POLÍTICAS Y PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL

TABLA DE CONTENIDO

1. CONTROL DE REGISTROS Y CAMBIOS

Versión	Fecha	Descripción	Elaboró	Revisó	Aprobó
0.1	2019	Elaboración Política	Elizabeth Medina	Dra. Alba Cecilia Vélez Lara	Dr. Francisco Javier Vélez Lara Gerente General
0.2	2023 – Agosto - 23	Actualización de la Política	Leggat	Coordinadora de Calidad Directora Financiera	Dr. Francisco Javier Vélez Lara Representante Legal

2. INTRODUCCIÓN

En la presente política de gestión de incidentes, se establecen los lineamientos y directrices para gestionar los Incidentes de Seguridad de la Información Personal que puedan presentarse al interior de ESTUDIOS ENDOSCÓPICOS S.A.S, a través de un modelo específico para ello.

3. OBJETIVO

Dar a conocer los lineamientos para la gestión de incidentes de la seguridad de la información que puedan presentarse al interior de la IPS, con el fin de prevenir los mismos, así como mitigar el impacto de aquellos que se generen.

4. ALCANCE

Esta política da a conocer los componentes generales de la gestión de incidentes, las acciones a desarrollar en caso tal de que se presenten, sea a través de medios virtuales o físicos.

5. DEFINICIONES

- **Incidente de seguridad:** son todos aquellos eventos que afecten la confidencialidad, la integridad y la disponibilidad de la información de carácter personal, por lo que, en el caso en que dispongan de ellas, generan una violación a la política de seguridad de la información de las organizaciones.

- **Integridad**: mantener con exactitud la información que fue entregada para su tratamiento, sin ser manipulada por parte de quienes no están autorizados para ello.
- **Confidencialidad**: propiedad de la información que permite garantizar que esta es accedida solo por las personas que cuentan con la autorización para ello dentro de la organización o por parte de los encargados que la organización designe como tales.
- **Disponibilidad**: propiedad de la información que busca garantizar el acceso y uso de la información y los sistemas de tratamiento de la misma por parte de las personas o entidades autorizadas para el momento en que lo requieran.
- **Dato**: representación simbólica de un atributo o variable.
- **Disponibilidad**: Propiedad de la información que pretende garantizar el acceso y uso de la información por parte de quienes están autorizados para ello, sea de carácter público o privado.
- **Evento de seguridad de información:** trata de una ocurrencia que indica una posible vulneración al sistema de seguridad de la información, a través de un sistema digital o físico.
- **Incidente de seguridad de la información**: Uno o más eventos de seguridad de la información que suceden de forma inesperada y no deseada y que tienen la probabilidad de comprometer las normales operaciones de la organización, amenazando los principios de confidencialidad e integridad de la información.

6. MARCO NORMATIVO

- **Ley 1581 del 2012 en sus artículos:**

  - **Artículo 17. Deberes de los responsables del tratamiento.**

  Los responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: …
  n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

  - **Artículo 18. Deberes de los Encargados del Tratamiento.** Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

De igual manera, en la Circular Única de la Superintendencia de Industria y Comercio, se establece que las organizaciones que están obligadas a inscribir las Bases de Datos Personales ante el Registro Nacional de Bases deberán reportar el incidente de seguridad dentro los quince días hábiles siguientes al momento en que sean detectados y puestos en conocimiento de la persona o área encargada. …

7. CAUSAS DE LOS INCIDENTES DE SEGURIDAD

- Inexistencia de políticas preventivas de seguridad
- Errores o negligencia humana.
- Casos fortuitos.
- Actos maliciosos o criminales.
- Fallas en los sistemas de la organización.
- Procedimientos defectuosos.
- Deficiencias o defectos en las operaciones.
- Alteración; destrucción; robo o pérdida de archivos físicos.

Todos los incidentes de seguridad deben ser tratados con la misma diligencia, pues cada uno de ellos puede generar un nivel bajo-alto, dependiendo de las circunstancias en que suceda y el nivel de afectación de los datos personales.

8. PROCEDIMIENTO APLICABLE

8.1. IDENTIFICACIÓN:

Toda persona que identifique eventos adversos en la seguridad de la información que reposa en las bases de datos de Estudios Endoscópicos, deberá reportar al área de Gerencia Administrativa a través del correo electrónico gerencia@estudiosendoscopicos.co dicha situación que perciba como anormal y que pueda trascender a un incidente de seguridad de la información.

- **Los incidentes se dividen en:**

- **Bajo riesgo:** es improbable que el incidente de seguridad tenga un impacto en las personas, y de generarlo, este sería mínimo.
- **Riesgo medio:** el incidente de seguridad puede tener un impacto en las personas, pero es poco probable que el impacto sea sustancial.
- **Riesgo alto:** el incidente de seguridad puede tener un impacto considerable en las personas afectadas.
- **Riesgo grave:** el incidente de seguridad puede tener un impacto crítico, extenso o peligroso en las personas afectadas.

8.2. CÓMO DETECTAR EL NIVEL DE RIESGO:

8.2.1. En los Titulares de la información

- Cantidad de personas que fueron afectadas.
- Categoría de personas que fueron afectadas.
- Características especiales de las personas afectadas, tales como datos de niños, niñas o adolescentes, personas de la tercera edad, personal de partidos políticos, etc.

8.2.2. En los Datos Personales:

- Cuál fue el volumen de los datos afectados.
- En qué periodo afectaron los datos o estuvieron comprometidos.
- Cuál tipo de información personal fue comprometida, tal como la edad, el sexo, tipo de sangre, dirección de residencia, datos biométricos, historia clínica en general, etc.
- Nivel de sensibilidad de la información afectada.
- Contexto de la información personal que se vio afectada.
- Cómo se encontraba protegida la información, si a través de contraseñas, detección biométrica, candados, etc.
- En qué puede ser utilizada la información que fue comprometida.
- Determinar si dicha información comprometida puede generar afectación a nivel personal al titular de la información.
- La información logró recuperarse una vez sucedió el incidente.
- Si es posible que se cometa un fraude o delito con la información sustraída de las bases de datos de la organización.

8.2.3. En la organización:

- Qué ocasionó el incidente de seguridad, si fue la falta de protección cifrada, la falta de capacitación al personal, etc.
- Con qué frecuencia suceden incidentes de seguridad.
- En qué periodos se suelen desarrollar los incidentes de seguridad.
- Qué alcance tuvo el incidente.
- Qué medidas se habían adoptado para proteger esos datos.
- Qué medidas de protección se implementaron posteriormente al incidente.

8.2.4. Encargado de sistemas de información física y digital:

Ingeniero de sistemas encargado de información digital: Deberá indicar, de acuerdo con el riesgo generado, si el tipo de incidente que se presentó tuvo una afectación baja, media o alta. Igualmente, realizará los procedimientos informáticos necesarios para asegurar que la información depositada en las bases de datos vuelva a ser segura. Una vez realice lo necesario para ello, informará a la Gerencia Administrativa, de manera escrita, sobre las actuaciones realizadas.

Gerente administrativo encargado de información física: Deberá indicar, de acuerdo con el riesgo generado, si el tipo de incidente que se presentó tuvo una afectación baja, media o alta. Reposará de manera escrita la manera en que se identificó el incidente, la afectación y lo que conllevó a su clasificación en el nivel que se determine.

8.3. Reporte

Una vez identificado el nivel de riesgo, la Gerencia Administrativa realizará un informe escrito que detalla las circunstancias del incidente de seguridad, las bases de datos afectadas y el tipo de dato que reposa en las mismas, fecha y hora del incidente de seguridad, así como la fecha y hora en que fue identificado por quien generó el primer reporte, detallará las indagaciones preliminares e investigaciones realizadas por parte de la organización, las medidas correctivas para mejorar la gestión del incidente. Esta información deberá ser objeto de reporte ante la Superintendencia de

Industria y Comercio, al igual que deberá informarse a los Titulares de la información de la base de datos afectada, el incidente ocurrido. En caso de ser necesario, incluir detalles personales.

Finalmente, deberá realizarse un cierre formal del incidente a través de documento escrito y fechado, donde conste haber cumplido con cada uno de los requerimientos para el tratamiento del incidente, así como la mejora del sistema de seguridad afectado.
En resumen, todos los incidentes de seguridad deben tener:

- Conocimiento del incidente: quién lo identificó, cómo se produjo, fecha, hora, naturaleza del incidente, base de datos afectada, personas con autorización a ingresar a dichas bases de datos.
- Evidencia de lo sucedido después del incidente: todo incidente debe contar con evidencia, por lo cual es necesario ser cuidadosos con no suprimir ningún dato, aunque se considere irrelevante.
- Análisis por parte del encargado del área digital o física: determina el nivel de riesgo según su conocimiento en el área digital o física.
- Enviar detalles del análisis del riesgo a la Gerencia Administrativa.
- Elaboración del informe con los detalles de lo ocurrido, datos involucrados, bases de datos y nivel de afectación.
- Velar por la mejora del nivel de seguridad que se vio afectado ante tal incidente: cumpliendo con los tiempos de ejecución establecidos para ello.
- Reporte a los titulares de la información afectada a través del incidente.
- Reporte del incidente ante la SIC.
- Cierre formal del incidente.

8.4. Tiempo de ejecución:

El tiempo de ejecución de la atención de los incidentes de seguridad debe ser de, máximo una semana a partir del conocimiento del incidente. El nivel de tiempo para ejecutar el presente plan dependerá del nivel de riesgo del incidente, pero no debe superar una semana hábil, después de la cual ya deberá estar generándose el respectivo reporte ante la SIC.

8.5. Seguimiento:

Por parte de las áreas encargadas del manejo de incidentes electrónicos o físicos, deberá realizarse monitoreo del protocolo establecido para verificar si el mismo debe ser actualizado conforme los incidentes que se vayan realizando, de manera que se pueda mejorar el periodo de atención y respuesta a los mismos una vez sucedan.

Importante: todas las personas al interior de la organización deben velar por el cumplimiento de la presente política y procedimiento para la gestión de incidentes de seguridad, razón por la cual es de suma importancia que todos los cargos que se encuentran dentro de la organización la conozcan y sean capacitados respecto a ella. Asimismo, el Gerente Administrativo podrá realizar comités de seguridad de la información para discutir la implementación y actualización de los protocolos, el cual podrá estar conformado con personas con distintas profesiones u oficios que aporten al desarrollo de éste desde su conocimiento.

9. OTRAS MEDIDAS DE PREVENCIÓN.

- Capacitar de manera periódica a los contratistas sobre la manera correcta de actuar al momento de percibir un incidente de seguridad.
- Recordar la importancia de saber identificar cuáles incidentes de seguridad afectan los principios de integridad, disponibilidad y confidencialidad.
- Cumplir con lo establecido por la ley 1581 del 2012 y sus decretos reglamentarios, generando auditorías externas o internas que permitan dar seguimiento al nivel de seguridad de la información y el cumplimiento de las medidas técnicas, humanas y administrativas implementadas al interior de Estudios Endoscópicos.
- Disponibilidad del presente manual en las sedes de la IPS, de manera que todas las personas que accedan a la misma, puedan ser conocedores de la presente política.

La misma comienza a regir a partir del 23 de agosto del 2023.

Aprobado por:

FRANCISCO JAVIER VÉLEZ LARA
Representante Legal