
 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 1 de 19

CONTENIDO

1	OBJETIVO	2
2	DESTINATARIOS	2
3	GLOSARIO	2
4	GENERALIDADES	7
5	DESCRIPCION DE ACTIVIDADES	7
5.1	REALIZAR LA RECEPCIÓN Y ESCALAMIENTO DEL INCIDENTE	7
5.2	REALIZAR ANALISIS TECNICO DEL INCIDENTE	8
5.2.1	Validación de Información RUES	8
5.2.2	Validación de Información RNBD	9
5.2.3	Validaciones en el sistema de trámites	12
5.2.4	Validación de Vulnerabilidades WEB	14
5.3	IDENTIFICAR PREGUNTAS RELACIONADAS CON EL INCIDENTE REPORTADO	15
5.4	REALIZAR CLASIFICACION MANUAL DEL INCIDENTE	16
5.4.1	Severidad Baja	16
5.4.2	Severidad Media	16
5.4.3	Severidad Alta	17
6	DOCUMENTOS RELACIONADOS	19
7	RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN	19

Elaborado por: Nombre: María Isabel Vargas Pérez Cargo: Contratista	Revisado y Aprobado por: Nombre: Carolina García Molina Cargo: Directora de Investigaciones de Protección de Datos Personales	Aprobación Metodológica por: Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2024-11-25
--	--	--

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.

 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 2 de 19

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 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.

2 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.

3 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.

	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 3 de 19

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.


Contramedita: 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,

 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 4 de 19

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.

 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 5 de 19

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

	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 6 de 19

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.


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.

 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 7 de 19

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 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.


5 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:

5.1 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, 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, de realizar el **reporte electrónico** de los incidentes de seguridad,

	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 8 de 19

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.

5.2 REALIZAR 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.

5.2.1 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.



The screenshot shows the RUES website interface. At the top, there is a red header with 'Acceso Privado' and a search bar with 'ENVIAR' button. Below the header, there are navigation links: 'Consulta Beneficio a Empresarios', 'Guía de Usuario Público', 'Guía de Usuario Registrado', and 'Cámaras de Comercio'. The main content area features a banner for 'registro Único Empresarial y Social' with a description: 'A través de esta consulta, los beneficiarios pueden descargar la información de comerciantes inscritos en el RUES a nivel nacional que tengan su matrícula establecimientos renovada.' Below the banner, there is a search section titled 'Realice su consulta empresarial o social' with two search boxes: 'Consultar por Nombre o Razón Social' and 'Número de Identificación', both with red search buttons. There are also some small icons and text at the bottom of the search section.

	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 9 de 19

- Ingresar a la plataforma RUES desde la página web <https://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.



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

CON FUNDAMENTO EN LA MATRÍCULA E INSCRIPCIONES EFECTUADAS EN EL REGISTRO MERCANTIL, LA CÁMARA DE COMERCIO CERTIFICA:

NOMBRE, IDENTIFICACIÓN Y DOMICILIO

Razón social: CARACOL PRIMERA CADENA RADIAL COLOMBIANA S.A.
Sigla: CARACOL S.A.
Nit: 860014923 4
Domicilio principal: Bogotá D.C.

MATRÍCULA


Matrícula No. 00013633
Fecha de matrícula: 3 de abril de 1972
Último año renovado: 2023
Fecha de renovación: 31 de marzo de 2023

UBICACIÓN

Dirección del domicilio principal: Cl1 67 No 7-37 ESO 7
Municipio: Bogotá D.C.
Correo electrónico: impuestoscaracol@caracol.com.co
Teléfono comercial 1: 3487600
Teléfono comercial 2: 3178114562
Teléfono comercial 3: No reportó.
Páginas web: WWW.CARACOL.COM.CO
WWW.LOS40.COM.CO
WWW.TROPICANAFM.COM
WWW.OXIGENO.FM
WWW.RADIOACTIVA.COM
WWW.WRADIO.COM
WWW.BESAME.FM

5.2.2 Validación de Información RNBD

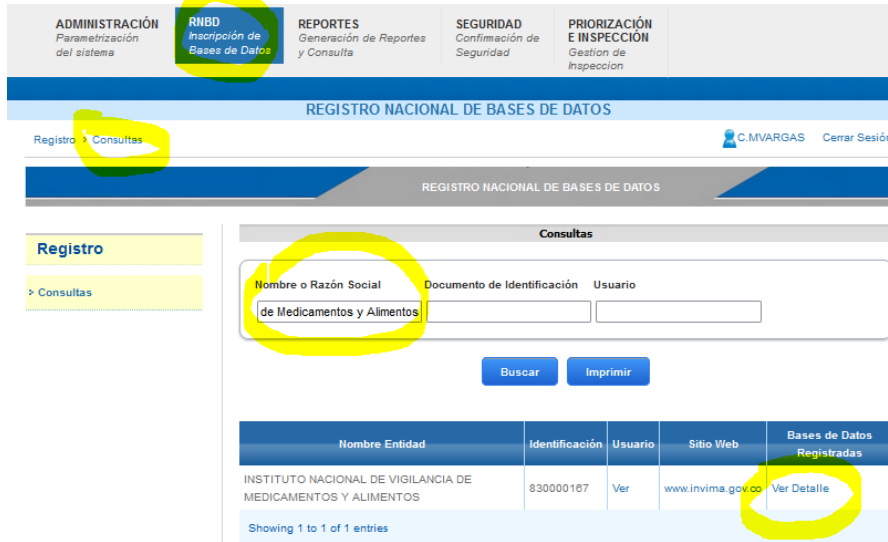
El Servidor público y/o contratista al cual le fue asignado el análisis técnico del incidente, inicia validando la información de la sociedad consultando en el RNBD este se accede por medio del enlace <https://rnbd.sic.gov.co/sisi/login> con un usuario de dominio y contraseña habilitados anteriormente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

	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 10 de 19

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.



ADMINISTRACIÓN
Parametrización del sistema

RIBD
Inscripción de Bases de Datos

REPORTE
Generación de Reportes y Consulta

SEGURIDAD
Confirmación de Seguridad

PRIORIZACIÓN E INSPECCIÓN
Gestión de Inspección

REGISTRO NACIONAL DE BASES DE DATOS

Registro Consultas C.MVARGAS Cerrar Sesión

REGISTRO NACIONAL DE BASES DE DATOS

Registro

> Consultas

Consultas

Nombre o Razón Social Documento de Identificación Usuario

de Medicamentos y Alimentos

[Buscar] [Imprimir]

Nombre Entidad	Identificación	Usuario	Sitio Web	Bases de Datos Registradas
INSTITUTO NACIONAL DE VIGILANCIA DE MEDICAMENTOS Y ALIMENTOS	830000167	Ver	www.invima.gov.co	Ver Detalle

Showing 1 to 1 of 1 entries

Tipo Incidente: Afecta la Disponibilidad de los datos personales

Causal: Fraude externo

Descripción:

El pasado 6 de febrero del presente año, nuestra plataforma tecnológica institucional fue objeto de un ataque cibernético que produjo indisponibilidad de la información. Dicho incidente de seguridad fue reportado de manera inmediata ante la Fiscalía General de la Nación, ente investigador que actualmente se encuentra realizando las pesquisas correspondientes para identificar la procedencia y los responsables de este acto delictivo. Este complejo escenario de afectación a la disponibilidad de la información institucional, ha impactado, también, la seguridad de las bases de datos personales tratadas por el Invima. El Invima informa, dentro del término legal, que ante la violación de los códigos de seguridad institucionales previstos para la protección de los datos personales tratados, procedió con las acciones necesarias para contener y revertir el impacto del incidente de seguridad, entre ellas el aislamiento de los equipos de accesos a la red para evitar que se propagara el ataque recibido con Ransomware BlackByte, así como los equipos de los servidores; posteriormente, se realizó la revisión de forma segura del nivel de afectación a la información y la infraestructura tecnológica institucional, determinando que la información, sistemas operativos, máquinas virtuales, aplicativos administrativos, bases de datos y las carpetas compartidas fueron cifrados. Asimismo, dentro de los efectos derivados del referido ataque cibernético, se logró identificar que el cifrado de la información institucional incluyó, igualmente, cifrado de los datos personales objeto de tratamiento por parte del Invima. En este escenario de innegable impacto a la capacidad operativa institucional, el Invima evaluó los riesgos y afectaciones asociadas con el incidente de seguridad, respecto de toda la información del Instituto, concluyendo que la misma se encuentra salvaguardada en copias de seguridad que no fueron afectadas. Asimismo, estamos implementando un proceso gradual y progresivo de restauración de la información institucional a partir de las copias de seguridad que se ejecutan de acuerdo con las políticas de respaldo establecidas por la entidad, proceso que se viene adelantando por etapas, de acuerdo con la complejidad de la afectación.


Cantidad de Titulares Afectados: 36508

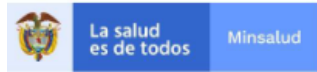
Fecha Incidente: 06/02/2022

Fecha de Conocimiento: 06/02/2022

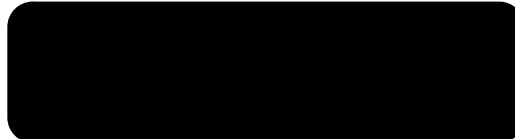
Archivo adjunto: 06.MMP.250222_INFORME SIC.pdf

COPIA

	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 12 de 19



Bogotá D.C. febrero 24 de 2022



Asunto: Reporte de incidente de seguridad en los datos personales tratados por el Invima

Respetado Dr. Remolina, cordial saludo:

Ha sido prioridad para el Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, como entidad responsable del tratamiento de datos personales en relación con nuestra misión, funciones y trámites, adoptar e implementar medidas técnicas, administrativas y organizativas necesarias para otorgar seguridad a los registros de información, bajo condiciones que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Pese a lo anterior, el pasado 6 de febrero del presente año, nuestra plataforma tecnológica institucional fue objeto de un ataque cibernético que produjo indisponibilidad de la información.

Dicho incidente de seguridad fue reportado de manera inmediata ante la Fiscalía General de la Nación, ente investigador que actualmente se encuentra realizando las pesquisas correspondientes para identificar la procedencia y los responsables de este acto delictual.

- 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.

5.2.3 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>), 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.

Datos del Trámite (PENDIENTE)

Radicación: Año: 2022 | Número: 155325 | Ctr: | Cons Rad: 0 | Secu Even: 0
 Rad. SuperServicios: Año: | Número: | Ctr: |
 Tipo Trámite: 424 INCIDENTES
 Tipo Evento: 500 SIN EVENTO
 Tipo Actuación: 411 PRESENTACION
 Dependencia Origen: |
 Dependencia Destino: 7100 DIRECCION DE INVESTIGACIONES DE PROTECCION DE DATOS PERSONALES
 Solicitante/Destinatario: GAMES AND BETTING S.A.S | Tipo: Contenido
 Identificación: MI - MI | Número: 901153940 | Ver RUES | Ver Autorización Notificación
 Dirección: c.ramirez@yajuego.co BOGOTA D.C. BOGOTA COLOMBIA
 Tipo de Radicación: EN - ENTRADA | Folios: 17
 Fecha de Radicación: Día: 20 | Mes: Abril | Año: 2022 | 10:52:04 | Entrega: EMAIL ELECTRONICO - CARGA DIGITAL
 Observaciones: Se realiza cambio del trámite de 384 a 424 debido a que es un incidente. la solicitud fue hecha por Detsy Alejandra Suarez bajo a la autorización de la Dra. Claudia Biliama

Otros Datos

[Documentos] Ubicación [25] Exportar todo

Nueva Consulta | Regresar

Registro: 1 / 4

Información adicional en la Oficina de Sistemas

Año	Número	Ctr	Cons Rad	Sec Eya	Trámite	Evento	Actuación	Tipo	Fecha	Solicitante/Destinatario	Asignación/ Estado-Correspondencia
22	155325		0	0	INCIDENTES	SIN EVENTO	PRESENTACION	EN	2022-04-20 10:52:04	GAMES AND BETTING S.A.S	

- 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.

1 - 4 Documentos

- 0 - presentación
 - presentación - página 1
 - presentación - página 2
 - presentación - página 3
 - presentación - página 4
 - presentación - página 5
- 1 - traslado queja / denuncia / expediente
- 2 - traslado queja / denuncia / expediente
- 3 - traslado queja / denuncia / expediente

Información Inicio de sesión realizada exitosamente.

Radicación de Entrada 1 / 1 | 96%

De: delegaturaconsumidor@sic.gov.co
Enviado el: 2022-04-19 16:27:03
Para: Contactenos Sticker Digital <contactenos@sic.gov.co>
Copia:
Asunto: Radicar denuncia con número nuevo -Dependencia 7100

Radicación: 22-155325-00000-0000
Fecha: 2022-04-20 10:52:04
Trámite: 384 PROTECCION DE DATOS
Actuación: 411 PRESENTACION

Dependencia: 7100 DIRINVDATOSPERS
Evento: 328 DENUNCIAS
Folios: 17

Buenas tardes estimados señores, Por favor radicar denuncia con número para la dependencia 7100. Referencia: Información sobre estado de relaciones de consumo entre YAJUEGO y sus jugadores. Respetada Dra. Soacha ORLANDO CARRILLO BUITRAGO, identificado como aparece al pie de mi firma, actuando en calidad de representante legal de GAMES AND BETTING S.A.S., nos dirigimos a su Delegatura - como autoridad encargada de controlar que las relaciones de consumo se desarrollen bajo el respeto de los derechos de los consumidores y, en especial, a recibir información oportuna y veraz -, para exponerle de manera directa la actual situación que enfrentamos en nuestra operación y las actuaciones y planes de trabajo que hemos venido ejecutando con el fin de que ésta coyuntura no afecte los intereses de nuestros usuarios. Para tales efectos adjuntamos comunicación. Agradecemos su atención y estamos atentos a su respuesta. Cordialmente ORLANDO CARRILLO BUITRAGO Presidente GAMES AND BETTING S.A.S. 1 / 2 ----- Mensaje Original ----- Asunto: Información sobre estado de relaciones de consumo entre YAJUEGO y sus jugadores.

- 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

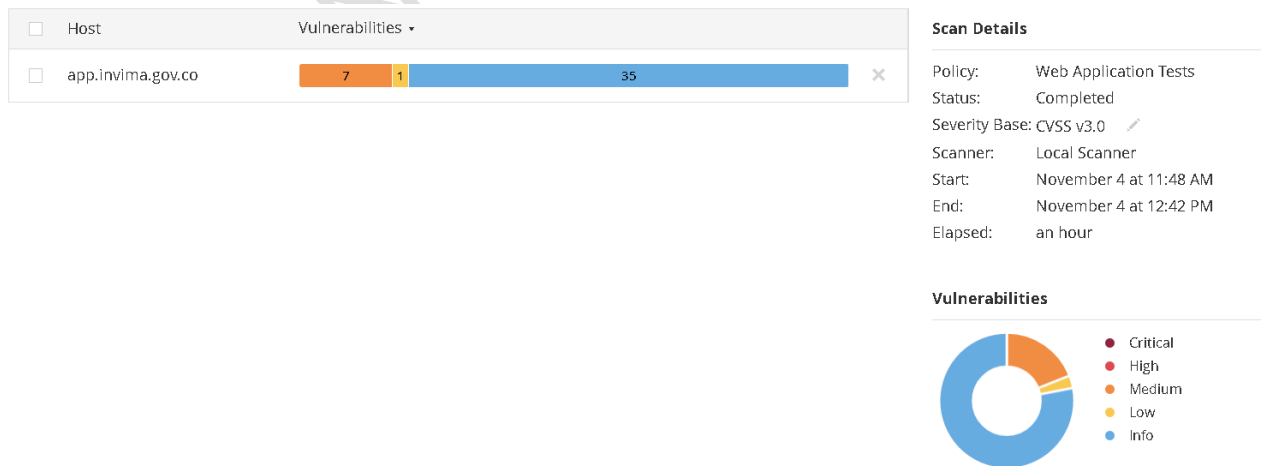
esta información sea necesaria para determinar la gestión adecuada del incidente reportado.


- 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.

5.2.4 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 Críticas (*Criticas, Altas y Medias*), se procede a anexar el reporte generado y se incluyen estos hallazgos de seguridad al informe de análisis del incidente.




 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 15 de 19

5.3 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.

 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 16 de 19

5.4 REALIZAR 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:

5.4.1 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.

5.4.2 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.

	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 17 de 19

5.4.3 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	<i>Ninguna</i>	<i>Ninguna</i>	<i>Ninguna</i>	<i>Ninguna</i>
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.

 <p>Superintendencia de Industria y Comercio</p>	INSTRUCTIVO CLASIFICACIÓN Y TRATAMIENTO PARA LOS INCIDENTES RELACIONADOS CON LAS BASES DE DATOS PERSONALES	Código: PD101-I01
		Versión: 2
		Página 19 de 19

- 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.

6 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.

7 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