**Estrategia de prevención de vulnerabilidades informáticas en el sistema ERP de la empresa Vosavos SAS**

Diego Ferney Puentes Delgadillo Autor 1, Carlos Andrés Garzón Benavides 2, Juan David Martínez Mican Autor 3, Héctor Julián Garzón González Autor 4 y Daniela José Polanco Gómez

Especialización en Seguridad informática, Fundación Universitaria Compensar

Proyecto fin de grado

Miguel Ricardo Pérez

24 de noviembre de 2023

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

# Estrategia de prevención de vulnerabilidades informáticas en el sistema ERP de la empresa Vosavos SAS

**Diego Ferney Puentes Delgadillo, Carlos Andrés Garzón Benavides, Juan David Martínez Mican, Héctor Julián Garzón González y Daniela José Polanco Gómez**

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

**Especialista en Seguridad Informática**

Director:

Ingeniero Jaime Andrés Chaparro Sánchez

Codirector:

Jairo Cesar Gomez Acero

Línea de Investigación:

Ciberseguridad en sistemas ERP

Grupo de Investigación:

Ingeniería en Telecomunicaciones y Sistemas

Fundación Universitaria Unipanamericana – Compensar

Facultad de Ingeniería, (Especialización en Seguridad Informática)

Bogotá, Colombia

Año 2023

# Resumen

El presente informe se enfoca en la formulación de una estrategia de seguridad informática para el sistema ERP de la empresa VOSAVOS S.A.S., con el propósito de mitigar riesgos asociados a la seguridad de la información; el estudio se llevó a cabo en el entorno del sistema ERP que alberga datos y procesos internos de la compañía., considerando las directrices del Instituto Nacional de Estándares y Tecnología (NIST) así como documentos y estudios mencionados en el presente informe. Se plantean una serie de procesos y procedimientos para la prevención de las vulnerabilidades, que reduzca los riesgos relacionados con la seguridad informática en el sistema ERP.

**Palabras clave: seguridad informática, sistema ERP, vulnerabilidad, NIST**

# Abstract

The present report focuses on the formulation of an information security strategy for the ERP system of the company VOSAVOS S.A.S., with the purpose of mitigating risks associated with information security. The study was carried out in the environment of the ERP system that hosts internal data and processes of the company, considering the guidelines of the National Institute of Standards and Technology (NIST), as well as documents and studies mentioned in this report. A series of processes, procedures, and tools are proposed for the prevention of vulnerabilities that reduce risks related to information security in the ERP system.

**Keywords: information security, ERP system, vulnerability, NIST**

# Contenido

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

**INTRODUCCIÓN** ..... **10**

ANTECEDENTES Y JUSTIFICACIÓN ..... 11
FORMULACIÓN DEL PROBLEMA ..... 11
OBJETIVO GENERAL ..... 12
*Objetivos Específicos* ..... *12*
ALCANCES Y LIMITACIONES ..... 12

**1. MARCO TEÓRICO** ..... **13**

1.1 SISTEMA DE PLANIFICACIÓN DE RECURSOS EMPRESARIALES (ERP) ..... 13
1.2 VULNERABILIDADES INFORMÁTICAS ..... 14
1.3 NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ..... 14

**2. DISEÑO METODOLÓGICO** ..... **15**

**3. RESULTADOS** ..... **21**

**4. CONCLUSIONES Y RECOMENDACIONES** ..... **22**

4.1 CONCLUSIONES ..... 22
4.2 RECOMENDACIONES ..... 22

**BIBLIOGRAFÍA** ..... **23**

# Introducción

Actualmente las compañías se rigen por la creciente importancia de la información y la competencia en entornos comerciales, en la administración de los recursos de manera eficiente y en la toma de decisiones informadas y acertadas, pilares decisivos para el logro de metas y éxitos en cualquier empresa o entidad, en este contexto, los Sistemas de Planificación de Recursos Empresariales, conocidos como ERP (Enterprise Resource Planning), han surgido como herramientas esenciales para las empresas, representan un conjunto completo de aplicaciones y tecnologías diseñadas específicamente para gestionar y optimizar los procesos de negocio en una organización. Estos sistemas permiten la integración de una amplia gama de funciones, que abarcan desde la gestión financiera y contable hasta la logística, la administración de recursos humanos y la cadena de suministro. (oracle, 2023).

En el mundo empresarial actual, la seguridad de los sistemas ERP se presenta como un tema crítico, según Shawn Windle, fundador y principal gerente de ERP Advisors Group, destaca las principales prácticas en seguridad de los sistemas ERP y la necesidad de salvaguardar activos empresariales valiosos, una buena cultura de seguridad se rige como un factor central, la cual no debe ser simplemente una preocupación del departamento de TI, sino una parte esencial de la filosofía de toda la organización, además, se insiste en que la formación en seguridad informática es crucial (larepublica, 2022).

A lo largo del presente documento se abordarán definiciones correspondientes a tipos de ataques de Ransomware que afectan a las empresas especialmente aquellas donde se alojan los sistemas de información ERP en la nube (erpadvisorsgroup, 2023 ), es por ello que se enfatiza la importancia de la ciberseguridad como prioridad clave para proteger activos y asegurar la continuidad operativa bajo una estrategia que siga las directrices del NIST (National Institute of Standards and Technology) para reducir los riesgos en la seguridad informática del sistema ERP de la empresa Vosavos SAS.

# Antecedentes y Justificación

La empresa Vosavos SAS ha experimentado un crecimiento constante en su operación desde el año 2015, respaldado por la implementación de un sistema ERP (Enterprise Resource Planning). El sistema es vital para la gestión y decisiones estratégicas, pero la seguridad informática es una preocupación crítica en el entorno empresarial debido al incremento de amenazas cibernéticas y la sensibilidad de los datos lo hace un objetivo atractivo para ciberdelincuentes.

De acuerdo con el artículo publicado por la compañía SAP (SAP, s.f.), los expertos en seguridad informática detectan que en diversas ocasiones los individuos con intenciones maliciosas se apropian de información variada por diversas motivaciones, enfocan sus esfuerzos en la obtención de datos corporativos, entre ellos los que se encuentran alojados en un sistema ERP, ya que pueden aprovecharlos de diferentes maneras, como extorsión a la empresa afectada o perjudicando a sus clientes en la información sustraída y buscando acceder a los recursos financieros.

Es importante destacar que los ciberataques han aumentado en todos los sectores empresariales., según un estudio publicado por (Brooks, 2022), las pymes, es decir pequeñas y medianas empresas son cada vez más objetos de ataques por los ciberdelincuentes, representando el 43% de los ataques, sin embargo, solo el 14% de estas empresas están preparadas para recuperarse de estos incidentes.

# Formulación del Problema

En la era digital, las empresas se enfrentan a desafíos significativos en términos de ciberseguridad, especialmente cuando se trata de la protección de datos sensibles y la confidencialidad de los clientes. Vosavos S.A.S, es una empresa que brinda servicios de aseo, y nació como respuesta a la demanda de servicios de aseo por horas en hogares y empresas, permitiendo a los clientes acceder a servicios profesionales de limpieza.

Gracias al crecimiento de la empresa se ha implementado un software para el sistema de planificación de recursos empresariales (ERP), el cual ha automatizado los procesos de todos sus departamentos permitiendo unificar todas las operaciones en un dominio comercial llamado hogaru.com, el sistema ERP, es crucial para la optimización de los procesos empresariales y el crecimiento sostenible, sin embargo, esta adopción

tecnológica debe ir acompañada de una sólida estrategia de seguridad informática. Los constantes ataques cibernéticos alrededor de los sistemas ERP en los últimos años son una evidencia clara de la creciente amenaza que enfrentan las empresas, especialmente las pequeñas y medianas (MORALES, 2020). Por lo anterior, esta transición digital presenta preocupaciones importantes sobre la seguridad de la información y la exposición a ataques cibernéticos, ya que la empresa Vosavos S.A.S cuenta con más de 900 trabajadoras y miles de servicios mensuales, existe la posibilidad de que el sistema ERP contenga vulnerabilidades de seguridad que puedan ser aprovechadas por actores malintencionados. Por lo anterior surge la siguiente pregunta de investigación, ¿es posible que planteando una estrategia de detención y prevención de vulnerabilidades en el sistema ERP de la empresa Vosavos SAS, se pueda reducir los riesgos relacionados con la seguridad informática de dicho sistema?

# Objetivo General

Plantear una estrategia de detención y prevención de vulnerabilidades que reduzca los riesgos relacionados con la seguridad informática en el sistema ERP (sistema de planificación de recursos empresariales) de la empresa Vosavos SAS.

## Objetivos Específicos

- Identificar la composición de los elementos que conforman actualmente el sistema ERP para la empresa Vosavos SAS
- Determinar las principales vulnerabilidades que se pueden encontrar en los sistemas ERP, según los controles que propone la NIST.
- Plantear una estrategia para la prevención de vulnerabilidades, que reduzca los riesgos relacionados con la seguridad informática en los sistemas ERP en la empresa Vosavos SAS.

# Alcances y Limitaciones

La investigación busca brindar a Vosavos S.A.S una visión clara de las amenazas al sistema ERP y soluciones efectivas, proponiendo procesos y estrategias para asegurar la continuidad operativa y así consigan proteger la información e infraestructura donde

se encuentra alojado el sistema ERP de la empresa, el plan estratégico está diseñando para divisar las principales vulnerabilidades informáticas que pueden existir en el sistema, es importante aclarar, que el entorno digital está en constante cambio y puede que surjan vulnerabilidades que no sean previstas, por lo que estos procedimientos pueden ser una guía mas no una solución.

# 1. Marco teórico

En el contexto actual de la transformación digital y la creciente interconexión de sistemas informáticos, la seguridad de la información se ha convertido en un aspecto crítico para las organizaciones. A medida que las empresas como VOSAVOS S.A.S implementan sistemas ERP para mejorar su eficiencia operativa, se ven en la necesidad de salvaguardar sus activos digitales contra una variedad de amenazas cibernéticas. Ahora bien, ¿Que es un sistema ERP?

## 1.1 Sistema de Planificación de Recursos Empresariales (ERP)

Es un sistema integrado que gestiona procesos empresariales de manera eficiente, al unificar información, facilita decisiones globales para alcanzar objetivos en finanzas, recursos humanos, inventario, compras y ventas en las empresas. (Oltra-Badenes, 2018), (Chang, 2020).

Los sistemas ERP, deben ser capaces de centralizar y administrar la totalidad de los datos y operaciones de una empresa en todos sus departamentos y funciones. Es importante destacar que una aplicación diseñada para gestionar un proceso específico de negocio no puede considerarse un ERP. Según (Greg Leiter, 2023), los beneficios de un sistema ERP basados en la nube son:

1. Reducción del trabajo manual.
2. Escalabilidad
3. Flexibilidad

## 1.2 Vulnerabilidades Informáticas

Estas vulnerabilidades pueden surgir por equivocaciones durante la programación, ajustes inapropiados o la ausencia de actualizaciones de seguridad u otro factor que exponga una brecha en las defensas de seguridad de un sistema tecnológico (Quintero Acevedo, 2022).

Identificar y corregir estas vulnerabilidades es esencial para prevenir ataques cibernéticos y garantizar la integridad de los sistemas y datos. Los sistemas ERP almacenan una amplia gama de datos confidenciales, lo que los convierte en objetivos interesantes para ciberataques, es esencial mantener un cumplimiento constante de las regulaciones y seguir las recomendaciones de los proveedores, de hecho, una de las principales causas de vulnerabilidades en los sistemas ERP radica en su complejidad y la presencia de numerosas aplicaciones personalizadas " (Esparza, 2022).

Los principales ataques que se pueden encontrar en los sistemas ERP pueden ser: ransomware que es un software malicioso que encripta los archivos de una persona y los vuelve inaccesibles, con el objetivo de obtener dinero por parte del atacante. Este tipo de ataque se ha posicionado como una de las amenazas más peligrosas en el mundo de la ciberseguridad (Kubovič, 2021). Otra modalidad de ataque es la suplantación de identidad para obtener información sensible mediante el uso de correos electrónicos o cuentas de acceso. Gran parte de estos ataques tienen éxito al comprometer redes o sistemas informáticos, lo que resulta en perdida económicas y de información. Estos incidentes pueden impactar la reputación de la organización de manera significativa (Ciberseguridad, s.f.)

## 1.3 NIST – National Institute of Standards and Technology

El Instituto Nacional de estándares y tecnología por sus siglas en ingles NIST es una agencia no reguladora que opera bajo el departamento de comercio, donde su principal misión es promover la innovación y la competencia industrial mediante el avance y la

difusión de estándares científicos y tecnológicos. Cuando hablamos de estándares o procedimientos para mejorar la ciberseguridad sobre las tecnologías de la información, podemos decir que dichos estándares o procesos ayudan a las organizaciones a mejorar su gestión de riesgos en cuanto a identificar y comprenden los activos, las vulnerabilidades, la gestión de riesgos y otros factores que afectan a la ciberseguridad, con el objetivo de detectar y proteger los activos para mitigar riesgos de seguridad. (IBM, s.f.)

# 2. Diseño Metodológico

El análisis y comprensión de los componentes clave dentro de un Sistema de Planificación de Recursos Empresariales (ERP) son esenciales para garantizar su eficiencia y seguridad. En este sentido, la identificación de elementos como la configuración, versiones, plataforma de alojamiento y herramientas específicas utilizadas resulta primordial. Este sistema ERP, implementado en la gran mayoría de compañías a nivel global, plantea desafíos de seguridad que deben abordarse según las normas pautadas por las organizaciones internacionales de ciberseguridad, en el que se incluyen controles y recomendaciones para mitigar vulnerabilidades que puedan afectar la integridad, disponibilidad e integridad de los datos que se gestionan a través de los sistemas ERP; de esta manera, se matizan estrategias clave para la prevención de vulnerabilidades, como elementos esenciales en la seguridad de la información empresarial en entornos ERP.

Para identificar los principales componentes del sistema ERP se deben tener en cuenta los siguientes aspectos:

- **Recolección de la configuración:** Determinar los componentes y/o aplicativos en los que se basa la configuración general del sistema.

- **Recolección de versiones:** Determinar las versiones actuales con las que cuentan los componentes y/o aplicativo del sistema.

El sistema ERP de la empresa Vosavos S.A.S, se encuentra alojado bajo el dominio hogaru.com mediante el uso de **Heroku**; una plataforma en la nube que permite implementar, administrar y monitorizar las aplicaciones web y móviles de forma sencilla automatizando muchas de las tareas de infraestructura, adicional tiene funcionalidades con respecto a la seguridad, como la actualización de sistemas operativos y parches de seguridad, su versión actual es la versión de Heroku CLI versión 8.

El framework utilizado en el sistema es **ruby on rails en su última versión** el cual es un entorno de desarrollo web de código abierto que se enfatiza en la productividad sostenible, permitiendo a los desarrolladores escribir código eficiente. Es una potente herramienta para la creación de aplicaciones web con acceso a bases de datos, proporcionando un conjunto de librerías, diseñadas para abordar los desafíos comunes del desarrollo web, por ello su usó en el sistema ERP mencionado de Vosavos SAS, siendo utilizado por plataformas destacadas como X(Twitter), Airbnb, GitHub. (rubyonrails, s.f.)

La base de datos del sistema ERP es **PostgreSQL,** es un sistema de bases de datos relacionales de código abierto y de alto rendimiento que permite crear funciones personalizadas, tipos de datos y operadores para adaptar la base de datos a necesidades específicas, esta base de datos es compatible con varios sistemas operativos entre ellos Linux, Windows y macOS adicional cuenta con características de seguridad como autenticación, autorización, cifrado de datos y se encuentra alojada en **Amazon Web Services (AWS - RDS)**, su versión actual de uso es la 15. (postgresql, s.f.)

Según (Arrieta & Rodriguez) Las recomendaciones del NIST a menudo incluyen pautas detalladas sobre cómo configurar sistemas de manera segura, por lo que se facilita la detección de errores comunes o configuraciones deficientes las cuales podrían ser explotadas por ciberdelincuentes.

La NIST ofrece pautas y controles para identificar y mitigar vulnerabilidades. Algunas de las principales vulnerabilidades que se pueden encontrar en los sistemas ERP según los controles de la NIST, incluyen:

- El control para abordar la vulnerabilidad de Gestión de acceso deficiente corresponde al Control AC-2 y AC3, indica que no se podrían permitir accesos no

autorizados o privilegios excesivos a usuarios internos o externos al igual que el uso de contraseñas débiles.

- El Control SI-2 de vulnerabilidad de gestión de actualizaciones de software, informa que es importante abordar esta debilidad ya que, si no se aplican las actualizaciones de seguridad o parches a tiempo, el sistema podría quedar expuesto a ataques.
- El control correspondiente a la vulnerabilidad de fallas en el cifrado y protección de datos corresponde a SC-13 de la NIST, en el que los datos almacenados por los sistemas ERP deben estar cifrados adecuadamente para protegerlos de accesos no autorizados.
- El control SI-4 para la vulnerabilidad de falta de monitoreo y detección de intrusiones, indica que la ausencia de sistemas de monitoreo y detección de intrusiones puede llevar a que las amenazas pasen desapercibidas.
- El control de la vulnerabilidad configuraciones inseguras corresponde al control CM-6 que muestra que los sistemas ERP mal configurados pueden dejar puertas abiertas para ataques, como configuraciones predeterminadas con permisos.
- El control para la falta de capacitación a usuarios es AT-2 sobre la seguridad en el uso de los sistemas ERP puede llevar a errores humanos que podrían ser aprovechados por atacantes.
- El control SA-9 de la vulnerabilidad de integraciones y terceros, donde dice que pueden surgir a través de las integraciones con otros sistemas o a través de proveedores externos que acceden al sistema ERP.

Estas prácticas de seguridad son fundamentales para proteger los datos y los procesos críticos de la organización, al seguir las directrices de la (NIST, 2022), las organizaciones pueden evaluar su sistema ERP y encontrar vulnerabilidades que pueden pasar desapercibidas en revisiones anteriores.

Para establecer una estrategia de detección y prevención de vulnerabilidades en los sistemas ERP y reducir los riesgos relacionados se deben seguir los siguientes procedimientos clave:

1. **Políticas de Seguridad:** Consiste en normas que se deben implementar en la compañía en este caso específicamente sobre el sistema ERP, algunos de los pasos a seguir para implementar las políticas son los siguientes:

- **Identificación de los recursos que conforman el ERP:** Implica reconocer los diferentes activos que conforman el ERP para determinar una estrategia de que activos requieren una mayor seguridad.
- **Evaluación de riesgos**: Teniendo en cuenta los activos ya identificados anteriormente se debe realizar un análisis de las posibles vulnerabilidades que estos tengan, y las posibles amenazas que puedan comprometer la información que manejan los activos.
- **Definir objetivos de seguridad**: Incluye la confidencialidad, integridad y disponibilidad de la información, además de prevenir accesos no autorizados y proteger contra posibles ataques maliciosos.
- **Lineamientos y procedimientos**: Con la información que se ha levantado se deben implementar procedimientos los cuales ayuden a la seguridad del sistema ERP, hay que tener en cuenta que con estos procedimientos se puede educar a los empleados.

2. **Monitoreo de Seguridad:** Se deben establecer parámetros de monitoreo del sistema ERP, incluyendo disponibilidad del sistema, y generación de alertas de posibles fallos, también se deben programar auditorias periódicas para determinar mejoras a implementar en el sistema, el monitoreo del sistema lo debe realizar el área de tecnología de la compañía.
3. **Pruebas de Penetración:** La evaluación de la eficiencia de las defensas de la organización, abarcando tecnología, procesos y personas, se lleva a cabo mediante la simulación de un ataque, replicando acciones y objetivos de acuerdo con el control CCS20 NIST. Esto se puede implementar a través de métodos como la prueba de caja negra, donde los ataques se ejecutan sin conocimiento de la estructura interna, utilizando únicamente una dirección IP o URL.

   Por otro lado, la prueba de caja blanca implica considerar toda la información disponible, incluyendo diagramas, detalles de hardware, software y sistemas operativos, para lograr una evaluación más objetiva. (Caballero, 2015)
4. **Control de acceso y autenticación:** La autenticación y control de acceso de los usuarios es algo fundamental en la seguridad. La autenticación consiste en verificar la identidad del usuario mediante credenciales como nombre y contraseña, y también puede involucrar métodos más avanzados, como la

autenticación de dos factores. La empresa de consultoría (Axial ERP, 2022), especializada en sistemas ERP, destaca que el Control de Acceso Basado en Roles (RBAC) es un enfoque esencial para gestionar la autorización de usuarios en los sistemas ERP. Al asignar permisos a roles específicos, la administración se vuelve más eficiente, ya que las actualizaciones se aplican a todo el grupo de usuarios asociados con ese rol, facilitando la auditoría y garantizando el cumplimiento de las normas de seguridad.

5. **Protección contra Malware:** Para la protección contra malware se debe implementar soluciones de seguridad que permitan salvaguardar la información de la empresa, para esto se deben mantener los componentes del sistema actualizados. Algunas de las soluciones principales que se pueden implementar para la seguridad del sistema ERP puede ser un antivirus y firewall que en este caso se aplicarían sobre la base de datos alojada en AWS.

# 3.Resultados

Al realizar la estrategia planteada de prevención y detección de vulnerabilidades para el sistema ERP de la empresa Vosavos SAS, se concluye que es posible reducir los riesgos de seguridad informática en base a la información recolectada de los componentes tecnológicos que conforman el sistema ERP de la empresa Vosavos SAS.

Se han identificado y catalogado las vulnerabilidades más críticas en los sistemas ERP, utilizando el marco de referencia proporcionado por NIST como guía. Este proceso permitirá establecer una serie de controles y recomendaciones para abordar y reducir los riesgos asociados con estas vulnerabilidades del sistema ERP de Vosavos SAS. Estas medidas buscan fortalecer la seguridad y proteger la integridad de los datos empresariales, asegurando una respuesta efectiva ante posibles amenazas y desafíos de seguridad.

Se deben aplicar las estrategias sugeridas como lo son políticas de seguridad, implementación de sistemas de monitoreo, además de autenticación de usuarios, y pruebas de penetración al igual que la utilización de tecnologías avanzadas como antivirus y firewall en AWS. La combinación de estrategias no solo resguarda los datos empresariales, sino que también promueve una cultura de conciencia y de capacitación, consolidando la protección del sistema ERP de la empresa Vosavos SAS.

Al realizar la estrategia planteada para prevenir y detectar vulnerabilidades en el sistema ERP de Vosavos SAS, se evidencia la posibilidad de reducir los riesgos de seguridad informática, apoyados en la recolección y análisis de información sobre los componentes tecnológicos inherentes al sistema ERP de la empresa. Estos aspectos no solo permiten identificar los puntos críticos de riesgo, sino que también sienta las bases para una implementación efectiva de medidas proactivas y específicas que salvaguarden de manera continua la integridad y seguridad de los datos que se pueden manejar dentro del sistema ERP de la empresa Vosavos SAS

# 4. Conclusiones y recomendaciones

## 4.1 Conclusiones

- La ejecución de este proyecto permite destacar la importancia de desarrollar una estrategia para identificar y abordar las vulnerabilidades potenciales en los sistemas ERP. Esta estrategia no solo se convierte en un pilar fundamental para la organización, sino que también actúa como un elemento crucial en el mantenimiento y la optimización de los procesos operativos.
- Al reconocer y comprender las vulnerabilidades en los sistemas ERP, se facilita la implementación de medidas preventivas proactivas, fortaleciendo así las infraestructuras empresariales y minimizando el riesgo de posibles interrupciones o fallos en el funcionamiento de los sistemas ERP.
- Es importante saber que la intervención humana es una de las principales causas de que el sistema ERP quede expuesto a vulnerabilidades, por este motivo se deben realizar capacitaciones de ciberseguridad a el personal que maneje el sistema.

## 4.2 Recomendaciones

- Implementar procedimientos para las estrategias que se han descrito en este documento con el fin de mantener un óptimo rendimiento en cuanto a ciberseguridad del Sistema ERP para la empresa Vosavos SAS.
- Capacitar al personal de la compañía en temas de Ciberseguridad en el sistema ERP de la empresa Vosavos SAS ya que es una aplicación crítica la cual debe tener los mejores estándares de seguridad.

- Mantener actualizada la topología del sistema ERP, ya que al estar en constante cambio pueden surgir nuevas formas de sufrir ataques informáticos a estos nuevos sistemas.

# Bibliografía

Arrieta, S., & Rodriguez, R. (s.f.). Propuesta de adaptación del Framework de ciber seguridad de NIST a los sectores que soportan infraestructuras críticas en Colombia: enfoque sobre el sector de las telecomunicaciones. *Tesis de Licenciatura.* Universidad Piloto Colombia, Bogota.

Axial ERP. (Octubre de 2022). *Axial ERP*. Obtenido de Axial ERP: https://axial-erp.co/comprendiendo-la-importancia-de-la-seguridad-en-los-sistemas-erp-en-el-entorno-empresarial-actual/

Brooks, C. (2022). Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. *Forbes*, https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=235f00de6b61.

Caballero, A. (16 de 10 de 2015). Hacking con Kali Linux. En A. E. Quezada, *Hacking con Kali Linux.* Lima. Obtenido de https://www.forbes.com.mx/: https://www.forbes.com.mx/el-secuestro-de-datos-afectara-a-una-empresa-cada-11-segundos-a-partir-de-2021/?__cf_chl_tk=gkeynGSRqSrx9cfo1URh4ozmkzozOdL8pxBcjtzGjsk-1697238782-0-gaNycGzNESU

Chang, Y.-W. (2020). What drives organizations to switch to cloud ERP systems? The impacts of enablers and inhibitors. *Journal of Enterprise Information Management*, 600-626.

*Ciberseguridad*. (s.f.). Obtenido de Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas: https://ciberseguridad.com/amenzas/suplantacion-identidad/

erpadvisorsgroup. (2023 ). *erpadvisorsgroup*. Obtenido de https://www.erpadvisorsgroup.com/: https://www.erpadvisorsgroup.com/blog/erp-security

Esparza, J. M. (02 de Septiembre de 2022). *spiceworks*. Obtenido de spiceworks: https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/ransomware-as-a-service-unravelling-this-ecosystem/

Greg Leiter, D. J. (29 de agosto de 2023). *https://www.oracle.com/*. Obtenido de https://www.oracle.com/mx/erp/what-is-erp/erp-benefits/

IBM. (s.f.). *IBM.com*. Obtenido de https://www.ibm.com/: https://www.ibm.com/mx-es/topics/nist

Imagine Easy Solutions. (09 de 2016). *Normas APA*. Obtenido de http://normasapa.net/

Kubovič, O. (10 de Agosto de 2021). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2021/08/10/ransomware-no-detiene-como-combatir-amenaza/

larepublica. (15 de diciembre de 2022). *larepublica*. Obtenido de https://www.larepublica.co/: https://www.larepublica.co/empresas/los-ciberataques-suman-54-121-casos-en-lo-que-va-del-ano-y-han-crecido-mas-de-20-3509163

Mendeley. (09 de 2016). *Mendeley*. Obtenido de https://www.mendeley.com/

MORALES, F. B. (2020). *IDENTIFICACIÓN DE BARRERAS DE ENTRADA PARA LA IMPLEMENTACIÓN.* Obtenido de https://intellectum.unisabana.edu.co/bitstream/handle/10818/47156/Proyecto%20de%20Grado%20-%20V.F.pdf?sequence=1&isAllowed=y

NIST. (4 de Mayo de 2022). *National Institute of Standards and Technology*. Obtenido de National Institute of Standards and Technology: https://www.nist.gov/

Oltra-Badenes, R. (23 de 11 de 2018). *Metodología para la selección de sistemas ERP para PYMES.* Obtenido de https://3ciencias.com/: https://3ciencias.com/wp-content/uploads/2018/11/ART-1.pdf

oracle. (2023). *https://www.oracle.com/mx/erp/what-is-erp/#link1*. Obtenido de https://www.oracle.com/mx/erp/what-is-erp/#link1: https://www.oracle.com/mx/erp/

postgresql. (s.f.). *postgresql.org*. Obtenido de https://www.postgresql.org/

Quintero Acevedo, N. (2022). *Repositorio Uniandes.* Obtenido de Repositorio Uniandes: https://repositorio.uniandes.edu.co/server/api/core/bitstreams/32ab7069-1a56-4a2a-9dc6-a5207954a1ea/content

Roy Rosenzweig Center for History and New Media. (09 de 2016). *Zotero*. Obtenido de https://www.zotero.org

rubyonrails. (s.f.). *rubyonrails.org*. Obtenido de https://rubyonrails.org/

Sáenz, J. (09 de 09 de 2016). *Wiki Sistemas Digitales*. Obtenido de http://sistdig.wikidot.com

SAP. (s.f.). *SAP*. Obtenido de SAP: https://www.sap.com/latinamerica/insights/erp-security.html

Suárez, R. (2015). Energías renovables, Impacto y Efectividad. *Revista Científica Ingeniería y Desarrollo en Energía*, 48-53.

Thomson Reuters. (09 de 2016). *EndNote*. Obtenido de http://endnote.com/