APLICACIÓN Y ANÁLISIS DE UNA PIA (*PRIVACY IMPACT ASSESSMENT*) PARA LA EVALUACION DE IMPACTO EN LA PROTECCION DE DATOS PERSONALES DE LA INSTITUCIÓN EDUCATIVA "HERALDO ROMERO SANCHEZ"

Danny Andres Taipe Perez, ✉ **ing.dannyantape@gmail.com**

Proyecto de Grado presentado como requisito
Para optar al título de Ingeniero de Sistemas

Asesor
Ing. EDGAR DULCE

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
SAN JUAN DE PÀSTO
NOVIMBRE, 2022

Nota de Responsabilidad

"Las ideas y conclusiones aportadas en la Tesis de grado, son responsabilidad exclusiva de los autores"

Artículo 1°. Acuerdo N. 324 de octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

Nota de Aceptación

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

San Juan de Pasto, Noviembre de 2022.

AGRADECIMIENTOS

Agradezco a mis padres, a quienes amo y me han dado todo su apoyo económico, amoroso haciéndome sentir lo importante que es siempre la familia en tu desarrollo como persona y profesional.

A mi tío Carlos arcos e institución heraldo Sánchez por ser parte de esta etapa permitiéndome realizar este trabajo y darme todas las herramientas necesarias para culminar con éxito este proyecto y de paso mi carrera profesional.

Al ingeniero de sistemas Edgar dulce por su colaboración y disposición en el desarrollo de este trabajo, ya que por su orientación fue posible cumplir con cada uno de los objetivos propuestos y culminación de este proyecto.

A los ingenieros Manuel Bolaños y Francisco Solarte quienes fueron mis jurados y quienes actuaron rápidamente con dedicación y rapidez con la revisión y aprobación de mmi propuesta final.

A todos los profesores de la Universidad de Nariño, que me acompañaron en todo mi proceso de formación a lo largo de la carrera brindándome sus conocimientos y despejando todas las dudas que tuve durante toda la trayectoria de estudio.

DEDICATORIA

Dedico este trabajo de forma muy especial a mis padres, German Enrique Taipe Arcos y Delis Yanira Pérez Benavides, por darme siempre todo su amor, consejos, apoyo y fortaleza para seguir adelante y formarme como un profesional integro.

A mi hermana Lina Marcela Taipe Pérez, porque ella ve en mí un ejemplo a seguir y siento más ganas de seguir adelante y ser mejor cada día para demostrarle que todo lo que uno se propone se puede conseguir con esfuerzo y disciplina.

A mi esposa Yuly Liliana Bravo Erazo, por ser siempre mi apoyo y darme fuerzas para seguir adelante cuando tenía momentos difíciles además de creer en mí y mis capacidades.

A mi hija Valeria salome Taipe bravo, porque desde que llego a mi vida fue y es mi motor para seguir adelante, para que siempre se sienta orgullosa y vea en mí un padre ejemplar y del cual pueda ver un espejo donde se refleje ´para que sea una persona íntegra.

A mi abuelo Gonzalo Pérez, quien desde hace un tiempo vivo extrañando su presencia, pero estoy seguro que donde se encuentre estará feliz y orgulloso por haber culminado esta etapa de mi vida y la cual el esperaba con muchas ansias y siempre creyó en mis capacidades como estudiante y como persona, además que fue un ejemplo a seguir para darme cuenta que todo lo que uno se propone se puede llegar a cumplir.

A todos mis demás familiares a quienes amo y que siempre confiaron en mí y estuvieron pendientes de cada paso que di en esta etapa.

RESUMEN

La información es uno de los activos más importantes de las empresas y con un alto nivel de vulnerabilidad si no se toman medidas necesarias. las políticas de seguridad de datos personales se hacen necesarios para minimizar los peligros a los que se expone una persona frente violaciones en la privacidad de su información personal. una PIA (*PRIVACY IMPACT ASSESSMENT*) permite evaluar el impacto en la protección de datos personales del proyecto. la institución educativa "heraldo romero Sánchez" maneja un sistema de información para la gestión académica y dentro de si toda la información de los estudiantes, docentes y personal administrativo haciéndola vulnerable a riesgos. por lo anterior, es necesario aplicar y analizar una PIA con el objetivo de evaluar el impacto en la protección de la privacidad de los datos personales de las personas. la aplicación de la PIA permitirá mejorar la protección de los datos personales de la institución educativa "heraldo romero Sánchez".

Palabras clave: PIA, privacidad, datos personales, seguridad de la información.

ABSTRACT

Information is one of the most important assets of companies and with a high level of vulnerability, if necessary measures are not taken. personal data security policies are made necessary to minimize the dangers to which a person is exposed against violations of the privacy of your personal information. a pia allows evaluating the impact on the protection of personal data of projects. educational institution "heraldo romero sánchez" operates an information system for the academic management and within all information of students, documents and personal administrative making it vulnerable to risks. therefore, it is necessary to apply and analyze a pia with the aim of evaluating the impact on protection of the privacy of personal data. the application of the pia will allow improving the protection of personal data of the educational institution "heraldo romero sánchez".

Key words: pia, privacy, personal data, information security.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Cookies: Fichero de texto que los navegadores almacenan en los ordenadores de los usuarios y que, posteriormente, pueden ser actualizados y recuperados por la entidad responsable de su instalación con diversas finalidades. Entre ellas destaca la posibilidad de realizar un seguimiento y monitorización de la navegación del usuario en internet.

Intrusion Detection System (IDS): Sistema diseñado para monitorizar el tráfico entrante y saliente en un sistema informático para identificar patrones sospechosos que pudieran indicar la posibilidad de un ataque malicioso.

Intrusion Prevention System (IPS): Herramienta por la que se pueden definir reglas y procedimientos para alertar sobre tráfico sospechoso en un sistema o red informática y, basándose en las mismas, permitir a los administradores de sistemas definir acciones que se ejecutarán tras la alerta.

Logging: Registro de las actividades de un sistema de información y de las acciones que los usuarios realizan en él. Puede utilizarse para detectar debilidades de seguridad y comportamientos ilícitos de los usuarios.

Metadatos: Literalmente, significa «datos sobre los datos», es decir, son datos que describen otros datos y que permiten que los mismos sean localizados y procesados más fácilmente. Por ejemplo, cuando se produce una llamada telefónica, la hora, el número de origen, el número de destino y la duración de la misma son metadatos relativos a dicha llamada telefónica y que pueden ayudar a su localización o selección.

Minería de datos (*Data Mining*): Es un proceso computacional para el descubrimiento de patrones comunes y la extracción de información y conocimiento analizando grandes volúmenes de datos con técnicas de inteligencia artificial.

Privacidad desde el diseño: Aproximación al diseño de sistemas de información que tiene en cuenta los requisitos de privacidad desde las etapas iniciales del mismo y a lo largo de todo su ciclo de vida.

Privacy Impact Assessment (PIA): Revisión sistemática de un producto, servicio o sistema de información para identificar los riesgos que puede suponer para la privacidad e implantar las medidas necesarias para eliminarlos o mitigarlos hasta niveles aceptables.

I. INTRODUCCIÓN

La información contenida en las diferentes organizaciones e instituciones públicas y privadas a través de sus sistemas de información es uno de los activos más importantes y es un tema que puede generar preocupación en temas de seguridad, ya que dicha información es un recurso fácilmente vulnerable sino se adoptan medidas preventivas necesarias. Las políticas internas, correctas administraciones de datos personales y conjuntos de procesos instructivos se hacen verdaderamente necesarios en las organizaciones, en virtud a que permitan minimizar los peligros a los que se expone una persona frente a intentos de fugas de información personal. Una PIA (*PRIVACY IMPACT ASSESSMENT*) se considera como un proceso donde se lleva a cabo un esfuerzo consciente y sistemático para evaluar el impacto en la protección de datos personales de las opciones que pueden adoptarse en relación con una determinada propuesta o proyecto o como una evaluación de cualesquiera efectos actuales o potenciales que una determinada propuesta o proyecto podrían tener en la privacidad individual y las formas en las que estos efectos adversos se pueden mitigar.

La institución educativa “Heraldo Romero Sánchez” maneja dentro de sus procesos administrativos un sistema de información para la gestión académica y dentro de si toda la información de los estudiantes, docentes y personal administrativo. Por lo anterior, y los riesgos que pueden tener los usuarios, es necesario aplicar y analizar una PIA con el objetivo de evaluar el impacto en la protección de la privacidad de los datos personales de las personas de la institución. La aplicación de la PIA permitirá conocer el estado en aspectos de seguridad de la información y de esa manera tomar medidas que ayuden a mejorar la protección de los datos personales de la institución educativa “Heraldo Romero Sánchez”.

II. PRESENTACIÓN DEL PROYECTO DE INVESTIGACIÓN

A. Título

APLICACIÓN Y ANÁLISIS DE UNA PIA (*PRIVACY IMPACT ASSESSMENT*) PARA LA EVALUACION DE IMPACTO EN LA PROTECCION DE DATOS PERSONALES DE LA INSTITUCIÓN EDUCATIVA "HERALDO ROMERO SANCHEZ"

B. Línea de investigación

Este proyecto corresponde a la línea de investigación de gestión de seguridad y control.

C. Alcance y delimitación

Este proyecto aplicó una PIA sobre el sistema de información usado en la institución educativa "Heraldo Romero Sánchez". Para guiar el proceso de aplicación se utilizó la Guía para una evaluación de impacto en la protección de datos personales de la [1] en las fases 1 a la 6 que están dispuestas para tal fin. A partir de la aplicación de la PIA se realizó un proceso de análisis de la evaluación de impacto en la protección de datos personales de la institución y un informe final del mencionado proceso.

El sistema de información que usa la institución educativa "Heraldo Romero Sánchez" para la gestión académica cuenta con los siguientes módulos a los cuales se les aplicará la PIA propuesta en este proyecto:

- Administración del sistema.
- Notas.
- Gestión de estudiantes.
- Gestión de mensajes.
- Gestión de grados
- Gestión del personal
- Boletines
- Observaciones de los estudiantes

D. Modalidad

Este proyecto corresponde a la modalidad trabajo de investigación.

E. Planteamiento del problema

La información contenida en las diferentes organizaciones e instituciones públicas y privadas a través de sus sistemas de información puede generar preocupación en temas de seguridad, ya que dicha información es uno de los activos más importantes de las empresas, es un recurso fácilmente vulnerable sino se adoptan medidas preventivas necesarias. [2]

Para tener una visión global de la problemática en Colombia, es necesario revisar la información generada por el laboratorio del delito de la Policía Nacional, en donde se observa una alta vulnerabilidad en la información de las organizaciones y los ciudadanos. [3]

A partir del boletín generado por la Policía Nacional denominado "Tendencias Cibercrimen Colombia 2019 – 2020" [4] se puede observar la magnitud del riesgo en la que se encuentran los datos en las organizaciones, entendiendo esto como una alarma la cual motiva a la implementación de medidas preventivas para disminuir en una gran proporción la probabilidad ataques informáticos en especial a los a los datos personales.

Un ataque informático a la información, por pequeño que parezca genera una vulnerabilidad en la organización, misma que puede ser usada en muchas formas por delincuentes que sin estar facultadas para utilizar esta información, sacan provecho propio o para un tercero, que obtengan, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes aun siendo estos, causales de prisión y multas. [5]

Actualmente, existe la Ley 1581 de 2012 en el país para la protección de información, sin embargo dicha leyes por si solas no pueden prevenir los riesgos de no tener una política de protección de la información. [6]

En las instituciones educativas de Colombia, una serie de políticas internas, una correcta administración de datos personales y un conjunto de procesos instructivos se hacen verdaderamente necesarios, todo ello en virtud a que permiten minimizar los peligros a los que se expone un alumno menor de edad frente a intentos de fugas de información personal, contribuyendo a la mayor seguridad de un sistema más aún cuando los aplicativos de información de las instituciones tienen un continuo contacto con redes de datos externas, y cuando los hackers y ciberdelincuentes proliferan siempre en la búsqueda de oportunidades de robo de información que les permita su propio lucro. [7]

Por lo anterior, se aplicó una PIA (*PRIVACY IMPACT ASSESSMENT*) para la evaluar el impacto en la protección a datos de la institución educativa "Heraldo Romero Sánchez". Dicha institución

educativa utiliza sistemas de información los cuales manejan gran cantidad de datos, como son la Plataforma de Gestión Académica y el SIMAT, que funcionan con conexión a internet, y bases de datos de un nivel alto de importancia y concurrencia a nivel nacional, tanto de personal administrativo, docente y alumnado.

Teniendo en cuenta que hasta el momento no se ha realizado un proceso evaluativo de la protección de datos personales en la institución, ni se cuentan con protocolos o políticas de seguridad de la información, es necesario aplicar una PIA y analizar los resultados generados a partir de dichos procesos, de esa manera la institución podrá tomar medidas en el aspecto de seguridad de la información.

F. Formulación del problema

Debido a la importancia que tiene prevenir posibles intrusiones en los sistemas de información, se genera la siguiente pregunta de investigación:

¿Cómo la aplicación y el análisis de una PIA (PRIVACY IMPACT ASSESSMENT), permitirá mejorar la protección de los datos personales en la institución educativa "Heraldo Romero Sánchez"?

G. Sistematización del problema

¿Qué tan necesario resulta aplicar una PIA para la evaluación de Impacto en la protección de datos personales en la institución educativa "Heraldo Romero Sánchez"?

¿Qué sistemas de información son adecuados para aplicarles una PIA?

¿Qué aspectos determinan que los sistemas de información son vulnerables al mal uso de los datos personales en la institución educativa "Heraldo Romero Sánchez"?

¿Cuáles son los resultados de la aplicación de la PIA para la evaluación de impacto en la protección de los datos personales en la institución educativa "Heraldo Romero Sánchez"?

H. Objetivo general

Mejorar la protección de los datos personales de la institución educativa "Heraldo Romero Sánchez" mediante la aplicación de una PIA (*PRIVACY IMPACT ASSESSMENT*).

I. Objetivos específicos

- Identificar el sistema de información y los datos personales que utilizan en la institución educativa “Heraldo Romero Sánchez”.
- Aplicar una PIA (*PRIVACY IMPACT ASSESSMENT*) para la evaluación de impacto en la privacidad de los datos personales de la institución educativa “Heraldo Romero Sánchez”.
- Analizar y generar un informe de la aplicación de la PIA (*PRIVACY IMPACT ASSESSMENT*) en el sistema de información de la institución educativa “Heraldo Romero Sánchez”.

J. Justificación

Es importante destacar que junto con la proliferación y manejo de información de datos personales por parte de diferentes organizaciones se evidencia el gran riesgo al que se enfrentan cada vez más las personas al tener que confiar su información a las mismas. [8]

Uno de los procesos más utilizados para medir el impacto de la protección de datos corresponde a la aplicación de PIA (*PRIVACY IMPACT ASSESSMENT*), ya que se puede aplicar a cualquier sistema de información de las organizaciones con el fin de encontrar vulnerabilidades y que puede servir como insumo para el desarrollo de políticas de privacidad de datos personales o protocolos de seguridad.

Las políticas de privacidad de datos personales permiten manejar de manera efectiva la información de los usuarios que puede ser sensible robo o malos manejos. Debido a que la institución educativa “Heraldo Romero Sánchez” no cuenta con una política de privacidad de datos personales es necesario aplicar una PIA en el sistema de información que usan datos personales de alumnos, docentes y administrativos. [9]

A partir de la aplicación de la PIA y el informe generado, la institución educativa “Heraldo Romero Sánchez” podrá tomar medidas a posibles vulnerabilidades en aspectos de seguridad de la información y de esa manera mejorar niveles de vulnerabilidad posibles.

K. Antecedentes

Dentro del marco de desarrollo de este proyecto se revisaron diversas propuestas de diversos autores los cuales aportan al entendimiento del contexto de esta investigación. Cada propuesta describe características que son fundamentales en aspectos de privacidad de la información y seguridad, en los puntos siguientes se describen con mayor detalle.

L. Protección de datos personales

A partir de las investigaciones y consultas que se realizaron en la literatura de diferentes países, se encontró que existe una gran cantidad de material digital relacionado con los derechos a la protección a datos personales como derecho fundamental, como también la auditoria a las bases de datos de las organizaciones, investigaciones realizadas en diferentes organizaciones. [10]

Según Sánchez Perez & Rojas [11], diversos países han promulgado leyes de protección de datos personales y en cada país se ha buscado adaptar, a sus propias condiciones culturales, económicas y políticas, las bases de alguno de los dos modelos de protección de datos personales existentes.

A continuación, se mencionan algunos casos relevantes sobre las leyes de protección de datos personales de distintos países, organizaciones y regiones del mundo:

- Organización de Naciones Unidas (ONU): En 1948, adopta el documento conocido como Declaración Universal de Derechos Humanos, en la que el artículo 12 señala que las personas tienen derecho a la protección de la ley de sus datos personales.
- Alemania: En 1970 fue aprobada la primera ley de protección de datos (Daten Schütz). En 1977, el Parlamento Federal Alemán aprueba la Ley Federal Bundesdatenschutzgesetz. Estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada.
- Suecia: En 1973 fue publicada la que fue una de las primeras leyes de protección de datos en el mundo.
- Estados Unidos de Norteamérica: La protección de datos tiene base en la Privacy Act de 1974.
- Unión Europea: El primer convenio internacional de protección de datos fue firmado en 1981 por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocido como "Convenio 108" o "Convenio de Estrasburgo". En los 90's, se establece una norma común que se denominó Directiva 95/46/CE. La directiva es referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- España: La ley Orgánica 15 de 1999, establece la Protección de Datos de Carácter Personal. Está ley ha sido importante para Latinoamérica porque se ha utilizado como firme referente del modelo europeo.
- Latinoamérica: En América Latina, las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las tecnologías de la información y el aumento de las vulnerabilidades asociadas. En su mayoría, estas leyes se asemejan al modelo europeo: En Argentina la Ley 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), Uruguay (2008).
- Rusia: En el año 2006 fue aprobada una exhaustiva ley de protección de datos personales.
- Perú: La ley 29.733 del 2 de julio de 2011 es la más reciente ley de protección de datos personales en el mundo.

- México. La Ley Federal de Protección de Datos Personales en Posesión de Particulares fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010, entró en vigor un día después y tiene efecto a partir de enero del año 2012

Desde la década de los 80´s se encuentran antecedentes en Colombia en cuanto al derecho de protección a datos personales, iniciativa liderada por la Universidad de los Andes en 1986, la cual elaboró un proyecto de ley de datos personales que sirvió de punto de referencia para dar inicio a un debate parlamentario de perfil permisivo sobre habeas data. Lo anterior consistió en la licitud de construir bancos de datos de información personal, previa condición de ser comunicados a una autoridad de control, y tiene como objeto la tutela, por vía de un desarrollo legislativo, de los datos de las personas físicas y jurídicas frente a bancos de datos públicos y privados, ya sean manuales o informáticos. [12]

En la institución educativa "Heraldo Romero Sánchez" no se evidencia una política de privacidad de datos ni con un protocolo de seguridad de la información disponible para sus estudiantes, docentes y personal administrativo, sin embargo, se manifiesta por parte de sus directivos conocer la ausencia de dicho protocolo y la voluntad de conocer algunas recomendaciones para tomar las medidas necesarias.

M. Mecanismos para medir la privacidad de datos

1) ISO 27000

La norma ISO 27000 es un conjunto de estándares de Seguridad de la Información, se usa como estrategia de seguridad de la información en una empresa determinada, donde se aplican una serie de pasos o fases para llevar a cabo esta metodología. [13]

Como primera fase están los requerimientos del modelo de seguridad de la información, en la cual se utilizan talleres con los niveles estratégicos de la empresa.

La segunda fase es la determinación del alcance de la aplicación de la norma en la empresa.

La tercera fase contiene la guía para implementar y operar el Sistema de Gestión de la Seguridad de la Información, la cual se compone de los siguientes pasos:

- Definir el Comité de Seguridad de la Información.
- Designar el Oficial de Seguridad de Seguridad.
- Definir los objetivos de control y controles.

- Detección de incidentes y eventos de Seguridad.
- Realización de revisiones periódicas al Modelo de Seguridad de la Información.
- Imprentar las acciones correctivas y preventivas.
- Capacitación en el manejo de acción correctiva y preventiva.

En la cuarta fase se encuentra el análisis y evaluación de riesgos, la cual contiene los siguientes pasos:

- Establecer las guías de implementación para la identificación de Riesgos estratégicos para la empresa.
- Establecer las guías de implementación para la identificación de Riesgos operativos para la empresa.
- Definir la matriz para documentar los Riesgos Estratégicos.
- Definir la matriz para documentar los Riesgos Operativos

La quinta fase definida como guía para la elaboración del plan de continuidad del negocio, regida por los siguientes pasos:

- Establecer los pasos para la implementación del Plan de Continuidad el Negocio.
- Definir el Registro de Acciones antes de una Interrupción.

A pesar de que la norma ISO 27000 cuenta con una aceptación mundial en su aplicación además de sus excelentes resultados a aplicarla, no es apropiada para la aplicación en la institución educativa "Heraldo Romero Sánchez" puesto que el alcance de la medición de impacto se realizar sobre el sistema de información que maneja y esta norma se recomienda aplicar a aspectos más generales y de tipo administrativo.

2) ISO/IEC 15408

Los "Common Criteria" (ISO/IEC 15408) son el resultado de la unificación de las diferentes normativas internacionales confluyendo en un estándar único y común reconocido a nivel mundial. [14]

La norma ISO/IEC 15408 se entiende según Perito [15], como una guía muy útil que define un criterio estándar a usar como base para la evaluación de las propiedades y características de seguridad de determinado producto o Sistema IT y proporciona criterios y argumentos comprensibles para los diferentes perfiles de actores que se encuentran relacionados con las tecnologías de la seguridad:

- Los desarrolladores de productos o sistemas de tecnologías de la información (fabricantes) pueden ajustar sus diseños y explicar lo que ofrecen.
- Los evaluadores de seguridad, que juzgan y certifican en qué medida se ajusta una especificación de un producto o Sistema IT a los requisitos de seguridad deseados, es decir, puede evaluar y certificar lo que asegura.
- Los usuarios pueden conocer el nivel de confianza y seguridad que los productos de tecnologías de la información y sistemas le ofrecen. Pueden expresar cuáles son sus necesidades.

La Fig. 1 muestra gráficamente el proceso que lleva a cabo la norma ISO/IEC 15408.

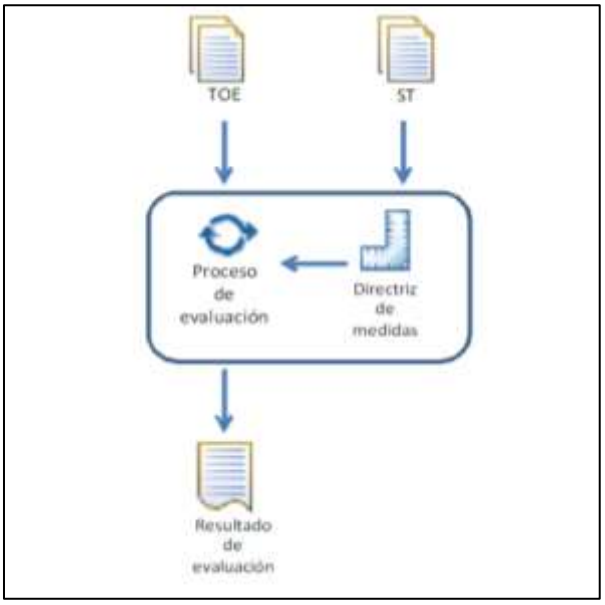

Fig. 1. Proceso de la norma ISO/IEC 15408
Fuente. Proceso de la norma ISO/IEC 15408. Tomado de [15]

A pesar de la efectividad de la aplicación de la norma ISO/IEC 15408, no se opta para usarla en este proyecto de investigación pues dicha norma es recomendada para equipos de desarrollo o procesos que involucran etapas tempranas en la implantación de tecnología en las organizaciones.

N. Resultados esperados

A partir de la aplicación de la PIA en el sistema de información de la institución educativa "Heraldo Romero Sánchez" se permitirá realizar un análisis de la situación actual en aspectos de seguridad de información relativo a la privacidad de la información personal de los usuarios.

El informe final de aplicación y análisis permitirá a la institución educativa tomar medidas para proteger la integridad de la información como activo de la institución educativa.

Este proceso de aplicación de una PIA, permitirá a futuros investigadores tener un marco de referencia para evaluar la privacidad de la información de diferentes organizaciones de la región y del país.

III. METODOLOGÍA

La metodología para la el desarrollo de este proyecto se enmarca en las fases que propone la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos [16], este proceso se describe en la Tabla 1.

TABLA I. METODOLOGÍA

Fase	Actividad
1	Análisis de la necesidad de evaluación
2	Descripción del proyecto
3	Identificación de riesgos
4	Gestión de riesgos identificados
5	Análisis del cumplimiento normativo
6	Informe final
7	Implementación de recomendaciones
8	Revisión y retroalimentación

Fuente: Elaboración propia a partir de Agencia Española de Protección de Datos [16]

IV. MARCO TEÓRICO

A. PIA (Privacy Impact Assessment)

El instrumento de evaluación de privacidad (PIA) o evaluación de impacto de protección de datos se refiere a la obligación del controlador de realizar una evaluación de impacto y documentarla antes de comenzar el procesamiento de datos previsto [17]. La evaluación del impacto de la protección de datos se debe llevar a cabo cuando existe un alto riesgo para los derechos y libertades de las personas. [18]

Dicha evaluación permite analizar los riesgos que un producto o servicio puede tener en temas de seguridad de la información y como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos. Este proceso se convierte en una herramienta que va más allá de una evaluación de cumplimiento normativo pues también se la privacidad que tienen las personas ante cualquier tratamiento de sus datos personales como en las percepciones generales de la sociedad o, concretamente, de los colectivos más afectados por el tratamiento del que se trate. [19]

Una de las definiciones de PIA más usada y que se propuso en un primer momento es la de la empresa [20], que afirma que: “una PIA se considera como un proceso donde se lleva a cabo un esfuerzo consciente y sistemático para evaluar el impacto en la protección de datos personales de las opciones que pueden adoptarse en relación con una determinada propuesta o proyecto o como una evaluación de cualesquiera efectos actuales o potenciales que una determinada propuesta o proyecto podrían tener en la privacidad individual y las formas en las que estos efectos adversos se pueden mitigar”.

Otra definición la propone [21] que afirma que una PIA se caracteriza por ser una metodología para evaluar el impacto en la privacidad de un proyecto, política, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales y, tras haber consultado con todas partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos.

La gran ventaja derivada de la aplicación de una PIA en sistema de información es que permite identificar los posibles riesgos y corregirlos rápidamente, además, la es un excelente ejercicio de transparencia, base de una relación de confianza pues ayuda a planificar las respuestas a posibles impactos en la protección de datos de los afectados, a gestionar las relaciones con terceras partes implicadas en el proyecto y a educar y motivar a los empleados para estar alerta sobre posibles problemas o incidentes en relación con el tratamiento de datos personales. [22]

B. Fases para la aplicación de una pia (Privacy Impact Assessment)

Según la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos [23], la cual es utilizada a nivel mundial para evaluar el impacto en la privacidad de los datos personales en las organizaciones, se deben seguir una serie de fases para su aplicación, a continuación se describen las fases:

1) Fase 1: Análisis de la necesidad de evaluación

Antes de adentrarse en los aspectos concretos de realización de una PIA es fundamental llevar a cabo una reflexión previa sobre las situaciones que aconsejarían su realización, ya que pequeños cambios o proyectos que no signifiquen modificaciones importantes o nuevos usos de datos personales pueden no justificar, por su sencillez y escasos riesgos para la privacidad, la realización de una evaluación de impacto.

Por otra parte, no todas las EIPD tienen por qué realizarse con la misma intensidad ni con el mismo grado de profundidad. Habrá casos en los que será posible llevarlas a cabo de una manera menos exhaustiva y formalizada (porque se ponga de manifiesto que los riesgos son escasos o fácilmente mitigables) mientras que en otras situaciones podrían incluso requerirse acciones adicionales a las aquí recogidas por la complejidad o la importancia de los riesgos existentes.

En efecto, en pequeñas o medianas organizaciones o en aquellas cuya actividad no implique un tratamiento masivo de datos de carácter personal o no esté orientada a la explotación de los mismos con finalidades que supongan una invasión notable de la privacidad, sería posible decidirse por una aproximación menos formalizada que conlleve una reflexión seria y responsable sobre los tratamientos de datos personales que se vayan a llevar a efecto y, así, detectar y minimizar los riesgos para los derechos de los afectados que los mismos pudieran entrañar.

2) Fase 2: Descripción del proyecto

Es importante conocer la información del proyecto y los sistemas de información en donde se va a aplicar la PIA. El contenido de esta documentación podrá contener objetivos, actores implicados, características de las tecnologías utilizadas, la necesidad que tienen los participantes de acceder y utilizar datos personales o categorías de datos personales específicas, etc.

La claridad con la que se expongan todos estos apartados es fundamental y para ello, además de utilizar un lenguaje claro, directo y comprensible, es de máxima importancia la inclusión de material gráfico que explique, de forma visual y resumida, las principales características.

3) Fase 3: Identificación de riesgos

En esta fase comienza específicamente la evaluación de impacto que el proyecto tendrá en la protección de datos personales, a través del análisis de toda la documentación generada se podrán conocer los riesgos, reales y percibidos, existentes para la privacidad.

Los riesgos pueden ser de dos tipos. El primero y principal es el que afecta a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

Pero tampoco hay que descuidar los riesgos que puede afrontar una organización por no haber implantado una correcta política de protección de datos o por haberlo hecho de forma descuidada o errática, sin poner en marcha mecanismos de planificación, implantación, verificación y corrección eficaces.

Entre estos riesgos podemos incluir los derivados de una percepción de falta de respeto a la privacidad o de cumplimiento de las expectativas de privacidad de las personas, lo que puede motivar una baja utilización de los productos o servicios ofertados; la aparición o el incremento de los costes de rediseño del sistema e, incluso, la retirada del mismo; la falta de apoyo de actores clave para la viabilidad del proyecto; la pérdida de reputación e Fig. pública y, por supuesto, la posibilidad de acciones de investigación y, en su caso, sancionadoras por parte de la autoridad de protección de datos competente.

4) Fase 4: Gestión de riesgos identificados

Una vez que se han identificado los riesgos del nuevo sistema, producto o servicio a través del análisis llevado a cabo por él, llega el momento de gestionar dichos riesgos.

En la teoría general de análisis de riesgos se contemplan diversas opciones dependiendo del impacto que su materialización tendría para la organización: evitarlo o eliminarlo, mitigarlo, transferirlo o aceptarlo.

5) Fase 5: Análisis del cumplimiento normativo

Uno de los aspectos decisivos en el proceso es el relativo a la verificación de la conformidad del proyecto con las distintas regulaciones que pueden contener elementos relativos a la privacidad y a la protección de datos que le sean de aplicación.

6) Fase 6: Informe final

El equipo debe prestar una gran atención a la presentación de sus conclusiones a través de su informe final, que debería hacerse público (de forma completa o parcial si existen apartados que no pueden ser divulgados por restricciones legales, comerciales o de seguridad), por ejemplo, a través del sitio web de la organización o de forma física en las instalaciones.

7) Fase 7: Implementación de recomendaciones

El informe final debe ser remitido a la alta dirección de la organización para que tome las decisiones necesarias en relación con las recomendaciones realizadas y las medidas sugeridas.

Este informe tiene dos motivos, el primero de ellos es que la dirección defina y tome las decisiones necesarias para poner en marcha los cambios o mejoras que hubieran de ser introducidas en el proceso tomando como base las sugerencias realizadas en el informe y, en segundo lugar, debe establecer la persona o unidad responsable de coordinar que se implanten las medidas recomendadas y, para que su labor resulte eficaz, investirla de la necesaria autoridad para realizar su trabajo, y comunicar a la dirección los avances y dificultades que encuentre en el mismo.

8) Fase 8: Revisión y retroalimentación

Una vez que se han obtenido los resultados y se han implantado las medidas correctoras y de mejora adoptadas por la alta dirección de la organización llega el momento de la revisión y comprobación de su implantación real y de su eficacia.

Es necesario, pues, examinar el proyecto una vez operativo para verificar que los riesgos detectados se han abordado correctamente y que no existen otros nuevos que en su momento pasaron desapercibidos o que han surgido posteriormente, lo que llevaría aparejada una nueva iteración de las fases de la PIA.

Por ello, una evaluación de impacto, aunque tiene una importancia y un protagonismo especial en las fases iniciales de un proyecto, es un proceso que acompaña al sistema de información, producto o servicio durante todo su ciclo de vida.

V. DESARROLLO DEL PROYECTO DE INVESTIGACIÓN

El desarrollo de este proyecto de investigación se realiza mediante las fases que propone la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos [24], dado que los objetivos determinan que el alcance del proyecto, sea la aplicación de una PIA y el análisis de los resultados hasta la entrega de un informe final, para el desarrollo de este proyecto se contemplan las fases de la 1 a la 6. Las fases 7 y 8 de la Guía no se tienen en cuenta en este proceso, puesto que hacen referencia a la implementación de las recomendaciones por parte de la institución educativa, y la revisión y retroalimentación a dicha implementación.

El proceso desarrollado en cada fase de aplicación de la PIA se describe a continuación:

A. Fase 1: Análisis de la necesidad de evaluación

Para el desarrollo del proyecto y siguiendo la metodología propuesta, se analizó inicialmente la situación actual en aspectos de seguridad de la información personal en las instituciones educativas del municipio de Pasto, que según la Policía Nacional y el observatorio del delito, evidencian que existen vulnerabilidades y que las cifras están en crecimiento. [25]

Igualmente, desde el municipio se tiene la necesidad de mejora en el aspecto de la privacidad de la información. El Concejo Municipal de Pasto, al ver esta necesidad decide seguir los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a Ia información dando cumplimiento al Decreto 1078 de 2015. [26]

Se realizó un entrevista con Ritha Jurado, secretaria de la institución educativa “Heraldo Romero Sánchez” de la ciudad de Pasto, siendo ella una de las encargadas del manejo del sistema de información que usa la institución, es dicha entrevista, la secretaria dio a conocer que no sabía si este sistema de información fue creado bajo alguna norma de seguridad, a pesar de esto, ella piensa que es de vital importancia y es muy relevante que este sistema de información este regido por alguna norma de seguridad de información.

Por lo anterior, ya que es necesario mejorar los aspectos de seguridad en el municipio, por ende, en las instituciones educativas y dada la necesidad de la institución educativa “Heraldo Romero Sánchez en mejorar sus aspectos de seguridad de la información, se propone realizar la aplicación de una PIA en el sistema de información que la institución maneja.

B. Fase 2: Descripción del proyecto

La aplicación de la PIA se realiza sobre el sistema de información que usa la institución educativa "Heraldo Romero Sánchez", la cual tiene la siguiente descripción:

1) Datos generales:

- Nombre de la Institución: I. E. "HERALDO ROMERO SÁNCHEZ"
- Registro Dane: 152001001153
- NIT: 800019467 – 8
- Código ICFES: : 046326 Clave OKUNEWVS
- Dirección: Carrera 2ª No. 23 – 45, Barrio La Carolina
  Calle 22 No. 4 – 74, Barrio El Ejido
- Teléfono: 7300080 – 7309499
- Municipio: Pasto
- Departamento: Nariño
- Modalidad la Institución: Académica
- Oferta Educativa: Nivel de Preescolar
  Nivel de Básica: Primaria - Secundaria
  Nivel de Media
  Programa Educación de Jóvenes y Adultos
- Rector: Esp. Ricardo Campaña

2) Misión

La Institución Educativa Municipal Heraldo Romero Sánchez, propicia procesos de formación integral, con énfasis en competencias académicas, ciudadanas y laborales generales. Promueve espacios participativos, fundamentados en los derechos humanos y en los valores éticos, sociales y ambientales en la búsqueda de una sana convivencia.

3) Visión

La Institución Educativa Heraldo Romero Sánchez, forma seres integrales, capaces de tomar decisiones, liderar procesos de desarrollo humano, académico y tecnológico, con calidad y calidez; haciendo de ellos personas transformadoras de su realidad individual y comunitaria a través de la construcción y realización de su proyecto de vida.

4) Estructura organizacional:

En la Fig. 2 se presenta la estructura organizacional de la institución educativa “Heraldo Romero Sánchez”.

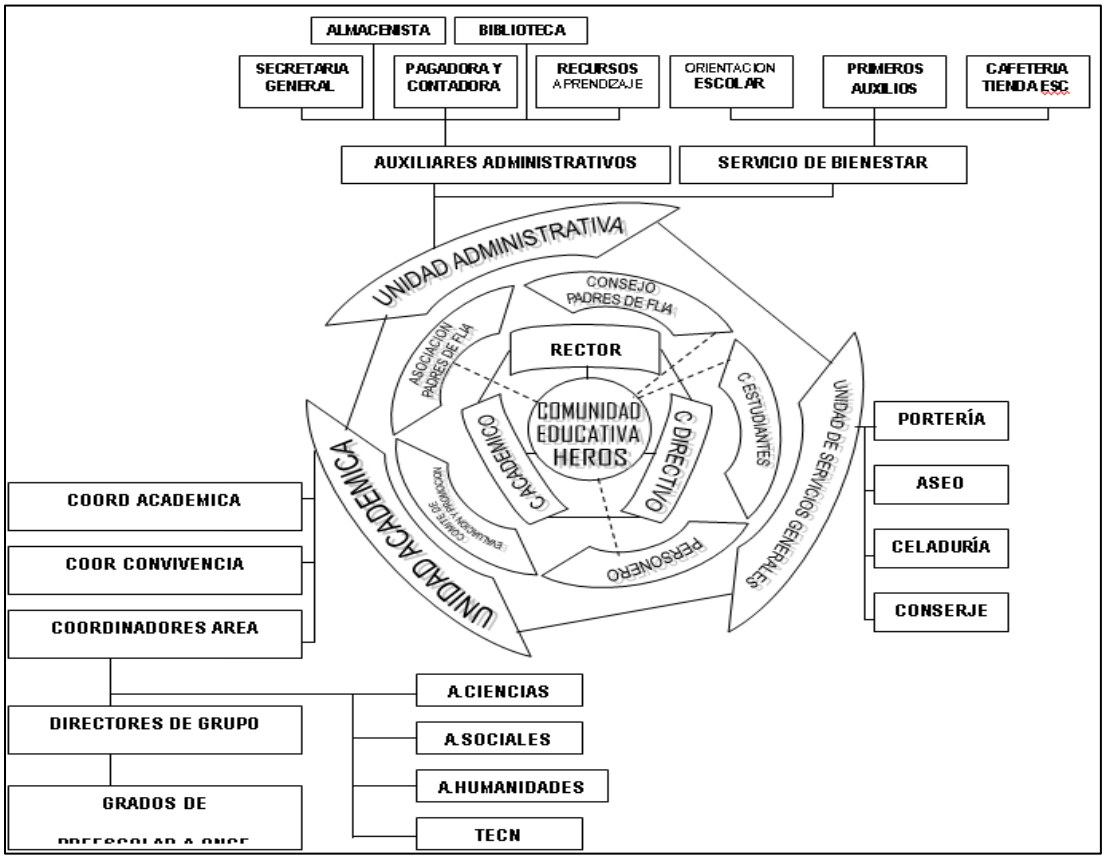

Fig. 2. Estructura organizacional institución educativa “Heraldo Romero Sánchez”
Fuente. Estructura organizacional. Tomado del archivo de la institución educativa “Heraldo Romero Sánchez

5) Sistema de Información utilizado:

El sistema de información que utiliza la institución educativa “Heraldo Romero Sánchez” se denomina GAWSS, producto que hace parte de una empresa colombiana dedicada al desarrollo de software, especialmente para ambientes Web, uno de sus grandes productos es el Sistema De Gestión Académica y Administrativa, el cual fue creado para un mejor manejo de la información de las instituciones educativas, dando así un mejor uso de las herramientas informáticas y así una mejor gestión de todos los datos.

En la entrevista con Ritha Jurado, secretaria de la institución educativa “Heraldo Romero Sánchez” de la ciudad de Pasto, manifiesta que su sistema gestiona la información de todos los

estudiantes, profesores y administrativos de dicha institución, además por ser un entorno orientada a la web no es necesario que los equipos utilizados por la institución tengan características muy altas a nivel de hardware ni software.

La secretaria Ritha Jurado y el secretario Raúl Caicedo son los encargados de matricular a todos los estudiantes que ingresan a la institución educativa.

Por otro lado, se entrevistó a la coordinadora académica la cual es la encargada del manejo general, es la única persona en la institución que tiene acceso al súper usuario del sistema de información, la coordinadora afirma que este sistema es fácil de manejar, porque su interfaz es muy sencilla de entender, además que no existe ninguna complejidad a la hora de ingresar y obtener datos y está de acuerdo que la información que maneja este sistemas es de vital importancia para el funcionamiento de la institución, en la parte académica y disciplinaria.

Por lo anterior, se concluye que el sistema de información utilizado por la institución maneja una base de datos de los padres de familia, manejan estadísticas las cuales sirven de planeación, para sacar información de cada estudiante, para las izadas de banderas, etc. y por lo tanto esta debe ser protegida correctamente. Un aspecto importante en la entrevista con la coordinadora académica fue que el proveedor del sistema de información no dejó ningún manual para usuario, simplemente realizaron capacitaciones al personal en el manejo de la herramienta.

Es importante resaltar que la copia de seguridad es constante, aunque el servidor y la base de datos la tienen en sus manos los proveedores

Este sistema maneja la información de más de 1200 personas en la cual la mayoría son estudiantes, 46 profesores, 2 administrativos, 4 directivos, cada uno con su respectivo usuario y contraseña con acceso a cada una de las funciones que necesita cada usuario, ya que todos no tienen permitido hacer gestión de todos los recursos del software

Desde que inicio el funcionamiento de este sistema de información ha tenido algunas fallas muy leves, pero las cuales han sido solucionadas únicamente por los proveedores ya que estos son los únicos encargados del mantenimiento de este sistema.

Este software cuenta con ventanas o formularios los cuales reciben variables de digitación numérica y de texto, a continuación, se presentan las principales funcionalidades del sistema en el que se usa información personal de los usuarios finales:

Fig. 3. Inicio de sesión
Fuente: Elaboración propia a partir del sistema de información de la institución

Al entrar al dominio establecido por el software se presenta una ventana en la cual se ingresa el nombre del usuario.

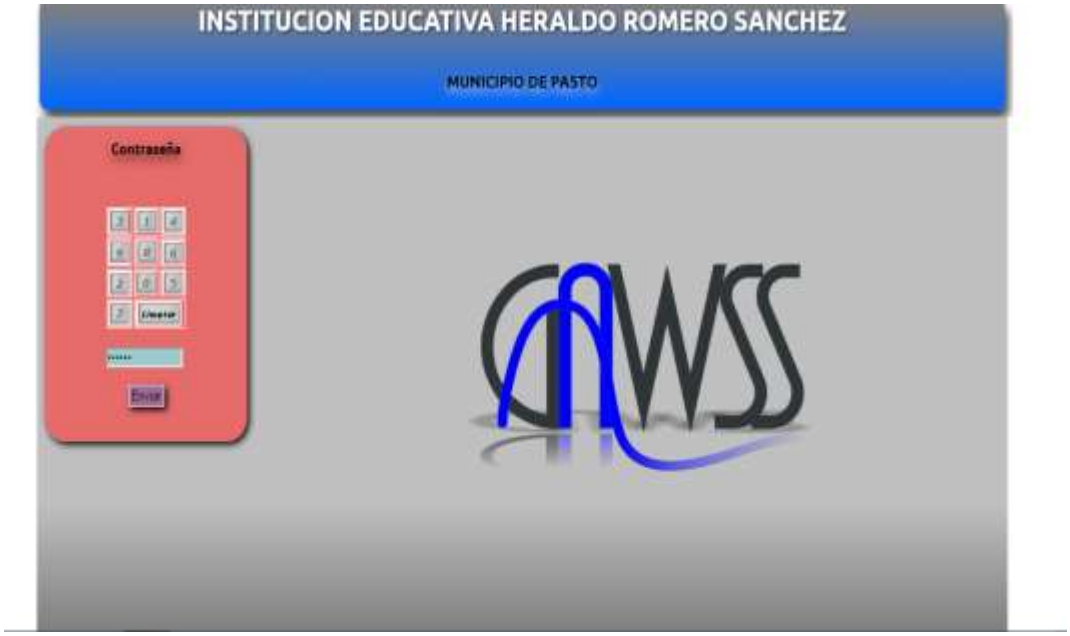

Fig. 4. Contraseña de usuario
Fuente: Elaboración propia a partir del sistema de información de la institución

En esta parte luego de haber ingresado el nombre de usuario se digita la contraseña respectiva y la cual el software válida para así mismo pasar a tener ingreso a todo lo que conforma el software Gawss

Fig. 5. Validación de credenciales
Fuente: Elaboración propia a partir del sistema de información de la institución

Esta es la pantalla principal que aparece luego de haber ingresado, en la parte izquierda se observa la caja de opciones las cuales maneja este sistema de información con respecto a todo el manejo de datos que necesita la institución educativa, en el centro se observa una cuadro de noticias e información para tener en cuenta en qué periodo se encuentra cada una de las jornadas que maneja esta institución, y en la parte derecha se encuentra una serie de funciones un poco más personales del usuario.

A continuación, se verá las figuras respectivas a cada uno de los módulos los cuales maneja el flujo de la información de la institución educativa.

Fig. 6. Gestión de año lectivo
Fuente: Elaboración propia a partir del sistema de información de la institución

En esta ventana podemos cambiar el año lectivo, el cual sirve para tener los datos en el año correcto y poder tener información de años anteriores.

Fig. 7. Gestión de grados y cursos
Fuente: Elaboración propia a partir del sistema de información de la institución

Esta parte maneja un formulario con la lista de los grados con sus respectivos cursos, y además su director de grupo.

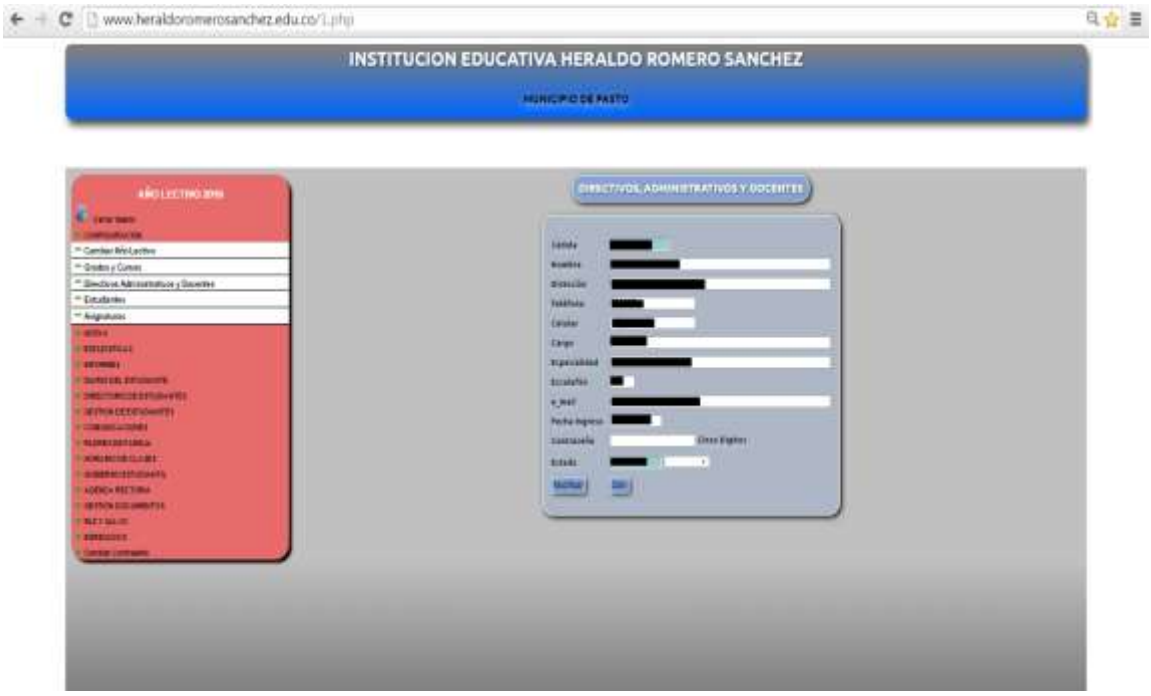

Fig. 8. Gestión del personal de la institución
Fuente: Elaboración propia a partir del sistema de información de la institución

En esta parte es donde se ingresa la información de cada uno de los docentes, directivos y administrativos de la institución educativa.

Fig. 9. Gestión de estudiantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En esta parte es donde se ingresa toda la información de los estudiantes que pertenecen a la institución, con una particular características en su estado, el cual puede cambiar, activo, retirado.

Fig. 10. Gestión de estudiante
Fuente: Elaboración propia a partir del sistema de información de la institución

Al ingresar a la parte de estudiantes aparecerá esta tabla donde aparece el número el curso, código, nombre, repitente y estado. Además, que aparecen dos botones uno de ellos es ingresar el cual nos lleva a un nuevo formulario el cual ingresamos todos los datos de un estudiante nuevo.

Fig. 11. Gestión de desempeño
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se lista el desempeño de la asignatura según el grado, de acuerdo a un periodo.

Fig. 12. Gestión de temas
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se listan los temas que se han visto en la asignatura según el grado y de acuerdo al periodo académico que se desea.

Fig. 13. Consultar notas por curso
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se puede consultar las notas de cada curso por área, ingresando la sede la jornada y el periodo exacto el cual se desea.

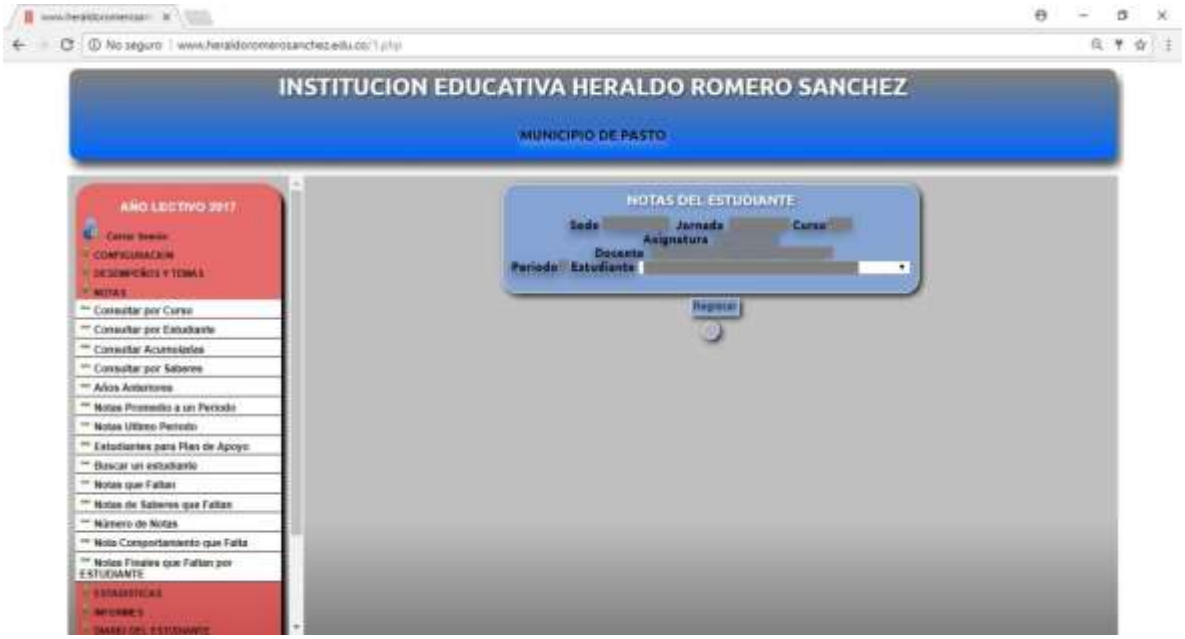

Fig. 14. Consultar notas de estudiante
Fuente: Elaboración propia a partir del sistema de información de la institución

Luego de ingresar la sede, jornada y periodo se procede a buscar el nombre del estudiante deseado, y en seguida mostrara las notas respectivas de dicho estudiante.

Fig.15. Consultar notas acumuladas
Fuente: Elaboración propia a partir del sistema de información de la institución

En esta parte elegimos la sede, jornada, curso y asignatura, inmediatamente aparecerá en pantalla la lista de los estudiantes de dicho curso y sus notas de los periodos que van cursando.

Fig. 16. Consultar notas de años anteriores
Fuente: Elaboración propia a partir del sistema de información de la institución

Se ingresa el nombre y apellido del estudiante del cual se desea saber la nota de los años anteriores cursados, y aparecerá una tabla con todas las notas de dicho estudiante y su respectivo año.

Fig. 17. Notas por periodos
Fuente: Elaboración propia a partir del sistema de información de la institución

Se elige la sede, la jornada, y posteriormente el periodo que desea, y aparecerá en pantalla las notas de todas las materias de dicho curso por cada estudiante.

Fig. 18. Notas del último periodo
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparecen las notas del último periodo de los estudiantes de cada curso.

Fig. 19. Plan de apoyo a estudiantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se hace una lista de todos los estudiantes que tienen las notas más bajas e integrarlos a un plan de apoyo para subir su rendimiento.

Fig. 20. Notas faltantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se lista el nombre del profesor, el curso y la asignatura que falta por entregar las notas.

Fig. 21. Número de evaluaciones digitadas
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se lista el nombre del profesor, curso, asignatura que dicta y el número de notas que ha realizado a un periodo determinado.

Fig. 22. Notas de comportamiento faltantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece la sede, jornada y el curso a los cuales no se le han digitado la valoración de comportamiento.

Fig. 23. Notas finales faltantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece el listado de los estudiantes a los cuales les faltan sus notas finales, y el profesor de dicha asignatura.

Fig. 24. Cuadro de honor de estudiantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se lista a los estudiantes con las mejores notas de cada curso, y el respectivo puesto que ocupa de manera descendente.

Fig. 25. Cuadro de honor por cursos
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparecerá el cuadro de honor de cada respectivo curso.

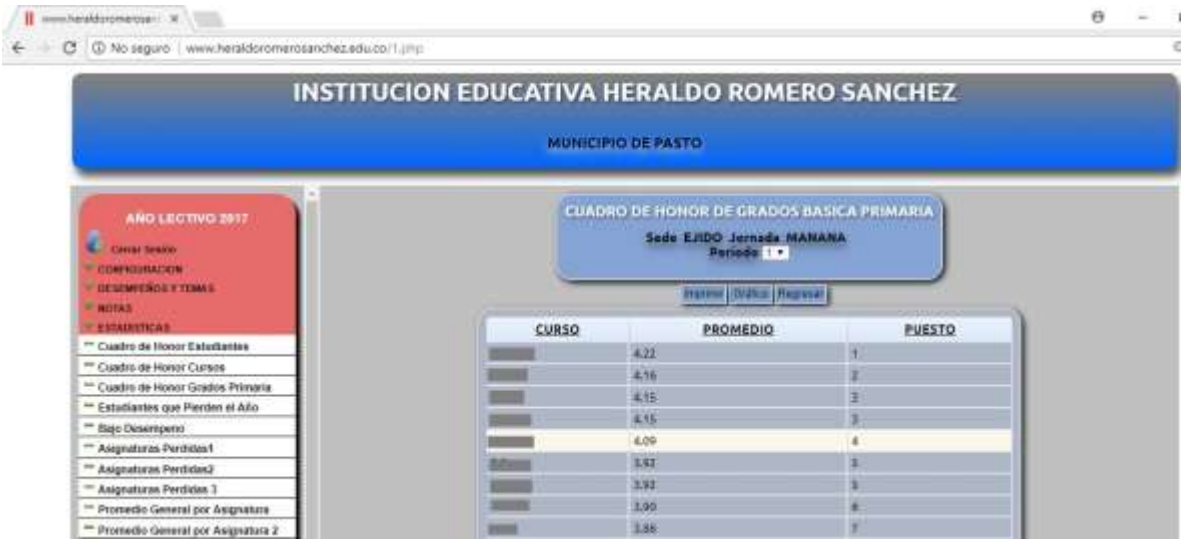

Fig. 26. Cuadro de honor de la primaria
Fuente: Elaboración propia a partir del sistema de información de la institución

En esta parte se hace una lista de los mejores promedios de los cursos de la primaria, con su respectivo puesto.

Fig. 27. Estudiantes que pierden el año
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se elige la sede y jornada del colegio que se desea saber cuántos alumnos perdieron.

Fig. 28. Rendimiento académico
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se lista el número de estudiantes por curso que tienen un bajo desempeño, con su respectivo porcentaje de acuerdo al número total de estudiantes por curso.

Fig. 29. Estudiantes con asignaturas perdidas
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece todas las sedes con sus respectivos grados, y al dar clic en elegir aparecerá cada curso que pertenece a cada grado, con las respectivas materias y el número de estudiantes que han perdido por materia.

Fig. 30. Promedios por asignaturas
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece el listado del promedio general de notas por materia y por curso.

Fig. 31. Impresión de boletines por curso
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece el listado de todos los cursos, y al elegir el formato en el que se quiere imprimir, aparece todos los boletines de los estudiantes de acuerdo a su curso.

Fig. 32. Carta comunicativa
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se imprime una carta para los padres de familia, para informarles sobre la entrega de boletines.

Fig. 33. Informe final
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece listado de acuerdo al año, todos los cursos con sus respectivos boletines de los estudiantes y las notas de los periodos, y sus logros de acuerdo a cada área, además aparece si aprobó o reprobó el año.

Fig. 34. Certificados de estudios
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario luego de haber ingresado la sede, jornada y el año lectivo del estudiante que desea el certificado, se despliega una lista de los cursos, al dar clic en elegir aparecen todos los estudiantes de ese curso y ya puedes imprimir el certificado.

Fig. 35. Certificados parciales
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario luego de haber elegido la sede, jornada y el curso, aparece un listado de los estudiantes con su respectivo código, nombre y estado. Luego se da clic en imprimir en el nombre del estudiante deseado, y así obtendrá el certificado parcial de estudios.

Fig. 36. Inicio de sesión
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formato aparece una lista de los estudiantes, y podremos imprimir la constancia de estudio del estudiante el cual queremos imprimir.

Fig. 37. Constancias de trabajo
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece la lista de todos los trabajadores que laboran en la institución, al dar elegir en el trabajador deseado imprime la constancia de trabajo requerida.

Fig. 38. Listado de docentes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece el listado de todos los docentes que trabajan en la institución, ya sea en la jornada de la mañana, tarde o noche.

Fig. 39. Registro de clases
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se registra el movimiento diario de clases que tienen los profesores según la asignatura, teniendo en cuenta la fecha el tema que se ha dictado, y el número de horas. Además, aparece una observación si algo fuera de lo normal ocurre en el transcurrir de la clase. Ej.: si no hubo clases porque el profesor no asistió.

Fig. 40. Consulta de faltas de asistencia
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece una lista por fecha del número de estudiantes que no asistieron a clases en un curso específico.

Fig. 41. Ingresar información al diario del estudiante
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se coloca todas las faltas disciplinarias, que comete el estudiante.

Fig. 42. Observaciones de estudiantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece el seguimiento disciplinario de todos los estudiantes de acuerdo a la sede y a la jornada. Además, que se puede modificar si algo esta herrado, y se puede imprimir dichas faltas disciplinarias.

Fig. 43. Resumen de inasistencia
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece el listado de los estudiantes de un curso con el resumen de la inasistencia que ha tenido en un periodo anteriormente seleccionado, detallado con el código, nombre, el número de faltas sin justificar, las llegadas tardes, permisos, evasiones y el total de horas.

Fig. 44. Informe general de observaciones
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece de forma general todas las observaciones de faltas disciplinarias de los estudiantes de un curso a un periodo específico.

Fig. 45. Información de observaciones de coordinación
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece de manera detallada la lista de los estudiantes las faltas disciplinarias, para la coordinación.

Fig. 46. Diario de un estudiante
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se puede apreciar todas las observaciones hechas por los profesores de las distintas materias a cada estudiante.

Fig. 47. Diario de un estudiante en coordinación
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario la coordinación tiene de manera detallada la información de todas las observaciones que han hecho los docentes a cada estudiante de la institución.

Fig. 48. Diario general de estudiantes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece la lista de los estudiantes de un curso con una parte de su información personal

Fig. 49. Información especial de un estudiante
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario tenemos a los estudiantes que tienen un problema más a fondo, y el cual necesita unas recomendaciones especiales.

Fig. 50. Mensajes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario aparece una especie de cartelera donde aparecen toda serie de mensajes, ya sea para docentes, estudiantes y padres de familia.

Fig. 51. Mensaje a docentes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se puede enviar un mensaje ya sea a un directivo o a un docente.

Fig. 52. Mensaje a todos los docentes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se puede enviar un mensaje a todos los docentes de la institución, de acuerdo a la sede y a la jornada.

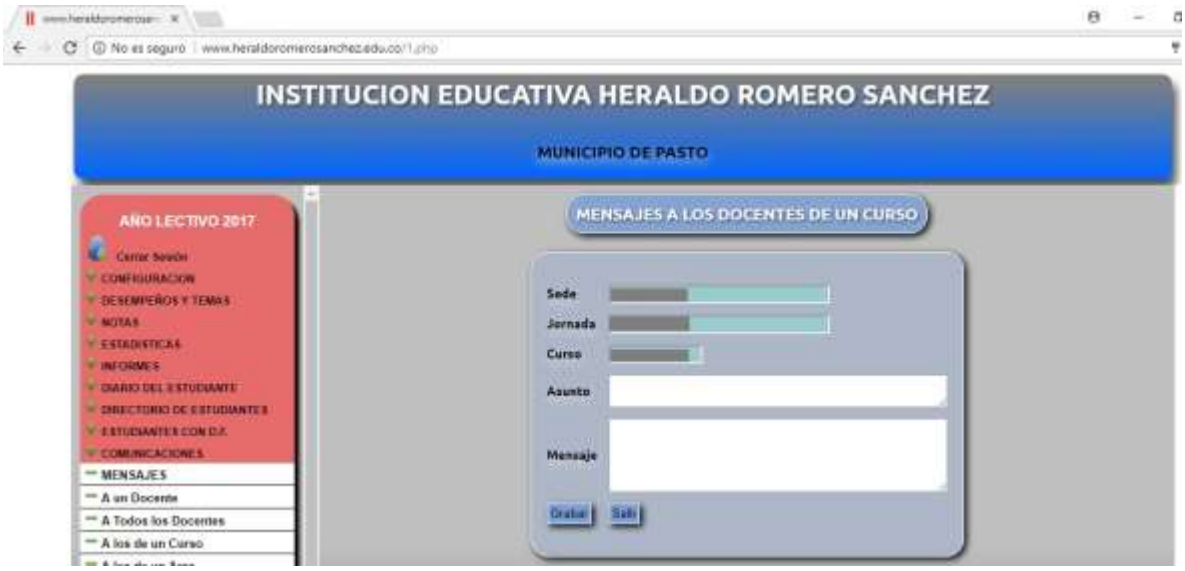

Fig. 53. Mensaje a docentes de un curso
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se puede enviar un mensaje a los docentes de un curso en específico.

Fig. 54. Mensaje a docentes por área
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario podemos enviar un mensaje a un docente según el área.

Fig. 55. Mensaje enviado
Fuente: Elaboración propia a partir del sistema de información de la institución

La institución no hace uso de este formulario.

Fig. 56. Mensaje a docentes
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario podemos realizar todas las noticias que se desee, además podemos ver el destinatario, ya sea docentes, estudiantes o padres de familia, y esto se podrá ver en el formulario de mensajes anteriormente visto.

Fig. 57. Visita a padres de familia
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario se registra las visitas que han hecho constantemente los padres de familia de cada estudiante.

Fig. 58. Noticias a padres de familia
Fuente: Elaboración propia a partir del sistema de información de la institución

Este formulario es el mismo anteriormente visto, pero solo para los padres de familia.

Fig. 59. Mensaje a padre de familia específico
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario podemos enviar un mensaje a un padre de familia de un estudiante específico. Ej.: podemos enviar una queja si el estudiante ha tenido un mal comportamiento.

Fig. 60. Mensaje a todos los padres de familia
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario podemos enviar un mensaje a todos los padres de familia. Ej.: cuando se tenga entrega de boletines.

Fig. 61. Mensajes a padres de familia
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario podemos enviar un mensaje a los padres de familia de un curso en específico.

Fig. 62. Novedades de personal
Fuente: Elaboración propia a partir del sistema de información de la institución

En este formulario podemos registrar alguna novedad que se presente a uno de los directivos, administrativos o docentes. Entre estas novedades están incapacidad, licencia, calamidad entre otras.

C. Fase 3: Identificación de riesgos

La escala de evaluación para medir el impacto de los riesgos identificados en este proceso sigue la categorización de escala de "Grados de valoración del conocimiento" que es apropiada cuando se pretende medir habilidades, actitudes, valores, competencias o despeño, dicha escala es propuesta por Hechavarría [27], la escala de medición se muestra a continuación:

- Muy Alto: Evento con ocurrencia de riesgo en curso.
- Alto: Evento con probabilidad de riesgo inminente a corto plazo.
- Medio: Evento con probabilidad de riesgo si no se toman medidas rápidas
- Bajo: Evento que no supone riesgo considerable
- Muy Bajo: Evento con riesgos mínimos o ausentes.

A continuación, se presentan los hallazgos encontrados en las visitas a la institución, entrevistas con el personal administrativo y uso del sistema de información.

- En revisión del sistema de información y la descripción que el mismo presente desde el proveedor, se evidencia que no cuentan con una política de privacidad de la información,

a pesar de ello, tanto las instituciones que manejan el software como el proveedor conocen la importancia de dicha política y están dispuesto a trabajar en ello.

- Es muy factible extraer los datos de los usuarios del sistema como nombres, identificación, teléfono y dirección, aunque se debe tener privilegios en el sistema para esta acción, es necesario establecer las políticas para evitar la extracción ilegítima de dicha información.
- En visitas a la institución educativa, se realizaron entrevistas informales con el personal en donde se evidencia que no conocen una política de tratamiento de datos ni de privacidad de los mismos, igualmente, las personas entrevistadas no conocen la posibilidad de ceder o negar el uso de su información a terceros.
- Se evidencia que los usuarios finales no conocen los datos que la institución tiene a su cargo, provocando dudas en el tratamiento de los mismos.
- Al revisar los procesos internos de la institución educativa, se encuentra que existen algunos datos repetidos y otros que se encuentran desactualizados en especial de los estudiantes graduados y de los docentes que salieron de la institución.
- Se evidencia información que no se utiliza en especial de usuarios que no hacen parte de la institución, dicha información debería tener un tratamiento especial.
- El sistema de información permite almacenar una mínima información mediante las cookies que maneja al ser un sistema Web. El proveedor afirma que es para mejorar la experiencia de usuario.
- No se evidencia un protocolo que garantice el resguardo de los datos personales para uso estadístico o uso comercial.
- Es posible que personas dentro del sistema utilicen información personal de los estudiantes para fines no académicos.
- En los procesos de la institución educativa se dificulta o imposibilita el ejercicio de los derechos de acceso, rectificación, Cancelación u oposición de los datos que se tiene de los estudiantes y docentes.
- No existe una política de seguridad de información que permita el acceso, rectificación, cancelación u oposición de los datos personales entregados.
- No existe una persona responsable de la seguridad de la información que maneja la institución, el rector asume que son competencias de la parte administrativa.
- Es necesario que los usuarios manejen contraseñas de acceso seguras para evitar accesos indebidos.
- Se desconoce por parte de los directivos de la institución las consecuencias de no contar con una política de protección de datos.

En la Tabla 2, se presentan los riesgos agrupados de acuerdo a los hallazgos encontrados anteriormente, por cada riesgo se muestra el nivel de impacto que tiene en la institución y la probabilidad de que dicho riesgo se materialice de acuerdo al análisis de los hallazgos y el estudio del sistema de información.

TABLA II. IDENTIFICACIÓN DE RIESGOS EN EL SISTEMA DE INFORMACIÓN DE LA INSTITUCIÓN EDUCATIVA "HERALDO ROMERO SÁNCHEZ"

Identificación del riesgo	Descripción del riesgo	Nivel de impacto	Probabilidad que se materialice
001	Pérdida de competitividad del producto o servicio derivada de los daños reputaciones causados por una deficiente gestión de la privacidad.	Bajo	20%
002	Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida.	Alto	85%
003	Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.	Medio	50%
004	Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.	Alto	90%
005	Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias.	Alto	85%
006	Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, , lo que puede derivar en la toma de decisiones erróneas.	Alto	80%
007	Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.)	Muy Bajo	20%
008	Garantías insuficientes para el uso de datos personales históricos, científicos o estadísticos.	Medio	40%
009	Carecer de procedimientos claros y de herramientas para garantizar la cancelación de oficio de los datos personales que han dejado de ser necesarios para la finalidad	Medio	35%
Identificación del riesgo	**Descripción del riesgo**	**Nivel de impacto**	**Probabilidad que se materialice**
010	Accesos no autorizados a datos personales.	Alto	75%
011	Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización.	Alto	90%
012	Dificultar o imposibilitar el ejercicio de los derechos de acceso, rectificación,	Medio	30%

	cancelación u oposición a la información personal		
013	Inexistencia de responsable de seguridad o deficiente definición de sus funciones y competencias	Alto	80%
014	Deficiencias organizativas en la gestión del control de accesos	Alto	90%
015	Deficiencias en la protección de la confidencialidad de la información.	Alto	75%

Fuente: Elaboración propia

D. Fase 4: Gestión de riesgos identificados

Una vez se encontraron y clasificaron los riesgos, el nivel de impacto y su probabilidad de materialización se analizan para buscar la gestión de dichos riesgos con la institución educativa. En la Fig. 63 se evidencia que el nivel de ocurrencia de la mayoría de riesgos es alto, por lo tanto, se es necesario tomar medidas correctivas.

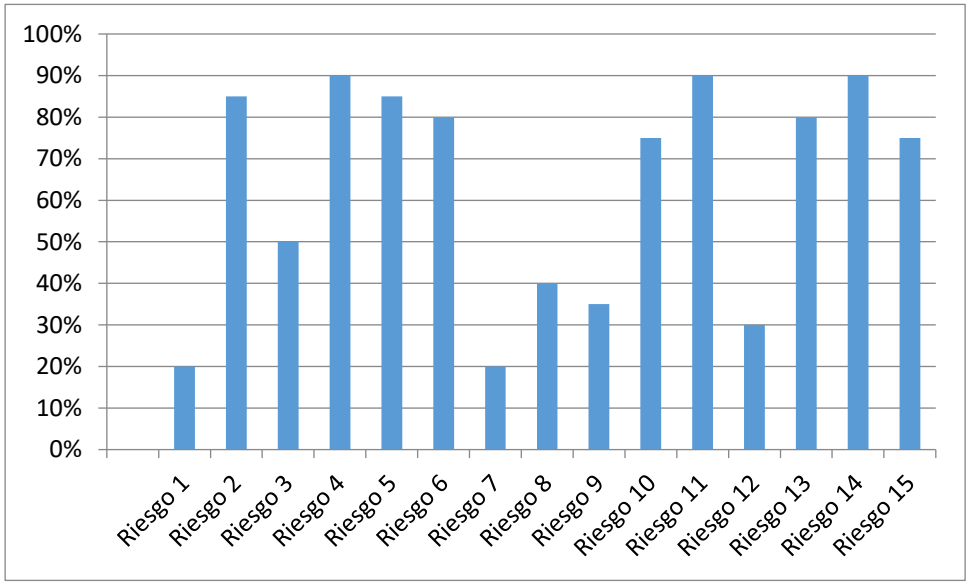

Fig. 63. Riesgos y probabilidad de que se materialicen
Fuente: Elaboración propia

Para poder mitigar los riesgos identificados, es necesario identificar un grupo de trabajo y de esa manera establecer responsabilidades, en especial en los riesgos que tienen un mayor nivel de impacto, como se muestran a continuación:

TABLA III. NÚMERO DE RIESGOS POR NIVEL DE IMPACTO

Nivel de impacto	Número de riesgos asociados
Muy Bajo	1
Bajo	1
Medio	4
Alto	9
Muy Alto	0

Fuente: Elaboración propia

Dicho grupo de trabajo será el encargado de realizar la respectiva investigación, y de facilitar cada detalle de la institución y colaborar de manera mutua para poder tener una evaluación más veraz y de mejor calidad, analizando los riesgos teniendo en cuenta que dicho software ya tiene un tiempo considerable de funcionamiento.

Con el equipo de trabajo conformado por los secretarios de la institución educativa, coordinador académico, coordinador disciplinario se definieron las siguientes medidas de mitigación de los riesgos:

TABLA IV. MEDIDAS ANTE LOS RIESGOS ENCONTRADOS

Identificación del riesgo	Medidas propuestas
001	• Formación apropiada del personal sobre protección de datos, seguridad y uso adecuado de las TIC
002	• Usar datos disociados siempre que sea posible y no implique un esfuerzo desproporcionado. • Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de personas. • Revisar de forma exhaustiva los flujos de información para detectar si se solicita datos personales que luego no son utilizados en ningún proceso. • Utilizar o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, si se pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas.
003	• Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas. • Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en un caso, las relativas a cesiones ulteriores así como a las posibilidades de supervisión y control del cumplimiento del acuerdo.

Identificación del riesgo	Medidas propuestas
004	• Asegurarse de que no existen otras causas de legitimación más adecuadas. • Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrece siempre la posibilidad de consentimiento separado para tratar daros con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato. • Evitar condicionar el disfrute de un producto o servicio al consentimiento para finalidades diferentes. • En el ámbito laboral, evitar basar los tratamientos de datos en el consentimiento de los trabajadores. • Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas
005	• Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas. • Verificar si el tratamiento está amparando o es requerido por una ley. • En caso contrario, establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.
006	• Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos los afectados se comunican a todos los sistemas de información y departamentos de la organización que estén autorizados a utilizarlos.

Identificación del riesgo	Medidas propuestas
007	• Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas. • Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada.
008	• Siempre que sea posible, utilizar datos anónimos o disociados. • Utilizar seudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, si pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un n mero reducido de personas. • Garantizar que se aplican las medidas de seguridad adecuadas y correspondientes al nivel de seguridad de los datos utilizados
009	• Definir claramente los plazos de cancelación de todos personales de los sistemas de información. • Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información. • Implantar mecanismos para llevar a cabo y gestionar dicha cancelación en el momento adecuado incluyendo, si corresponde, el bloqueo temporal de los datos personales.

Identificación del riesgo	**Medidas propuestas**
010	• Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales. • Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización. • Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento. • Notificar que se dará traslado a las autoridades competentes de las violaciones de confidencialidad que puedan entrañar responsabilidades penales. • Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales.
011	• Formación adecuada de los empleados sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información. • Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas
012	• Evitar establecer procedimientos poco transparentes, complejos y laboriosos. • Formar a todo personal para que conozca que ha de hacer si recibe una petición de derecho.

Identificación del riesgo	Medidas propuestas
013	• Nombramiento del responsable de seguridad y establecimiento por parte de la dirección de funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos. • Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del responsable de seguridad en las fases iniciales de los mismos
014	• Políticas estrictas de para la concesión de accesos a la información. • Establecer procedimientos que garantice la revocación de permisos para acceder a datos personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones, etc.) • Inventariar los recursos que contengan datos personales accesibles a través de redes de telecomunicaciones.

Identificación del riesgo	Medidas propuestas
015	• Adoptar medidas de cifrado adecuadas al riesgo y al estado de la tecnología de los datos personales Adoptar medidas de cifrado adecuadas al riesgo y al estado de la tecnología de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad. • Establecer procedimientos de notificación a las personas afectadas para el caso en que sus datos hayan podido ser accedidos o sustraídos por terceros no autorizados, informándoles de las medidas que pueden utilizar para minimizar los riesgos • Establecer procedimientos de notificación de quiebras de seguridad a la autoridad de control cuando ello sea legalmente exigible • Evitar, en general, las pruebas con datos reales y, en particular, cuando incluyan datos especialmente protegidos o un conjunto importante de datos que revelen aspectos relevantes de la personalidad de los afectados, cuando se empleen los de muchas personas o cuando participen en las pruebas un número elevado de usuarios. • Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc.)

Fuente: Elaboración propia

E. Fase 5: Análisis del cumplimiento normativo

Este proyecto se enmarca de acuerdo a las regulaciones de la Ley Colombiana y las normas establecidas por el Min TIC, quienes han avanzado en la creación de un marco legal y jurídico que protege el uso de estas tecnologías, la gestión de información a través de ella. Las leyes que rigen la aplicación de esta PIA son las siguientes:

1) Ley 1581 de 2012 - Protección de datos personales:

Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. [28]

Los principios y disposiciones contenidas en esta ley se aplican a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza ya sea pública o privada.

2) Ley 1273 de 2009 – Protección de la información:

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". [29]

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones". [30]

F. Fase 6: Informe final

A partir de la ejecución de la PIA sobre el sistema de información académico de la institución educativa "Heraldo Romero Sánchez", se presenta a continuación el informe ejecutivo de dicho proceso:

TABLA V. INFORME FINAL DE APLICACIÓN DE LA PIA EN LA INSTITUCIÓN EDUCATIVA "HERALDO ROMERO SÁNCHEZ"

Informe Ejecutivo

Aplicación PIA - Institución educativa "Heraldo Romero Sánchez"			
Versión	V01-2017	Fecha	Julio de 2020
Código	P01-EIP-2020	Responsable	Danny Taipe
Ciudad	Pasto	Tipo	Sistema de Información

Descripción:
Aplicación de una PIA sobre el sistema de información académico GAWSS usado por la institución educativa "Heraldo Romero Sánchez" a través de la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos.

Principales riesgos identificados:
Se identificaron 15 riesgos los cuales se encuentran en promedio con un nivel de impacto medio a alto, lo que quiere decir de qué se deben tomar medidas en aspectos de seguridad de la información.

Resumen de las medidas más importantes de mitigación propuestas:
De acuerdo a los hallazgos encontrados, se presenta una serie de recomendaciones a tomar en cuenta para minimizar el riesgo en aspectos de seguridad de la información. En términos generales, las recomendaciones apuntan a apropiarse del conocimiento de la importancia de la privacidad de la información, generar medidas de un resguardo seguro de dicho activo, informar los protocolos de privacidad de la información personal y generar una política de seguridad de la información.

Evaluación de privacidad

Nivel de Riesgo encontrado	Medio - Alto
Probabilidad de materialización de riesgos	63%

Motivación de la necesidad de la aplicación de la PIA:
La información contenida en las diferentes organizaciones e instituciones públicas y privadas a través de sus sistemas de información puede generar preocupación en temas de seguridad, diversas entidades a nivel nacional como (Policía Nacional, 2019), (Policía Nacional, Dijin, Tic Tac, & CCIT, 2019), y a nivel departamental afirman que se existe una gran probabilidad de ataques informáticos para afectar la privacidad de la información de las personas. A nivel de instituciones educativas no es la excepción puesto que como lo afirma (Data Protected, 2018), que se deben minimizar los peligros a los que se expone un alumno menor de edad frente a intentos de fugas de información personal, más aún cuando los aplicativos de información de las instituciones tienen un continuo contacto con redes de datos externas, generando oportunidades de robo de información.

Por lo anterior, se aplica una PIA (*PRIVACY IMPACT ASSESSMENT*) para la evaluar el impacto en la protección a datos de la institución educativa "Heraldo Romero Sánchez" de la ciudad de Pasto.

Cumplimiento normativo		Ley 1581 de 2012 - Protección de datos personales Ley 1273 de 2009 – Protección de la información	
Número de recomendaciones		44	
Tiempo estimado de aplicación de las recomendaciones		9 meses	
Inconvenientes	Ninguno	Duración de ejecución de la PIA	12 meses

Tareas

Descripción	Responsable
Presentar informe a directivos de la institución educativa "Heraldo Romero Sánchez" sobre la evaluación de la privacidad de los datos personales.	Danny Taipe
Realizar recomendaciones para mitigar los hallazgos encontrados.	Danny Taipe
Aplicación de las recomendaciones	Directivos I. E. "Heraldo Romero Sánchez"
Aplicación de las fase 6 y 7 de la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos.	Por asignar

Fuente: Elaboración propia

VI. ANÁLISIS DE RESULTADOS

Posterior a la aplicación de la PIA sobre el sistema de información académico de la institución educativa “Heraldo Romero Sánchez” en las fases de la 1 a la 6 de la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos [31], se puede analizar lo siguiente:

La evaluación de impacto en la protección de datos personales de la institución educativa “Heraldo Romero Sánchez” arroja como resultado general que la entidad presenta vulnerabilidades en aspectos de seguridad de la información, por ello los hallazgos apuntan a un riesgo intermedio en los datos de estudiantes, maestros y personal directivo.

Se lograron identificar exactamente 15 riesgos con un nivel de impacto medio a alto, lo que quiere decir de qué se deben tomar medidas en aspectos de seguridad de la información. Estos riesgos fueron enviados a las directivas de la institución para que desde la parte administrativa de la misma tomen las medidas correspondientes.

Como principales medidas, la institución debe tomar en cuenta para minimizar el riesgo en aspectos de seguridad de la información aspectos claves como apropiarse del conocimiento de la importancia de la privacidad de la información conociendo la información que se procesó mediante la herramienta de software de la institución, generar medidas de un resguardo seguro de dicho activo por medio de protocolos que garanticen la custodia de la información personal de estudiantes, docentes y administrativos, informar los protocolos de privacidad de la información personal mediante campañas de socialización de las medidas preventivas de la institución y generar una política de seguridad de la información basada en las recomendaciones que se generan a partir de la aplicación de esta PIA.

La institución educativa no cuenta con protocolos de seguridad de la información que permitan garantizar una adecuada protección de la privacidad de la información de los estudiantes, docentes y administrativos, sin embargo, se evidencia la voluntad de conocer las recomendaciones para mejorar la vulnerabilidad en este aspecto que tiene la institución.

La mayor cantidad de hallazgos se encuentran sobre el nivel de impacto medio y alto como se evidencia en la Tabla 3, mostrando la situación actual detallada de la institución en términos de seguridad de la información, lo anterior muestra que se deben tomar medidas para que dicho impacto no cause problemas en la información de los usuarios y miembros de la institución.

La probabilidad de que se materialicen los riesgos es en promedio del 63% lo cual muestra que tienen un nivel intermedio, por ello, se deben tomar medidas de manera prioritaria para no incrementar el riesgo y que dicha probabilidad aumente.

La obtención de la información se realizó en campo lo cual permite tener una información más completa al no tener intermediarios que interfieran involuntariamente los hallazgos encontrados, igualmente, el uso de la herramienta permitió extraer la información relevante en la que se evidencia un tratamiento de la información.

No fue posible conocer el estado de nivel de seguridad de las contraseñas de acceso de los usuarios del sistema puesto que esta es información confidencial y el sistema no cuenta con un mecanismo que obligue a los usuarios a que ingresen contraseñas seguras.

La aplicación de la PIA permite a la institución educativa “Heraldo Romero Sánchez” mejorar la protección de los datos personales al encontrar una evaluación de vulnerabilidades, unas recomendaciones, un análisis y un informe final para tomar medidas prioritarias.

VII. CONCLUSIONES

A partir del proceso de investigación realizado se pueden concluir los siguientes puntos:

- Se mejoró la protección de los datos personales de la institución educativa "Heraldo Romero Sánchez" al recomendar medidas a tomar y de esa manera reducir posibles riesgos y el impacto que podrían llegar a generar.

- El sistema de información de la institución educativa "Heraldo Romero Sánchez" corresponde a una herramienta de software privativa de uso comercial que permite gestionar la información académica de instituciones, el informe generado en este proyecto se compartió al proveedor de este servicio como recomendación para que tome medidas a futuro en su producto de software.

- Es posible aplicar una PIA para la evaluación de impacto en la privacidad de los datos personales de una organización a partir de la información que utilizan los sistemas de información, es importante aclarar que dicha información debe estar disponible de manera completa ante el equipo evaluador para que los resultados sean más veraces.

- La institución educativa "Heraldo Romero Sánchez" no contaba con un protocolo de privacidad de datos personales de los estudiantes, docentes y personal administrativo.

- Se generó un informe a partir de la aplicación de la PIA, el cual sirve como insumo para otras instituciones educativas y de esta manera se propone a la comunidad este conocimiento generado en la mitigación de riesgos en aspectos de seguridad de la información.

- Para la aplicación de una PIA es fundamental la voluntad de la organización en donde se aplicará dicho proceso, pues los resultados serán más acordes a la realidad.

- La aplicación de la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos, es apropiada para este tipo de organizaciones como lo son las instituciones educativas, al igual que para analizar sistemas de información ya desarrollados por terceros.

- La aplicación de la PIA y las recomendaciones que se realizan en este documento permitirán a la institución reducir los riesgos en aspectos de seguridad.

- Se concluye que es fundamental que las organizaciones tengan en cuenta en los procesos de compra e implementación de software el tema de seguridad y privacidad de la información pues es un aspecto relevante dentro de las organizaciones, mediante protocolos de seguridad de la herramienta y que estén disponibles a los usuarios finales. Lo anterior independiente si el proveedor de los servicios tecnológicos sea de carácter público o privado.

Como trabajo futuro a este proyecto de investigación, se recomiendan los siguientes puntos:

- Continuar con las fases 6 y 7 de la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos, usada para aplicar la PIA en la institución educativa "Heraldo Romero Sánchez" para analizar la medición de impacto en las medidas tomadas por los directivos.

- Sistematizar el proceso de aplicación de la norma para agilizar y obtener los resultados de manera ágil.

- Aplicar una PIA mediante la Guía para una evaluación de impacto en la protección de datos personales de la Agencia Española de Protección de Datos, en sistemas de información más complejos o de organizaciones más grandes para verificar su efectividad.

REFERENCIAS

[1] Agencia Española de Protección de Datos. “Guía para una evaluación de impacto en la protección de datos personales”. s.l: s.n., 2014.

[2] Universidad Distrital. “Revistas Universidad Distrital”. 2015. [Online]. Available: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/10518/11605

[3] Policía Nacional. “Observatorio del Delito”. 2019. [Online]. Available: https://caivirtual.policia.gov.co/#observatorio

[4] Policía Nacional. “Observatorio del Delito”. 2019. [Online]. Available: https://caivirtual.policia.gov.co/#observatorio

[5] A. Borealos. “Ciberataque o ataque informático”. 2018. [Online]. Available: https://borealos.com/post/ciberataque-o-ataque-informatico.html

[6] T. Consulting. “TyA Consulting”. 2019. [Online]. Available: https://www.tya-consulting.com/proteccion-de-datos-personales?gclid=EAIaIQobChMI3q_h9KPG6gIVmYrICh0WIQoZEAAYASAAEgKyiPD_BwE

[7] Data Protected. “Protección de datos personales para Colegios”. 2018. [Online]. Available: https://dataprotected.com.co/blog-proteccion-de-datos/noticias/proteccion-de-datos-personales-para-colegios-en-colombia/

[8] L. Sud. “Logística SUD”. 2015. [Online]. Available: http://www.logisticasud.enfasis.com/articulos/73074-las-vulnerabilidades-las-empresas-la-era-digital

[9] KPMG. “Tendencias”. 2018. [Online]. Available: https://www.tendencias.kpmg.es/2018/01/la-importancia-de-los-privacy-impact-assessment-pia-en-la-proteccion-de-datos/

[10] G. Sánchez & I. Rojas. “Leyes de protección de datos en el mundo”. S.l: s.n., 2017.

[11] G. Sánchez & I. Rojas. “Leyes de protección de datos en el mundo”. S.l: s.n., 2017.

[12] Corte Constitucional. “Sentencia T114/18”. 2018. [Online]. Available: https://www.corteconstitucional.gov.co/relatoria/2018/t-114-18.htm

[13] Intedya. “Intedya”. 2018. [Online]. Available: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html

[14] IT. Perito. “ISO/IEC 15408”. 2012. [Online]. Available: https://peritoit.com/2012/07/23/norma-isoiec-15408-common-criteria/

[15] IT. Perito. “ISO/IEC 15408”. 2012. [Online]. Available: https://peritoit.com/2012/07/23/norma-isoiec-15408-common-criteria/

[16] Agencia Española de Protección de Datos. “Guía para una evaluación de impacto en la protección de datos personales”. s.l: s.n., 2014.

[17] KPMG. “Tendencias”. 2018. [Online]. Available: https://www.tendencias.kpmg.es/2018/01/la-importancia

[18] General Data Protection. “GDPR”. 2016. [Online]. Available: https://gdpr-info.eu/issues/privacy-impact-assessment/

[19] Trans Union. “TransUnion”. 2017. [Online]. Available: https://www.iovation.com/topics/privacy-impact-assessment

[20] PrevenSystem. “PrevenSystem”. 2018. [Online]. Available: https://www.prevensystem.com/internacional/803/noticia-evaluacin-de-impacto-de-datos-

personales.html
[21] TechnologyinControl. “TechnologyinControl”. 2015. [Online]. Available: https://technologyincontrol2.wordpress.com/2015/07/27/evaluacion-de-impacto-en-la-privacidad/
[22] Agencia Española de Protección de Datos. “Guía para una evaluación de impacto en la protección de datos personales”. s.l: s.n., 2014.
[23] Agencia Española de Protección de Datos. “Guía para una evaluación de impacto en la protección de datos personales”. s.l: s.n., 2014.
[24] Agencia Española de Protección de Datos. “Guía para una evaluación de impacto en la protección de datos personales”. s.l: s.n., 2014.
[25] Policia Nacional. “Observatorio del Delito”. 2019. [Online]. Available: https://caivirtual.policia.gov.co/#observatorio
[26] Alcaldía de Pasto. “Plan de tratamiento de riesgos de seguridad y privacidad de la información”. 2018. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiQ7uOGh8jqAhXnRt8KHWXpCIEQFjAAegQIARAB&url=https%3A%2F%2Fconcejodepasto.gov.co%2Fwp-content%2Fuploads%2F2018%2F11%2F11-Plan-Riesgos-Seguridad-y-Privacidad-de-la-infor
[27] T. Hechavarría. “Material de apoyo al taller de diseño de proyectos de investigación”. España; La Habana, 2006.
[28] Gobierno de Colombia. “Decreto Número 1317”. Bogotá: s.n., 2013.
[29] Senado de la República. “Ley 1273” de 2009. Bogotá: s.n., 2009. [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[30] Senado de la República. “Ley 1273” de 2009. Bogotá: s.n., 2009. [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[31] Agencia Española de Protección de Datos. “Guía para una evaluación de impacto en la protección de datos personales”. s.l: s.n., 2014.