice el registro de información, siempre y cuando no se inicie ninguna modificación. Ayuda

No. Radicado (CIR)	Nombre de la Base de Datos	Cantidad de Titulares	Continuar
18-87262--000000-000	Aspirantes Utopía Automatizada	1.129	Consultar Registro
18-87262--000001-000	Aspirantes Utopía Automatizada	333	Consultar Registro
18-87260--000000-000	Aspirantes Utopía Física	284	Consultar Registro
18-87260--000001-000	Aspirantes Utopía Física	116	Consultar Registro
18-87239--000000-000	BioTrack	39	Consultar Registro
18-87254--000000-000	Campus Abierto	22.500	Consultar Registro
18-87252--000000-000	Carnetización	2.000	Consultar Registro
18-87216--000000-000	CCTV	26.900	Consultar Registro
18-87216--000001-000	CCTV	26.400	Consultar Registro
18-87204--000000-000	Clínica Optometría Física	75.693	Consultar Registro
18-87204--000001-000	Clínica Optometría Física	51.479	Consultar Registro
18-87207--000000-000	Clínica Veterinaria	2.229	Consultar Registro
18-87207--000001-000	Clínica Veterinaria	2.220	Consultar Registro
18-87255--000000-000	Convenios - Contratos EXEC	1.010	Consultar Registro
18-87255--000001-000	Convenios - Contratos EXEC	1.000	Consultar Registro
18-87251--000000-000	Convocatoria Administrativa	50	Consultar Registro
18-87264--000000-000	Donantes Filantropía	3.100	Consultar Registro
18-87264--000001-000	Donantes Filantropía	900	Consultar Registro
18-87200--000000-000	Dspace	6.358	Consultar Registro
18-87200--000001-000	Dspace	6.358	Consultar Registro

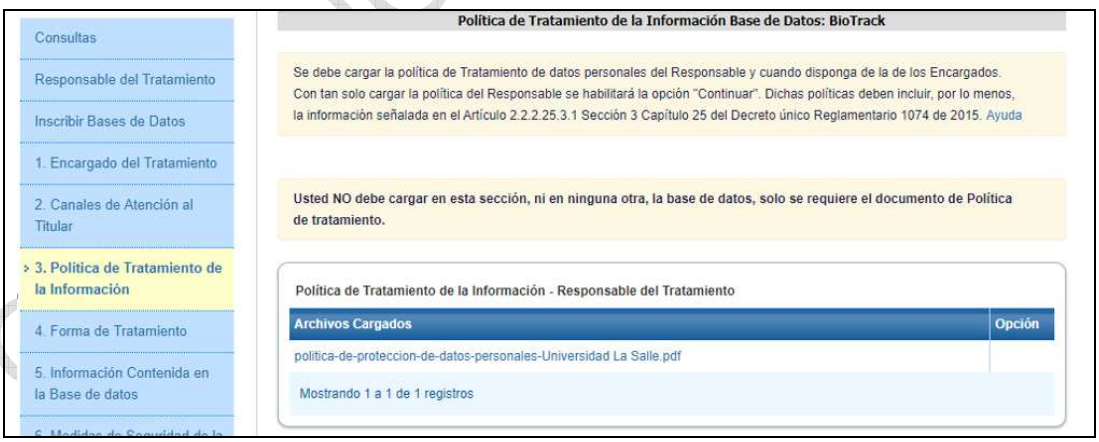
Mostrando 1 a 20 de 75 registros 1 2 3 4

En la opción Consultar Registro abrirá el formulario Nombre y Finalidad de la Base de Datos donde se podrá visualizar (Finalidad, Descripción de Finalidad y Cantidad de Titulares como información de interés):



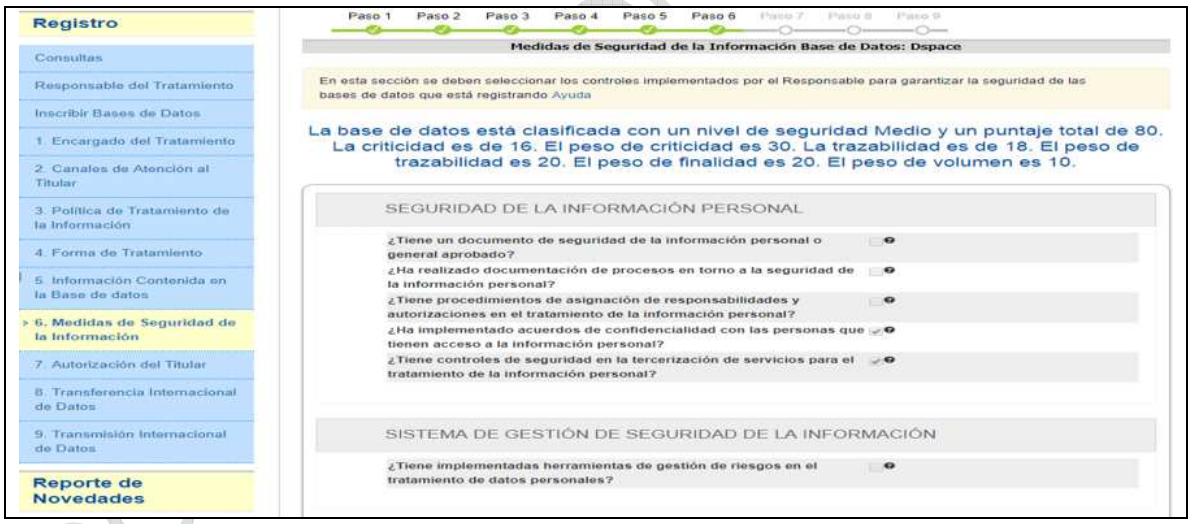
Al dar click en el botón Continuar el sistema desplegará los 10 módulos de Registro de los cuales se consultará:

- **Política de Tratamiento**



- **Información contenida en la Base de Datos**

- **Medidas de Seguridad de la Información**

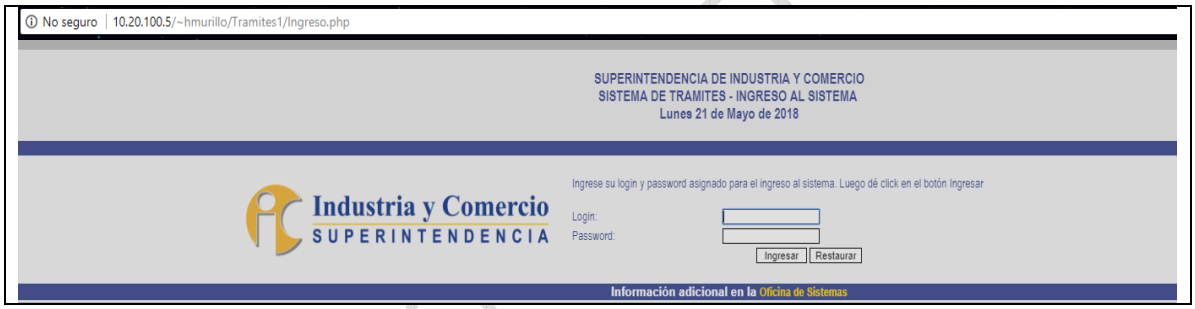


Es posible ingresar a los módulos Autorización del titular, transferencia Internacional y transmisión Internacional de datos, de ser necesaria su consulta.

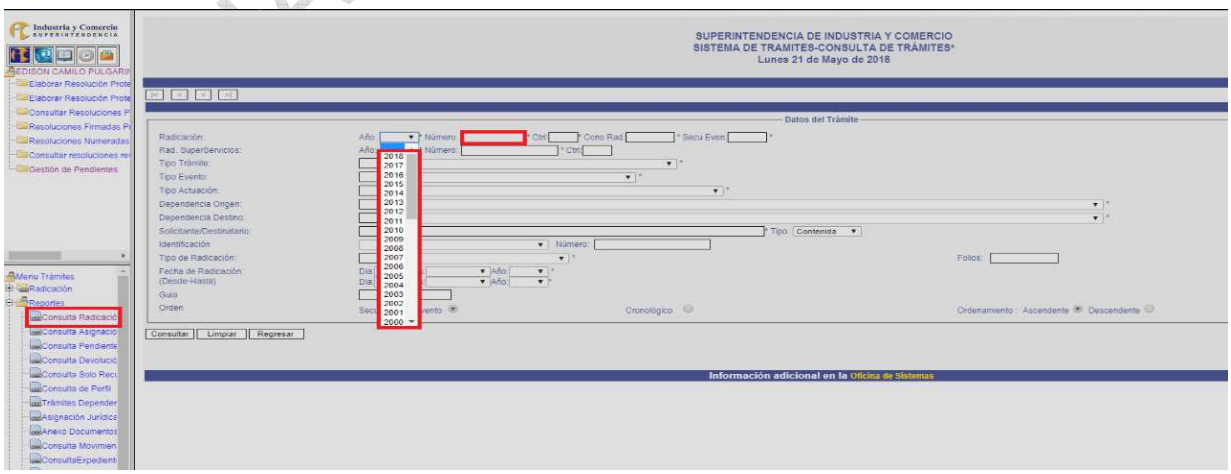
5.2.3 Verificar el sistema de trámites para validar la documentación relacionada al incidente.

Se deber ingresar a la INTRASIC en la siguiente URL http://intrasic/INTRASIC en donde aparecerá la opción Sistema de trámites:

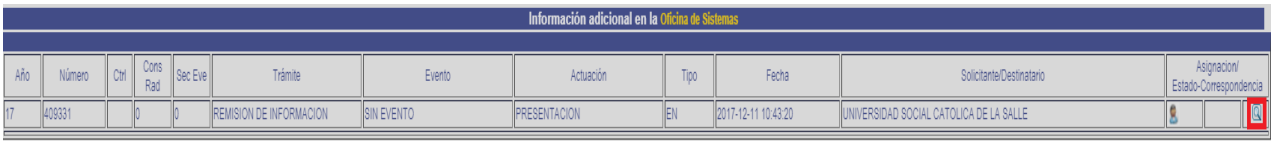
Para el acceso al sistema de trámites se debe suministrar el usuario y contraseña del funcionario o contratista designado, como se indica a continuación, http://10.20.100.5/~hmurillo/Tramites1/Ingreso.php.



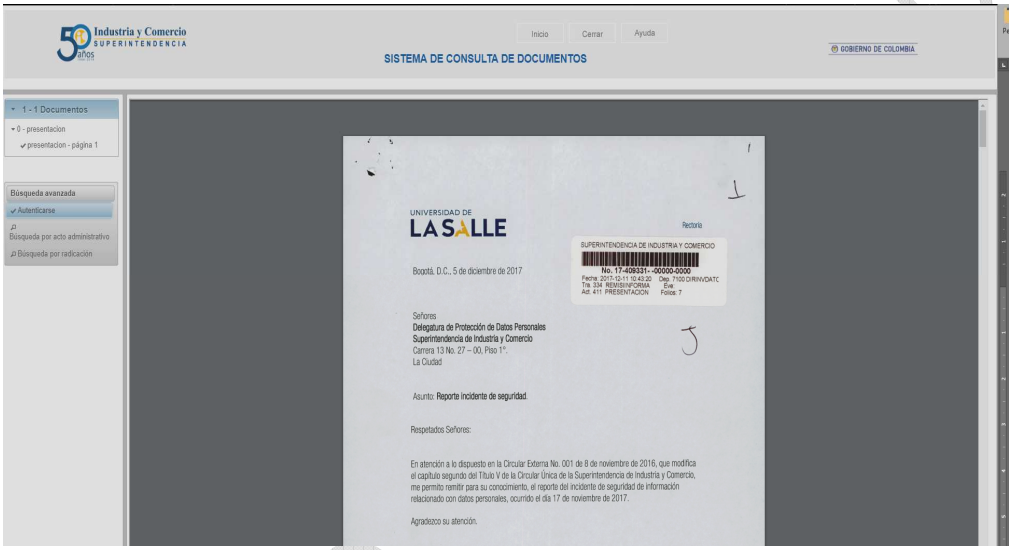
En la sesión se debe dirigir al menú de reportes, consulta radicación donde se visualizará el módulo desde el cual se ingresará por el número del radicado. Se podrá observar todo lo relacionado al incidente dando click en el botón Consultar.



Se verá reflejado el resultado de la búsqueda en sistema de trámites en donde se deberá dirigir al icono en forma de lupa:



Al hacer click en el icono se visualizará los documentos de la siguiente manera:



Nota 1: Por medio del visor del sistema de trámites se podrá descargar los archivos digitalizados en tal caso que se necesiten.

5.3 Identificar preguntas relacionadas con el incidente reportado (si aplica).

Después de la lectura del incidente reportado y revisión de los documentos encontrados en las plataformas anteriormente descritas a continuación, se adjunta un listado básico de las preguntas que se deberían solicitar a la empresa o razón social que reporta el incidente en caso de no tener claridad o presentar dudas adicionales que no se encuentren debidamente documentadas en el radicado inicial.

- ¿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?
- ¿Cuáles son los acuerdos de confidencialidad suscritos con los empleados?
- ¿Qué tipo de información comprometida en el incidente?

COPIA NO CONTROLADA

- Tipo de información almacenada en las bases de datos comprometidas, numero de titulares afectados.
- 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.
- Y demás preguntas necesarias según el incidente reportado.

5.4 Clasificar y dar tratamiento

Se inicia el proceso mediante el 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 y tratamiento para cada uno según el análisis descrito a continuación:

5.4.1 Severidad Baja

- El incidente no presenta afectación a los 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.

COPIA NO CONTROLADA

Se presento Afectación de Datos - Marque la Casilla.		
☐ SI	☑ NO	☐ Sin Identificar
Tipo de Incidente - Marque la Casilla.		
☐ Afecta la Confidencialidad de los Datos Personales	☐ Afecta la Disponibilidad de los Datos Personales	
☐ Afecta la Integridad de los Datos Personales	☐ Afecta la Confidencialidad y Disponibilidad de los Datos Personales	
☐ Afecta la Confidencialidad e Integridad de los Datos Personales	☐ Afecta la Disponibilidad e Integridad de los Datos Personales	
☐ Afecta la Confidencialidad, Disponibilidad e Integridad de los Datos Personales		
☑ Otros (Cuales): **Ninguno**		

Tratamiento: El reporte únicamente se registra y pasa a ser archivado, adicionalmente se anexa el informe de análisis del incidente de seguridad. Ver el *INFORME DE ANALISIS DE INCIDENTE DE SEGURIDAD.docx* o *INFORME DE SEGUIMIENTO DE ANALISIS DE INCIDENTE.docx*

5.4.2 Severidad Media

- Se presenta afectación de datos o se encuentra sin identificar.

Se presento Afectación de Datos - Marque la Casilla.		
☑ SI	☐ NO	☑ Sin Identificar

- En el incidente se identifica afectación de la integridad o confidencialidad o disponibilidad de la información. (Sólo uno)

Tipo de Incidente - Marque la Casilla.	
☑ Afecta la Confidencialidad de los Datos Personales	☑ Afecta la Disponibilidad de los Datos Personales
☑ Afecta la Integridad de los Datos Personales	☐ Afecta la Confidencialidad y Disponibilidad de los Datos Personales
☐ Afecta la Confidencialidad e Integridad de los Datos Personales	☐ Afecta la Disponibilidad e Integridad de los Datos Personales
☐ Afecta la Confidencialidad, Disponibilidad e Integridad de los Datos Personales	
☐ Otros (Cuales):	

- 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 clasifique como semi-publicos y/o pertenezcan a personas mayores de 18 años.

COPIA CONTROLADA

Tipo de Titular Afectado - Marque la Casilla.			
☑ Personas Menores de 18 años	☑ Personas Mayores de 18 años		
Datos afectados - Marque la Casilla.			
☑ Datos de Identificación	☐ Datos Socio Económicos	☐ Datos de Ubicación	☐ Datos Sensibles
☑ Otros Datos (Cuales):			

Tratamiento: El reporte se registra y se debe realizar seguimiento posterior de ***3 meses o 6 meses o 1 año***, según el criterio del encargado de la clasificación y tratamiento del caso para posteriormente ser archivado o pasar a severidad alta según el resultado del seguimiento. Adicionalmente se anexa el informe de análisis del incidente de seguridad. Ver el *INFORME DE ANALISIS DE INCIDENTE DE SEGURIDAD.docx* o *INFORME DE SEGUIMIENTO DE ANALISIS DE INCIDENTE.docx*

5.4.3 Severidad Alta

- Se presenta afectación de datos o se encuentra sin identificar.

Se presento Afectación de Datos - Marque la Casilla.		
☑ SI	☐ NO	☑ Sin Identificar

- 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).

Tipo de Incidente - Marque la Casilla.	
☐ Afecta la Confidencialidad de los Datos Personales	☐ Afecta la Disponibilidad de los Datos Personales
☐ Afecta la Integridad de los Datos Personales	☑ Afecta la Confidencialidad y Disponibilidad de los Datos Personales
☑ Afecta la Confidencialidad e Integridad de los Datos Personales	☑ Afecta la Disponibilidad e Integridad de los Datos Personales
☑ Afecta la Confidencialidad, Disponibilidad e Integridad de los Datos Personales	
☐ Otros (Cuales):	

- La descripción del incidente y las soluciones no se encuentran completas y/o no hay conformidad con el análisis realizado por el encargado de la clasificación y tratamiento del caso.
- Los controles y las medidas aplicadas no se encuentran completos y/o no hay conformidad con el análisis realizado por el encargado de la clasificación y tratamiento del caso.
- Los datos afectados sean privados y/o sensibles y/o biométricos, pertenezcan a personas mayores de 18 años y/o menores de 18 años.

Tratamiento: El reporte se registra, se sugiere la apertura de investigación para el caso analizado y recolección de evidencias digitales para asegurar la preservación de su validez legal en caso de juzgarse necesario, por el personal encargado de la

COPIA CONTROLADA

revisión del análisis entregado a la Delegatura de protección de datos. Se anexa el informe de análisis del incidente de seguridad. Ver el *INFORME DE ANALISIS DE INCIDENTE DE SEGURIDAD.docx* o *INFORME DE SEGUIMIENTO DE ANALISIS DE INCIDENTE.docx*

Clasificación	**Afectación Datos**	**Tipos de Datos Afectados**		
		Nivel Bajo Mayores de 18 Años *Datos Públicos	**Nivel Medio Mayores de 18 Años *Datos Semi-Privados**	**Nivel Alto Mayores de 18 Años Menores de 18 Años *Datos Privados *Datos Sensibles *Datos Biométricos**
Severidad Baja	***Ninguna***	***Tratamiento*** Registro Reporte y se archiva.	***Ninguna***	***Ninguna***
Severidad Media	***Afectación*** -Integridad - Confidencialidad - Disponibilidad ***(Solo Uno).***	***Tratamiento*** Registro Reporte y se realiza Seguimiento 3 Meses	***Tratamiento*** Registro Reporte y se Realiza Seguimiento 6 Meses	***Tratamiento*** Registro Reporte y se propone apertura de investigación
Severidad Alta	***Afectación*** -Integridad - Confidencialidad - Disponibilidad ***(Varios Factores de Afectacion Simultaneos).***	***Tratamiento*** Registro Reporte y se Realiza Seguimiento 6 Meses	***Tratamiento*** Registro Reporte y se propone apertura de investigación	***Tratamiento*** Registro Reporte y se propone apertura de investigación

Tabla 1-Mapa de Calor Análisis de severidad de incidente de seguridad
****Consulta de tabla de clasificación de Datos Delegatura Protección de Datos.***

6 DOCUMENTOS RELACIONADOS

PD01-F07 Formato Informe De Análisis De Incidente De Seguridad

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

7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Versión inicial del documento.

Fin documento

COPIA NO CONTROLADA