**Identificación de los riesgos asociados con el manejo de información del área de nómina de APRENDEX**

Autor 1, Andrea Jazmin Torres Vargas Autor 2, Carlos Hernán Romero Autor 3, Fabián Daniel Vargas Cruz Autor 4, Iván Andrés Ortega Díaz autor 5, Joset Milber Olaya Escobar

Especialización seguridad informática, Fundación Universitaria Compensar

Proyecto fin de grado

Tutor

Jaime Andrés Chaparro Sánchez

31 de mayo de 2024



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

# Identificación de los riesgos asociados con el manejo de información del área de nómina de APRENDEX.

**Andrea Jazmin Torres Vargas**
**Carlos Hernán Romero**
**Fabián Daniel Vargas Cruz**
**Iván Andrés Ortega Díaz**
**Joset Milber Olaya Escobar**

Trabajo de grado presentado como requisito parcial para optar al título de:

**Especialista en seguridad informática**

Director (a):
Ingeniero(a), Jaime Andrés Chaparro Sánchez

Línea de Investigación:

Descriptiva - Consultoría Seminario Grado

Fundación Universitaria Compensar
Facultad de Ingeniería, Especialización en Seguridad Informática
Bogotá, Colombia

2024

# Resumen

Este trabajo de grado está orientado en el análisis y gestión de riesgos asociados al uso de información confidencial del área de nómina en una empresa del sector educativo, la cual adoptará el nombre encubierto de Aprendex.

Se identificaron vulnerabilidades en los procesos y sistemas de gestión de nómina de "Aprendex". Basándose en las normas ISO 31000 y 27001, se evaluaron los riesgos potenciales y se propusieron medidas preventivas para garantizar la seguridad de la información.

El análisis reveló vulnerabilidades como la falta de controles de acceso, prácticas inadecuadas de almacenamiento de datos, carencia de capacitación en seguridad de la información, ausencia de un plan de respuesta a incidentes gestión de riesgos. Estas vulnerabilidades podrían exponer la información confidencial. Por ello, se enfatiza la importancia de la gestión de riesgos para proteger esta información.

**NOTA:** La utilización de un nombre apócrifo como "Aprendex" se adopta con el propósito de salvaguardar la privacidad y confidencialidad de la empresa real que se aborda en el proyecto de grado. Este enfoque asegura que el análisis y las recomendaciones se centren en aspectos académicos y preventivos sin exponer detalles sensibles o comprometer la seguridad de la entidad involucrada.

**Palabras clave: (vulnerabilidades, confidencialidad, riegos, controles, gestión, prevención, legislación).**

# Abstract

This degree work is focused on the analysis and management of risks associated with the use of confidential information from the payroll area in a company in the educational sector, which will adopt the covert name of Aprendex.

Vulnerabilities were identified in the payroll management processes and systems of "Aprendex". Based on ISO 31000 and 27001 standards, potential risks were evaluated, and preventive measures were proposed to ensure information security.

The analysis revealed vulnerabilities such as lack of access controls, inadequate data storage practices, lack of information security training, absence of a risk management incident response plan. These vulnerabilities expose sensitive information. Therefore, the importance of risk management to protect this information is emphasized.

NOTE: The use of an apocryphal name such as "Aprendex" is adopted with the purpose of preserving the privacy and confidentiality of the real company that is addressed in the degree project. This approach ensures that the analysis and recommendations focus on academic and preventive aspects without exposing sensitive details or compromising the security of the entity involved.

**Keywords: (vulnerabilities, confidentiality, risks, controls, management, prevention, legislation).**

# Contenido

PÁG.

**RESUMEN** ..... **V**

**INTRODUCCIÓN** ..... **11**

ANTECEDENTES Y JUSTIFICACIÓN ..... 12
FORMULACIÓN DEL PROBLEMA ..... 13
OBJETIVO GENERAL ..... 13
*Objetivos Específicos* ..... *13*
ALCANCES Y LIMITACIONES ..... 13

**MARCO TEÓRICO** ..... **15**

1. BASES TEÓRICAS ..... 15
2. ESTUDIOS PREVIOS ..... 15
3. APORTES Y DIFERENCIACIÓN: ..... 16
*3.1 Novedad:* ..... *16*
*3.2 Valor diferencial:* ..... *16*

**DISEÑO METODOLÓGICO** ..... **17**

DESCRIPCIÓN ..... 17
*FASE 1 Fase de Análisis, Evaluación de Procesos y Sistemas Actuales* ..... *17*
*FASE 2 Identificación de riesgos* ..... *17*
*FASE 3 Evaluación del riesgo* ..... *17*
*FASE 4 Tratamiento del Riesgo* ..... *18*
*FASE 5 Documentación y entrega de resultados* ..... *18*

**RESULTADOS** ..... **19**

**CONCLUSIONES Y RECOMENDACIONES** ..... **21**

1.1 CONCLUSIONES ..... 21
1.2 RECOMENDACIONES ..... 22

**BIBLIOGRAFÍA** ..... **25**

# Introducción

En el actual entorno empresarial, la gestión efectiva de la información es crucial para asegurar la continuidad y el éxito de las organizaciones. En este contexto, la nómina de los empleados destaca como uno de los conjuntos de datos más críticos al contener información personal y financiera sensible. El manejo adecuado de esta información es esencial tanto para proteger la privacidad y seguridad de los empleados como para cumplir con las regulaciones y leyes de protección de datos.

Aprendex, especializada en formación profesional y técnica, administra extensos datos de nómina de sus empleados. La eventual exposición de esta información sensible podría tener consecuencias significativas, afectando tanto a los empleados como a la reputación, operaciones y situación financiera de la institución. Abordar proactivamente la seguridad de esta información es esencial para prevenir riesgos potenciales y proteger los intereses de todas las partes involucradas.

Con el propósito de alcanzar este objetivo, se propondrá a Aprendex medidas preventivas como controles de acceso, tecnologías de encriptación y formación continua del personal en seguridad de la información, entre otras estrategias. Las acciones se respaldarán con metodologías de investigación cualitativa y cuantitativa, asegurando resultados precisos y confiables. Este enfoque proactivo no solo asegurará una protección inmediata de la información, sino también la capacidad de adaptarse a desafíos futuros en el ámbito de la ciberseguridad.

# Antecedentes y justificación

Aprendex es una entidad pública de educación que proporciona formación gratuita a través de programas técnicos, tecnológicos y complementarios. Actualmente, tiene 80 sedes distribuidas en varios departamentos del país.

El recurso humano necesario para la operación de la entidad está conformado por más de 20000 colaboradores, distribuidos entre contratistas, funcionarios y docentes, entre otros.

Desde el área de nómina, se gestiona la totalidad de la información del personal, manejando datos sensibles como salario, días de pago, cuenta bancaria, teléfono, documentos de identificación, préstamos de convenios, entre otros. Dada la naturaleza de esta información es crucial identificar los riesgos asociados a la pérdida o posible fuga de datos y comprender el impacto potencial en términos reputacionales, financieros y operativos para la entidad.

Durante el primer trimestre del año 2024, se evidenció que solo el 10% de los colaboradores del área de nómina dispone de una herramienta que facilita la identificación de la transferencia de datos clasificados como confidenciales. Es importante señalar que, para llevar a cabo dicha transferencia, se requiere contar con la aprobación de tratamientos de datos según lo estipulado en la Ley 1581 de Protección de Datos Personales.

En los datos registrados de la herramienta del 9 de febrero al 9 de marzo del 2024, se pueden observar transacciones de 109.002.644 documentos con datos financieros.

**Ilustración 1 Eventos relacionados con documentos financieros**




Fuente: Tomado de DLP Microsoft

Por lo tanto, este proyecto de grado busca abordar esta problemática mediante el análisis y la prevención de los riesgos asociados con el manejo de la información de nómina en Aprendex. Al identificar y mitigar estos riesgos, se busca proteger la privacidad y seguridad de los datos de manera efectiva y contribuir al fortalecimiento de las prácticas de seguridad de la información.

# Formulación del Problema

La necesidad de gestionar de manera correcta los datos sensibles de los empleados de Aprendex, asegurando la confidencialidad, integridad y disponibilidad de la información de nómina, constituye el origen de este problema. La identificación y prevención efectiva de los riesgos asociados con la gestión de esta información son esenciales para prevenir posibles filtraciones que podrían comprometer la seguridad y la reputación de la institución.

A raíz de lo anterior, surge la siguiente pregunta problemática: ¿Cuáles son los riesgos vinculados al manejo de la información de nómina en APRENDEX, y de qué manera pueden ser prevenidos para evitar la fuga de datos confidenciales?

# Objetivo General

Identificar los riesgos asociados con el manejo de la información de nómina en Aprendex mediante un proceso integral que incluya la evaluación y la propuesta de estrategias de mitigación.

## Objetivos Específicos

1. Analizar los procesos de manejo de información de nómina en Aprendex.
2. Identificar los riesgos asociados con el manejo de esta información.
3. Sugerir medidas preventivas y correctivas para reducir los riesgos identificados.

# Alcances y Limitaciones

El proyecto tiene como objetivo realizar un análisis detallado del manejo de información en el área de nómina de Aprendex. Este análisis abarcará la identificación y categorización de riesgos potenciales asociados, involucrando una revisión detallada de los procesos de recolección, procesamiento y almacenamiento de datos de nómina. Como resultado, se

desarrollarán recomendaciones específicas para mitigar los riesgos identificados, y se ofrecerá orientación sobre las mejores prácticas de gestión de la información. Entre las limitaciones se encuentran la disponibilidad restringida de datos específicos sobre riesgos pasados o actuales en el área de nómina de Aprendex, así como posibles restricciones en el acceso a información confidencial.

# Marco teórico

## 1. Bases teóricas

Gestión de riesgos: Es un proceso continuo que busca identificar, evaluar y controlar los eventos que pueden afectar negativamente a una organización.

Seguridad de la información: Es la práctica de proteger la información confidencial, la integridad y la disponibilidad de los sistemas y datos.

Análisis de riesgos: Es el proceso de identificar y evaluar los riesgos que pueden afectar a la seguridad de la información.

Tratamiento de riesgos: Es la aplicación de medidas para mitigar los riesgos de seguridad de la información.

## 2. Estudios previos

ISO/IEC 27001: Es un estándar internacional que proporciona los requisitos para un sistema de gestión de seguridad de la información.

NIST Cybersecurity Framework: Es un marco de referencia desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos para la gestión de riesgos de seguridad cibernética.

OCTAVE Allegro: Es una metodología para la evaluación de riesgos de seguridad de la información.

# 3. Aportes y diferenciación:

## 3.1 Novedad:

Este estudio se centra en la aplicación de la gestión de riesgos en seguridad de la información en el contexto específico de APRENDEX.

## 3.2 Valor diferencial:

El estudio propone un modelo de gestión de riesgos adaptado a las necesidades de APRENDEX, considerando su tamaño, sector y cultura organizacional.

# Diseño Metodológico

## Descripción

La propuesta definida para llevar a cabo el proceso de Identificación de riesgos de Aprendex y su gestión, está compuesta por cinco fases las cuales se describen a continuación:

### FASE 1 Fase de Análisis, Evaluación de Procesos y Sistemas Actuales

Se realiza una revisión de los sistemas de gestión de nómina de APRENDEX, identificando puntos críticos y vulnerabilidades mediante entrevistas a los colaboradores del área.

### FASE 2 Identificación de riesgos

En esta etapa se hará la Identificación de los riesgos potenciales que podrían afectar los objetivos de la organización. Mediante el análisis de datos históricos y análisis de causa raíz, para identificar los riesgos tanto internos como externos.

### FASE 3 Evaluación del riesgo

Una vez identificados los riesgos, se procede a evaluar su probabilidad de ocurrencia y el impacto potencial en los objetivos de la organización. Esta evaluación se realiza utilizando criterios definidos previamente y puede involucrar el análisis cualitativo y/o cuantitativo de los riesgos.

## FASE 4 Tratamiento del Riesgo

En esta etapa se desarrollan medidas y controles de seguridad que se pueden implementar para mitigar los riesgos identificados, siguiendo buenas prácticas y estándares reconocidos en seguridad de la información.

## FASE 5 Documentación y entrega de resultados

En esta etapa se elabora un informe detallado que muestra el proceso de consultoría, el cual incluye los riesgos identificados medidas preventivas propuestas, entre otros, estos resultados y recomendaciones serán entregados al equipo de dirección general de APENDEX.

# Resultados

Una vez concluidas las fases 1 y 2, Análisis y Evaluación de Procesos y Sistemas Actuales e Identificación de Riesgos, se elaboró una matriz que categorizó 15 riesgos potenciales. De estos, 9 fueron identificados como catastróficos en la etapa 3, en relación con la fuga de información de nómina en Aprendex. La matriz se construyó utilizando la fórmula Riesgo = Probabilidad × Impacto.

Dentro de los riegos identificados se encontraron tecnológicos, gerenciales, operacionales, de cumplimiento y de corrupción. Estos riesgos podrían tener un impacto significativo en la disponibilidad, confidencialidad e integridad de la información de nómina de Aprendex.

Las consecuencias potenciales incluyen:

- Pérdida de datos: La información de nómina podría ser robada, borrada accidentalmente o dañada por un ataque cibernético, un error humano o un desastre natural.
- Fuga de datos: La información de nómina podría ser divulgada a personas no autorizadas, lo que podría generar daños a la reputación de la empresa, demandas legales y sanciones regulatorias.
- Alteración de datos: La información de nómina podría ser modificada de manera fraudulenta, lo que podría conducir a pagos indebidos, fraudes financieros o robo de identidad.

**Ilustración 2 Matriz de riesgos Aprendex**

MATRIZ DE RIESGOS APRENDEX

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DEPENDENCIA: | NÓMINA | | | | | | | | | | | | | |
| VIGENCIA: | 12/12/2024 | | | | | | | | | | | | | |
| | | | | | | | RIESGO INHERENTE | | | RIESGO RESIDUAL | | | | |
| N° | Proceso | Riesgo | Descripción | Tipo de Riesgo | Causas | Efectos | Impacto | Probabilidad | Evaluación del Riesgo | Descripción de los Controles | Evalución del Control | Tipo de control | Valoración del Riesgo | Opcion de Manejo |
| 1 | NÓMINA | Fallas en el software de Nómina (NOMINA) | Software de Nómina no funciona correctamente. | Riesgos de Tecnología: | * Falta de mantenimiento al software de Nómina | * Retrasos en los pagos además, perdida de información. | Mayor | Probable | 16 = Zona de riesgo extrema. Evitar el riesgo. Reducir el riesgo, Compartir o transferir. | Contratación con una entidad encargada de hacer mantenimiento correctivo y preventivo periódicamente al software de nomina además de tener un antivirus en todos los equipos de la administración. | 1- Entre 0-50 | Correctivo | 8 = Zona de riesgo alta. Reducir el riesgo. Evitar el riesgo compartir o transferir. | Reducir el riesgo |
| 2 | NÓMINA | Alta rotación del personal (NOMINA) | Rotación del personal que labora en la subdirección de nomina | Riesgos Gerenciales: | Personal contratado por prestación de servicios por periodos iguales o inferiores 1 año. | Error en la ejecución de los diferentes procesos del área | MAYOR | Probable | 16 = Zona de riesgo extrema. Evitar el riesgo. Reducir el riesgo, Compartir o transferir. | Se tienen cuatro (4) personas Profesionales, tres (3) de carrera administrativa y una (1) de provisionalidad en el área de nomina a fin de dar continuidad a los procesos del área. | 2. Entre 51-75 | Correctivo | 8 = Zona de riesgo alta. Reducir el riesgo. Evitar el riesgo compartir o transferir. | Reducir el riesgo |
| 3 | NÓMINA | Distribucion inadecuada de la informacion ( - ARCHIVO) | Distribucion inadecuada de la informacion a los usuarios internos y externos de la entidad | Riesgos Operativos: | Errores en la clasificación de la documentación , Falta de personal capacitado en la gestión documental | Sanciones e Investigaciones, Retraso en las respuestas a las solicitudes. | Mayor | Posible | 12 = Zona de riesgo extrema. Evitar el riesgo. Reducir el riesgo, Compartir o transferir. | Manual de archivo y programa de formación documental | 2. Entre 51-75 | Preventivo | 8 = Zona de riesgo alta. Reducir el riesgo. Evitar el riesgo compartir o transferir. | Reducir el riesgo |
| 4 | NÓMINA | Deterioro de la documentación (ARCHIVO) | Daño o deterioro de la documentación salvaguardada en los archivos. | Riesgos Operativos: | Disposición física Proceso inadecuado al momento de archivar Humedad Clima | No disponibilidad de la información al momento de requerirse, Perdida definitiva de información | Mayor | Posible | 12 = Zona de riesgo extrema. Evitar el riesgo. Reducir el riesgo, Compartir o transferir. | Custodia y/o tercerización de la documentación | 2. Entre 51-75 | Preventivo | 8 = Zona de riesgo alta. Reducir el riesgo. Evitar el riesgo compartir o transferir. | Reducir el riesgo |

Fuente: Elaboración propia

Se realizó gestión de riesgos (Sugerencias de controles de seguridad a implementar) sobre aquellos que se encuentran categorizados como catastróficos los cuales se definieron como aquellos que podrían tener un impacto significativo en la confidencialidad, integridad o disponibilidad de la información de nómina, lo que podría generar graves consecuencias para la empresa, como el robo de identidad, el fraude financiero y el daño a la reputación.

En respuesta a los riesgos catastróficos identificados, se definieron controles con los cuales el riego residual disminuye quedando entre las categorías mayor y moderado acorde con el mapa de calor definido.

**Ilustración 3 Mapa de calor para gestión de riesgos**

| PROBABILIDAD | | | | | | |
|---|---|---|---|---|---|---|
| | Casi seguro | 5 | 10 | 15 | 20 | 25 |
| | Improbable | 4 | 8 | 12 | 16 | 20 |
| | Posible | 3 | 6 | 9 | 12 | 15 |
| | Probable | 2 | 4 | 6 | 8 | 10 |
| | Rara Vez | 1 | 2 | 3 | 4 | 5 |
| | | Insignificante | Menor | Moderado | Mayor | Catastrófico |
| | | IMPACTO | | | | |

Fuente: Elaboración propia

# Conclusiones y recomendaciones

## 1.1 Conclusiones

Este proyecto de consultoría se enfocó en analizar la seguridad de la información en los sistemas de gestión de nómina de Aprendex. Se identificaron las principales vulnerabilidades, riesgos y amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información de nómina.

- Los sistemas de gestión de nómina presentan controles de acceso deficientes, lo que permite el acceso no autorizado a información confidencial. Esta situación aumenta significativamente el riesgo de filtraciones, robos o uso indebido de datos. Se recomienda implementar controles de acceso más estrictos, como autenticación multifactor, segmentación de redes y control de roles de acceso.
- Los empleados no tienen un conocimiento adecuado sobre las amenazas a la seguridad de la información. Esta falta de conciencia puede ocasionar errores humanos que pongan en peligro los datos de nómina. Se recomienda implementar programas de capacitación en seguridad de la información para concientizar a los empleados sobre las amenazas y buenas prácticas en el manejo de información confidencial.
- Las filtraciones de información de nómina pueden tener graves consecuencias, incluyendo daños a su reputación, interrupciones en sus operaciones y pérdidas financieras. Se recomienda desarrollar un plan de respuesta a incidentes que defina los procedimientos para contener el daño, recuperar la información afectada y notificar a las partes interesadas.
- La entidad no cuenta con un proceso formal para identificar, clasificar y evaluar incidentes de seguridad. Esta situación dificulta la toma de decisiones oportunas para mitigar el impacto de los incidentes y proteger la información de nómina. Se recomienda implementar un proceso de gestión de incidentes que incluya la

evaluación de la gravedad del incidente, su posible impacto en la información de nómina y las acciones necesarias para su contención y recuperación.

## 1.2 Recomendaciones

Dentro de los hallazgos del análisis realizado, se encontraron riesgos asociados a acceso no autorizado, prácticas inadecuadas de almacenamiento de datos, carencia de capacitación en seguridad de la información, ausencia de un plan de respuesta a incidentes y plan de gestión de riesgos, se recomienda implementar las siguientes medidas para prevención de estos:

**Autenticación fuerte:** Implementar mecanismos de autenticación robustos, como contraseñas complejas, autenticación multifactor y biometría, para verificar la identidad de los usuarios antes de otorgar acceso a la información de nómina.

**Autorización basada en roles:** Limitar el acceso a la información de nómina solo a los empleados que la necesitan para realizar sus tareas laborales. Implementar un sistema de autorización basado en roles que defina claramente los permisos de acceso para cada rol dentro de la organización.

**Monitoreo y auditoría de accesos:** Monitorear y auditar regularmente los accesos a la información de nómina para detectar actividades sospechosas o intentos de acceso no autorizados. Implementar herramientas de auditoría que registren los accesos, las acciones realizadas y los datos consultados.

**Encriptación:** Encriptar la información de nómina tanto en reposo como en tránsito para protegerla de accesos no autorizados o divulgación accidental. Utilizar algoritmos de encriptación robustos y claves de seguridad seguras.

**Copias de seguridad regulares:** Realizar copias de seguridad regulares de la información de nómina y almacenarla en ubicaciones seguras y fuera del sitio. Implementar un plan de recuperación ante desastres para garantizar la disponibilidad de la información en caso de incidentes de seguridad.

**Control de acceso físico:** Implementar controles de acceso físico estrictos para proteger los dispositivos y medios de almacenamiento donde se almacena la información de nómina. Restringir el acceso físico a estas áreas solo a personal autorizado.

**Concientización sobre amenazas:** Sensibilizar a los empleados sobre las diferentes amenazas a la seguridad de la información, como phishing, malware, ingeniería social y ataques de denegación de servicio.

**Buenas prácticas de seguridad:** Capacitar a los empleados sobre las mejores prácticas para proteger la información confidencial, como crear contraseñas seguras, evitar compartir información confidencial por correo electrónico o redes sociales, y reportar cualquier actividad sospechosa.

**Manejo responsable de datos:** Educar a los empleados sobre sus responsabilidades en el manejo de la información confidencial, incluyendo las políticas y procedimientos de la empresa para la protección de datos.

**Recuperación y remediación:** Desarrollar un plan de recuperación para restaurar los sistemas afectados, recuperar la información de nómina y remediar las vulnerabilidades que permitieron la ocurrencia del incidente.

# Bibliografía


- Organización Internacional para la Estandarización (ISO). (2018). ISO/IEC 27005:2018 Técnicas de seguridad de la información tecnológica - Gestión de riesgos de seguridad de la información. https://www.iso.org/standard/75281.html
- Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (s.f.). Guía de gestión de riesgos. [PDF] Guía de gestión de riesgos - Min Tic. https://www.mintic.gov.co/gestionti/615/articles5482_G7_Gestion_Riesgos.pdf
- Organización Internacional para la Estandarización (ISO). (2013). ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos. https://www.iso.org/standard/27001
- Instituto Nacional de Estándares y Tecnología (NIST). (2014). Marco de Ciberseguridad. https://www.nist.gov/cyberframework
- Organización Internacional para la Estandarización (ISO). (2018). ISO/IEC 27001:2018 Sistemas de gestión de la seguridad de la información - Requisitos. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:en
- República de Colombia. Congreso de la República. (2012). Ley 1581 de 2012. Ley de Protección de Datos Personales. Bogotá, D.C.: Autor.
- Risk Management, Spanish Articles 14 November 2007 Gomez Meléndez, Mauricio https://www.pmi.org/learning/library/es-gestionando-proyectos-analizando-riesgos-7166