Seminario de Investigación

Estructuración de un artículo de revisión bibliográfica fase I

# ARTICULO DE REVISIÓN BIBLIOGRAFICA:
# GERENCIA DE LA SEGURIDAD EN LA INFORMACIÓN DE LAS ORGANIZACIONES
# MANAGEMENT OF SECURITY IN THE ORGANIZATIONS' INFORMATION

Actividad Evaluativa Eje 4

Presentado por:

José Luis Londoño Córdoba

Daniel Rodrigo Dorado Gutiérrez

Daniela Giraldo Rendón

Docente:

Nancy Milena Riveros Chávez

Universitaria del Área Andina

Especialización en Alta Gerencia

Grupo 11

2022

**Resumen**

El mundo es un lugar cambiante y evolutivo, el desarrollo que se ha incentivado es tan amplio, que la competitividad está en puntos muy elevados, y el desarrollo tecnológico es tan evidente, que todas las empresas se acoplan a esos nuevos medios digitales para muchas gestiones, como el albergue de información, que basado en esa innovación, es óptimo, integral, completo, disponible todo el tiempo, sin ser susceptible a daños externos como las características del papel, sin embargo, también se hace vulnerable a falencias como violación de la información, las empresas entonces deben invertir en políticas de seguridad en búsqueda de promover la integridad de los datos, evitando ser víctimas de hurto y fraude, protegiendo la información sin alterarla o modificarla. Para ello, el presente documento busca explicar mediante una revisión documental las estrategias de protección de la información empresarial para garantizar su seguridad, hallando que son muchas las metodologías y cada una se aplica a cada caso empresarial, resaltando que cada organización debe implementar las estrategias orientadas a sus objetivos, basado en pilares de confidencialidad, disponibilidad e integridad de la información, demostrando que no es un gasto, es una inversión que permite a la empresa optimizar el proceso de gestión, ya que en caso de ser víctimas de fraude de información, las pérdidas pueden incluso llevar al cierre de la organización, y cuando no, las pérdidas económicas si serán muy altas.

**Palabras Clave:** Empresa, Gerencia, Información, Seguridad, Sistemas.

**Abstract**

The world is a changing and evolving place, the development that has been encouraged is so extensive, that competitiveness is at very high points, and technological development is so evident, that all companies are attached to these new digital media for many procedures. , as the information shelter, which based on that innovation, is optimal, comprehensive, complete, available all the time, without being susceptible to external damage such as the characteristics of the paper, however, it is also vulnerable to shortcomings such as violation of the information, companies must then invest in security policies in search of promoting data integrity, avoiding being victims of theft and fraud, protecting information without altering or modifying it. For this, this document seeks to explain, through a documentary review, the strategies for protecting business information to guarantee its security, finding that there are many methodologies and each one is applied to each business case, highlighting that each organization must implement the strategies oriented to its objectives, based on pillars of confidentiality, availability and integrity of the information, demonstrating that it is not an expense, it is an investment that allows the company to optimize the management process, since in the event of being victims of information fraud, the losses can even lead to the closure of the organization, and when not, the economic losses will be very high.

**Keywords:** Company, Management, Information, Security, Systems.

## Introducción

Las organizaciones se han enfrentado a transformaciones tecnológicas en donde la información que se genera debe estar resguardada y protegida, ya que cualquier daño de este activo puede resultar devastador.

La información, uno de los recursos más relevantes en las organizaciones, cumple con un papel primordial, pues gracias a esta las empresas pueden unificar procesos, conectar áreas de negocio, diseñar estrategias y trazar objetivos. Rodríguez (2022)

En el desarrollo del informe se llevó a cabo diferentes consultas de autores tratando el tema de seguridad en la información que generan las diferentes organizaciones, beneficios, riesgos y oportunidades que dicho recurso representa, con el fin de realizar una identificación de los métodos aplicados desde la gerencia.

**Planteamiento del Problema**

Algunas organizaciones a nivel nacional o mundial manejan una problemática interna, toda vez que el crecimiento y falta de planeación conllevan a que en ocasiones no se cumplan con la política interna o se haga de manera parcial, el manejo, seguridad, privacidad y resguardo de la información de los datos generados, en ocasiones puede ser un problema que adolecen muchas de las organizaciones ya sea por el volumen de los mismos o por falta de personal que se ocupe de esta actividad.

Esta problemática es expuesta por Sánchez H. (2017), donde explica que muchas veces se suele cometer fraude empresarial con la información de la misma en búsqueda de un beneficio externo, resaltando: Bases de datos de clientes, registros de su comportamiento, sus proveedores con precios, beneficios, antigüedad, alternativas, negociaciones, básicamente suficiente información para que otra empresa del mismo sector económico surja con éxito y lleve a la quiebra a la empresa que se está hurtando la información.

En ese sentido, la problemática radica en cuestionar, ¿Cómo proteger los datos e información confidencial de una empresa?, pues en un mundo que se rige por las tecnologías digitalizadas, esto es fundamental, y es una problemática como se ha presentado, puede generar grandes daños empresariales, de acuerdo a ello, se presentan los siguientes objetivos de la investigación.

# Objetivos

## Objetivo General

Analizar los métodos y estrategias que permiten a las organizaciones un manejo eficiente de información, con una sólida privacidad, seguridad y resguardo de la misma.

## Objetivos Específicos

- Identificar casos de perdida de información que se han generado en algunas organizaciones.
- Analizar a nivel general las políticas de resguardo y seguridad de la información de los datos que se generan en las organizaciones.
- Realizar un comparativo a través de una matriz de las diferentes estrategias gerenciales para llevar un debido control de la información de datos generada por las organizaciones.

**Justificación**

La gestión y buen tratamiento de la información de los datos de cualquier organización se debe garantizar con un adecuado protocolo o instrucciones, tener un seguimiento y monitoreo para así llevar un control oportuno, de acuerdo con Moreno Cevallos & Dueñas Holguín, (2018), la información es un recurso estratégico de las organizaciones, es un factor determinante en el éxito de la misma, y una correcta gestión y tratamiento de la misma, garantiza el éxito de la organización, naciendo así el sistema de información, un sistema que influye sobre cómo se analiza, almacena, protege, utiliza y difunde la información de forma planificada en las empresas.

En ese sentido, es certero afirmar administrar de forma objetiva la información de las organizaciones permite alcanzar el éxito, sin embargo, la información es confidencial, únicamente es información libre los datos regulados por la ley, como balances generales, reportes de sostenibilidad, valor comercial y demás, pero las cuestiones internas como los proveedores, los clientes, los hábitos de consumo, las estrategias empresariales, básicamente todo lo demás, debe ser confidencial, pues si esos datos llegan a las manos incorrectas, puede ocasionar incluso el cierre de la compañía (Almanza Cano, 2020).

En ese sentido, en aras de garantizar una continuidad empresarial y permitir un desarrollo eficiente de la empresa, es necesario emplear estrategias objetivas, orientadas al manejo eficiente de información, con una sólida privacidad, seguridad y resguardo de la misma, pues es la forma por excelencia que una empresa puede surgir en su actividad comercial.

**Antecedentes**

Las empresas, vistas desde un panorama general, manejan grandes cantidades de información de diversos tipos (Lundgren & Bergström, 2019), y su seguridad ha sido un tema siempre de conversación, pues demanda acciones para protección de la misma, y aún con la evolución de los sistemas información, es un tema trasciende. Antes de los años de 1960, previo a la revolución digital, las empresas solían almacenar la información de diversos métodos, pero era complejo, porque era mucho, Folios, Carpetas y Disquetes era lo más utilizado (Rodríguez García, Fuentes Cabrera, & Moreno Guerrero, 2020).

Dejar el papel fue un logro grande para las compañías al momento de hablar de información, según Torres & Garzón, (2021) hasta 1960 el papel fue principalmente para realizar actividades como el procesamiento de transacciones, el mantenimiento de registros y la contabilidad, fue un recurso que se usó principalmente para el proceso de datos, era un método por excelencia del almacenaje de información, rústico, poco eficiente, complejo, muy estorboso y espacioso, pero funcional.

A raíz de ello, con el auge de las computadoras, nace el EDP, el cual, se describe como el uso de computadoras para registrar, clasificar, manipular y resumir datos. También se llama procesamiento de información o procesamiento de datos automático, que, posterior al Sistema de Procesamiento de Transacciones (TPS) fue el primer sistema computarizado desarrollado para procesar datos comerciales (Galindo & Riaño, 2019). El TPS estaba principalmente dirigido al personal administrativo de una organización. El TPS inicial utilizaba datos de procesamiento por lotes que se acumularon durante un período y todas las transacciones se procesaron

posteriormente, sin embargo, era una facilidad increíble para almacenar información en una organización.

Todas las organizaciones son libres de manejar sistemas de información a su criterio propio, sin embargo, es recomendable ajustar las estrategias a métodos eficientes, que garanticen la seguridad de la misma, respetando los tres pilares de datos e información.

Aunque todos estos sistemas de información gerencial tienen funcionalidades distintas, hay un elemento en común con todos: La seguridad de la información, se debe considerar que al momento en el que una empresa pierde la información de su cliente los daños son inmensos y la interrupción de la confianza de los clientes y los altos costos de recuperación de los datos son los que más impacto tienen en el negocio, ya que no hay forma de justificar un error de ese calibre (Pava & Amortegui, 2019).

Por ese motivo, las empresas buscan métodos de preservar la información, garantizar su continuidad eficiente de forma que sea posible proteger los datos y no arriesgarse a perderlos, pero con esos métodos, la información está expuesta, todo se maneja en recursos digitales, y como afirma, Galindo & Riaño (2019) la evolución es buena, pero es un arma de doble filo, ya que representa un riesgo para las organizaciones, en este caso, al acceso de la información.

Avalando esta premisa, la investigación Tejena Macías (2018) explica como la información de las organizaciones (desde una perspectiva general) está expuesta a fraude todo el tiempo, pues con la digitalización global, quien no incursione a albergar información en medios electrónicos se limita en muchos factores, pero al hacerlo, está queda susceptible a violentarla, un riesgo que puede ocasionar consecuencias sumamente negativas para la empresa, y aunque Moreno, Morales, & Denis (2021)  explican que las principales causas de pérdidas de información por

fraude son robo de discos duros externos, ataques informáticos, problemas de Software, Virus y errores humanos, no importa la causa, el resultado será igual de negativo.

Es necesario entender que el impacto siempre será negativo, pero nivel varía de acuerdo con el tipo de la información y el volumen de la pérdida, en todo caso, la recuperación de la información es lo que debe primar, y al tomar acciones correctivas frente a este factor, la prevención de los datos será el segundo paso a seguir, pues repetir el ciclo de pérdida de información será un acto sumamente cuestionable, la seguridad de la información será lo importante.

Para comprender el impacto de este factor, se presentan algunos ejemplos de pérdida de información empresarial con su respectivo impacto en la investigación de Ruiz A. (2021):

**Pruebas de Conducción**: En Francia, para el año 2015, una empresa privada autorizada por el gobierno nacional para dar cursos, evaluar y certificar personas para expedir su licencia de conducción fue víctima de fraude de información, más de tres millones de permisos de conducción se perdieron, incluyendo datos personales como nombre, identificación, números telefónicos y demás, el impacto fue muy negativo, tuvo que devolver el dinero de más de 200.000 casos que ya estaban listos para certificar y no había forma de corroborar, además, tuvo que indemnizar muchas personas por la información difundida a entidades fraudulentas que buscaban conocer datos personales.

**JP Morgan Chase:** Una importante empresa financiera de Estados Unidos fue víctima de un hackeo que hurtó información personal de más de 76 millones de personas y 7 millones de pequeñas empresas, un error en el cifrado de seguridad de la información que costo más de 30 millones de dólares a la compañía, lo cual, avala la teoría de que la seguridad de la

información es lo esencial en toda organización, pero es un proceso que por muy riguroso que sea, no deja exento a nadie para ser víctima de este medio.

**Marco Teórico**

La información constituye algún tipo de mensaje, ya que solo conociendo la información ya hay transferencia de datos, por ejemplo, el valor económico que se paga por un servicio, la información es el monto, y el mensaje corresponde a ese dinero para hacer un análisis de costos.

En el caso empresarial, la información es denominada: Información Organizacional o información de las compañías, y es básicamente lo mismo, conjunto de datos relevantes en este caso, para las empresas, sus clientes, competidores y cualquier persona que pueda acceder a la misma (Limón Sánchez & De la Garza Cárdenas, 2018). Entre las posibles ramas de información, existe ciertas que pueda tener una empresa y destacan más que otras, según Terreros (2022), la información de clientes es una de ellas, que constituye a toda la información relacionada con sus clientes y consumidores, resaltando hábitos de consumo, medios de pago, frecuencia de compras, con el fin de analizar la misma y permitir presentar promociones o sugerencias.

Por otro lado, la Información Administrativa también juega un rol de suma relevancia, ya que hace referencia a toda aquella información que involucra la gestión administrativa de la organización, como son procesos internos, métodos de trabajo, requerimiento de personal, entre otros afines. La Información de Transacciones es la información financiera, pero de forma digital, en transacciones digitales con clientes, consumidores, proveedores, socios y cualquier otra parte involucrada en intercambio de dineros, por lo cual, es infaltable en el proceso, irremplazable y de gran importancia a proteger, ya que, de ser víctima de pérdida, los daños serán casi irreparables.

Por otro lado, la información de mercadeo es la información que corresponde a las estrategias de publicidad, promociones, plaza, incursión digital, inversión en publicidad entre todos los criterios que involucran la impulsión de marca o empresa. La información de Ventas y Procesos

es la información que corresponde a todas las ventas producto del proceso productivo de la compañía, es decir, la relación producción – ventas, la utilidad general del mes, los costos operativos, los ingresos por ventas y los costos de producción.

Además, no son los únicos apartados informáticos, la información de Recursos Empresariales alberga la información de los recursos que se cuentan, es decir, que unidades de producto hay en inventario, cuantas se vendieron, que materias primas se cuentan, todo lo relacionado con recursos para la actividad comercial de la compañía y los complementarios. Se destaca también la información Contable y Estratégica, lo cual, es la información de contabilidad general de la compañía desglosada en cada factor, así como las estrategias que se desarrollan con base a esos mimos análisis contables según un periodo de tiempo determinado.

Como se puede notar, la información es muy densa, existen ramas para casi todos los criterios y, de hecho, no hay un estándar, hay empresas con más tipos de información, así como otras que tienen menos, las Pymes en la mayoría de casos, sin embargo, aún si es una empresa pequeña o no, la información por criterio es mucha y nace ahí, el sistema de información (Ruiz F. , 2017).

El uso de sistemas de información para las empresas, o por sus siglas S.I., ha aumentado exponencialmente conforme pasa el tiempo, según Melgarejo & Olarte (2020) implementar esta herramienta permite control, visibilidad, orden, disposición y vinculación de todo ese movimiento tan amplio de datos que tienen todas las empresas, aún las PYMES, cosa que con otros métodos tradicionales no alcanzaría. Sin importar el tamaño o el nivel de operación, siempre será necesario implementar diferentes sistemas de información en las empresas, pues es una herramienta competitiva, de innovación que genera grandes beneficios.

La transformación digital ha contribuido de forma notoria este ámbito, ha permitido contar cada vez con más y mejores programas o plataformas que ayudan a los negocios a ser más eficientes, realizar tareas más rápido, tener procesos óptimos y una mayor visualización de las operaciones (Alvarado, Acosta, & Buonaffina, 2019), sin embargo, se debe primero entender el concepto.

Según Proaño Castro, Orellana, & Martillo Pazmiño (2018) un sistema de información corresponde a un sistema constituido por un conjunto de componentes interrelacionados a través de diversos medios, métodos y tratamientos con el mismo fin: trabajar en unión para recopilar, procesar, almacenar, proteger objetivamente y difundir información para apoyar la toma de decisiones de una compañía, ya que como se mencionó, la información contiene mensajes que permiten desarrollar análisis o criterio sobre alguna situación determinada. Además, los sistemas de información apoyan la coordinación, control, análisis y visualización de una organización de forma objetiva.

El avance tecnológico ha brindado una ventaja competitiva a las empresas mediante el uso de los sistemas de información en las mismas, ya que cada vez son más intuitivos, con mayor capacidad para contener datos, gestionarlos e interpretarlos (Pinzón Riaño & Contreras Mejía, 2019), de hecho, el avance ha sido tan notorio, que diversas plataformas, sistemas y programas digitales se han vuelto imprescindibles dentro de las organizaciones.

Según Vivar Astudillo, Erazo Álvarez, & Narváez Zurita (2019) los sistemas de información generan grandes beneficios competitivos, resaltando la Integración de la Información, ya que permite la integración y centralización de información, lo cual representa una gran ventaja para las empresas, en tanto que permiten una vinculación efectiva entre sus áreas. Así podrán hacer

una mejor planeación y operar como un bloque sólido que permite interactuar de forma eficiente entre departamentos.

El tiempo es otro gran beneficio que genera este medio, ya que los procesos suelen tardar demasiado en enfoques tradicionales al acceder en la información, a raíz de ello, los colaboradores pierden tiempo en esa gestión, que con la integración de un sistema de información es posible que los trabajadores tengan más tiempo de operar en otras actividades.

Los procesos también cambian, ya que en las empresas se ven beneficios económicos con la reducción de costos al implementar un sistema de información, ya que se permitirá optimizar sus procesos, disminuir errores, tener diagnósticos de problemas y ser eficiente integralmente gracias a la concentración de información valiosa. La gestión también es un factor que se involucra y genera grandes cambios a la toda la gestión organizacional, ya que los sistemas son importantes porque brindan un mayor control de procesos, operaciones y actividades, lo cual permite una mejoría constante. Administrar bien los tiempos, recursos y actividades se traduce en ganancias para una empresa.

Otro gran beneficio de esto, es la disponibilidad de los datos, ya que una de las mayores problemáticas antes de implementar Sistemas de Información era la disponibilidad de la misma, tardaba en encontrarse y se esperaba autorización, con los sistemas es posible tener la información disponible y acceso a grandes volúmenes de datos ayuda a la estrategia, planificación y operación efectiva dentro de un negocio.

Los costos también se ven muy beneficios, pues cuando la información se traslada a medios digitales se reducen muchos costos operativos en su gestión, búsqueda, almacenaje, tratamiento y

demás, con esa nueva innovación se optimiza todo el proceso, y el resultado es ahorro en costos administrativos, de recursos humanos y operativos, el ideal de toda compañía es reducir costos.

La seguridad es sin duda alguna el gran beneficio, pues con la evolución de los sistemas de información en las empresas ha llegado a un nivel tal que garantizan la seguridad de los datos, mediante cifrado de los mismos, bloqueos de acceso y demás.

Ahora bien, es necesario resaltar que ese último “beneficios” de los sistemas de información empresarial no es tan bueno como parece, si bien es cierto que a primera medida genera gran valor para la organización al no permitir un acceso sencillo a quien no debería tener acceso de información, en un nivel especializado, puede ser un arma de doble filo (Brunner, Sauerwein, Felderer, & Brew, 2020), ya que la información digital está abierta ante la llave indicada, y esa llave puede ser conseguida por medio de actividades ilícitas, como hackeos, repetición de información, clonación de contraseñas, descifrados de seguridad entre otros.

Según Grishaeva & Borzov (2020) la gestión de riesgo de seguridad de la información en una organización es una actividad fundamental para las empresas, pues es un medio que garantiza el éxito de las empresas, perder la información puede ocasionar perder clientes potenciales, proveedores exclusivos, negocios por cerrar, socios estratégicos, lo cual, se resume todo en pérdidas económicas que afectan a cualquier organización. La gestión de riesgo busca mitigar esa problemática y proteger la información mediante diversas estrategias como doble cifrado de seguridad, claves de acceso personales y no operativas, entre buenas prácticas de trabajo y confidencialidad.

**Resultados**

De acuerdo con la investigación, hay varias hipótesis que se han confirmado, otras se descartan, por ejemplo, los impactos que genera la pérdida y fraude de información al interior de una organización varía de acuerdo a dos factores principales: El volumen de la información perdida y el tipo de información, es decir que no existe una relación de medición ajena a estos dos criterios, y la relación indica que a mayor información quebrantada, el impacto es más negativo, y el nivel de importancia de la misma hará que su resultado sea más cuestionable, en todo caso, la seguridad de esta debe primar, pues la información es el activo más importante de toda empresa (Figueroa Suárez J. , Rodríguez Andrade, Bone Obando, & Saltos Gómez, 2019).

La seguridad prima en todo contexto, hay millones de casos en todo el mundo de importantes empresas que son víctimas de fraude en la información, la seguridad de esta no se trata de un medio negociable, o un gasto irrelevante en la empresa, es una inversión más que necesaria, determinante en el desarrollo de la compañía, por lo cual, implementar medidas y estrategias de seguridad es fundamental, en efecto, se corrobora la hipótesis inicial: Lo más importante para una compañía es proteger su información, ya que de esto depende su éxito.

Más allá de solo perder información, ser víctima de este tipo de fraude para una empresa representa varias falencias: Pérdidas económicas, pérdida de confianza del cliente, consigo la percepción general, por ende el valor accionario y el crecimiento de la compañía, habrá menos clientes por la incertidumbre de saber con quien están albergando la información, y recuperar esos datos robados no es la solución real, recuperar la confianza del cliente es el reto, sanar el daño económico y social hacia la compañía es lo complejo, sin duda alguna, la inversión en

seguridad de la información es lo mejor que una compañía puede hacer, y prevenir este tipo de falencias, permitirá un desarrollo eficiente para la compañía.

La gerencia juega el rol más importante en el desarrollo de la organización, sin embargo, debe estar complementada con varias áreas o departamentos como informática, IT, seguridad interna, fraude organizacional, recursos humanos, para forjar todo un proceso de seguridad de la información basado en las ideologías propuestas, para garantizar la protección de la información, ya que de ser víctimas de fraude sobre esta, los daños son casi irreparables.

**Discusión de Resultados**

Aunque es cierto que no hay una política exacta de cómo debe ser un modelo de protección de datos e información en una empresa, es necesario resaltar que todo debe estar orientado a la integralidad, por lo cual, según Herrera, Casas, & Riaño ( 2021) se hace necesario idear una política con tres pilares infaltables: Confidencialidad, Integridad, y Disponibilidad. Lo cual, se cree es una posición muy acertada, ya que en complemento se cita a Chaverra Mojica, Restrepo Vélez, & Pérez García (2020) donde afirma que la seguridad de la información empresarial debe hacerse de forma estricta, pero sin alterar la información, garantizar la integridad de los datos y la confidencialidad de todo lo que contiene.

Asimismo, se debe pensar en algo más que solo la protección, según Castellanos Claramunt, (2020) aprovechar los recursos digitales es una forma integral de proteger información, mediante el apoyo de la inteligencia artificial y algoritmos cifrados en red, que garantice un difícil acceso a quien no debe, hacia la información, y es una opinión compartida por Cotino Hueso (2020), donde explica que el Big data debe protegerse con cifrados basados en inteligencia artificial, para consolidar un sistema más difícil de quebrantar.

En ese sentido, implementar una política de protección de información se hace importante para todas las empresas, pero además de basarla en los tres pilares de Disponibilidad, Integridad y Confidencialidad, se debe pensar en estrategias de cifrados de la misma. Según Figueroa Suárez J. Rodríguez Andrade, Bone Obando, & Saltos Gómez (2021) una manera de conseguirlo es mediante la implementación de un programa de mejora continua, basado en cuatro etapas principales: Análisis y Evaluación de Riesgos, Acceso a los Datos y Estudio, Proponer e Implementar estrategias, Evaluar estrategias, y luego se repite el ciclo en un periodo de tiempo.

La anterior metodología no es la única, tampoco es la más acertada, ya que es necesario entender que, para todas las compañías, la implementación de programas de seguridad informática será distinta, se debe evaluar a objetivos y funcionalidad empresarial. De acuerdo con Contero Ramos, (2019) otra metodología de protección seguridad de la información global para las empresas que utilizan muchos datos en nube, será la protección parcial y desarrollo en red, donde consiste en subir todos los datos a la nube (con cifrado especial, claves de acceso y demás impedimentos para el difícil acceso), y borrar la información del disco principal, así se consigue que la información esté reunida en un único sitio, donde está disponible, íntegra y menos propensa  fraude.

Finalmente Lewis, Arthur, & Cerma (2021) explica otra metodología muy acertada para el manejo de información, basada en sistema de información separados, la cual, consiste en separar toda la información según su tipo, cada una con un cifrado diferente, y accesos distintos, así, es posible permitir que, si hay fraude en información de clientes, por ejemplo, lo demás esté protegido. La tabla 1 a continuación compara las tres metodologías anteriormente descritas.

**Tabla 1.** Comparativa de Metodologías de Seguridad de la Información Empresarial

| **Seguridad Basada en Mejora Continua** | **Seguridad Basada en Almacén Nube con Borrar disco** | **Seguridad con Separación de Sistemas de Información** |
|---|---|---|
| Permite cada vez más proteger más la información albergada en el Sistema. | Es muy eficiente para proteger información delicada, albergando un solo sitio. | Es sumamente eficiente para las compañías que manejan un volumen de datos muy alto. |
| Se limita a información global, no enfatiza por tipos de información. | Es susceptible a pérdidas globales por limitarse de datos a un único sitio de almacenaje. | Se hace complejo por manejar muchos sistemas, cada uno con información relevante. |
| Es económico de implementar, pero los resultados no son óptimos. | Es promedio de implementar, más costoso que una mejora continua pero más limitado. | Su costo de implementación es muy elevado, muchas empresas no pueden costearlo. |

Autoría propia

**Conclusiones**

La información es un activo de suma importancia en todas las empresas, no existe relevancia alguna entre el tipo de organización o el sector económico en el que se especialice, todas las empresas dependen directamente de la información y su manejo, donde, una mala gestión de protección y seguridad de los datos que alberga, puede actuar como determinante en la continuidad del negocio, ya que perder información puede representar el cierre total de la empresa.

La seguridad de la información es un factor esencial, donde la inversión debe ser generosa en búsqueda de que sea eficiente, ya que, de ser víctima de fraudes en la información o víctimas de hurtos y hackeos de la misma, la empresa tendrá repercusiones muy negativas que superan el valor de la inversión, como pérdida de buena imagen corporativa y buen nombre, pérdida masiva de clientes, y pérdidas económicas muy elevadas.

Las políticas de protección de la información son muy variantes, cada empresa debe implementar un modelo distinto, acoplado de acuerdo a sus objetivos y manejo de la misma, una empresa financiera por ejemplo no manejara el mismo sistema que una empresa de construcción, sin embargo, todas deben acoplarse a un modelo básico, acorde a tres pilares: Disponibilidad, integridad y confidencialidad e la información.

En efecto, la gerencia de las organizaciones será la encargada del éxito de la compañía, pero es necesario un apoyo por parte de seguridad estratégica para un manejo integral de los métodos y estrategias de organización de información, con un manejo que permita cumplir los tres pilares, con una sólida privacidad, seguridad y resguardo de la misma, con integralidad, sin alterar o modificar los datos.

**Bibliografía**

Almanza Cano, M. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000-2018. *Revista Ibérica de Sistemas e Tecnologias de Informação: Volumen 27, número 1, pp. 470-483*, URI: https://www.proquest.com/openview/91b5a2323f58400389c80c48e01aa42d/1?pq-origsite=gscholar&cbl=1006393.

Alvarado, R., Acosta, K., & Buonaffina, Y. (2019). Need for management information systems for decision making in organizations. *InterSedes: Volumen 19, número 39, pp. 47-91*, DOI: http://dx.doi.org/10.15517/isucr.v19i39.34067 .

Arévalo Avecillas, D., Nájera Acuña, S., & Piñero, E. (2018). The Influence of the Implementation of Information Technologies in the Productivity of Service Companies. *Información tecnológica: Volumen 29, número 4, pp. 471-787*, DOI: http://dx.doi.org/10.4067/S0718-07642018000600199 .

Brunner, M., Sauerwein, C., Felderer, M., & Brew, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security: Volumen 92, número 1, pp. 101-176*, DOI: https://doi.org/10.1016/j.cose.2020.101776.

Castellanos Claramunt, J. (2020). Information management in the algorithmic paradigm: artificial intelligence and data protection. *Métodos de Información, volumen 11 número 21, pp. 59-74*, DOI: https://dx.doi.org/10.5557/IIMEI11-N21-059082.

Cepeda Riaño, L., Garzón Linares, A. R., & Pava Rubio, H. S. (2017). Competitividad e Innovación en el Siglo XXI para el Éxito Empresarial. *Engineering and Processing:*

*Process Industries; Volumen 206, número 271, pp. 633-641*, https://doi.org/10.21533/rib.udes.v39n2a03 .

Chaverra Mojica, J., Restrepo Vélez, H., & Pérez García, F. (2020). El teletrabajo y la seguridad de la información empresarial. *Revista Cintex: Volumen 20 Número 4, pp. 111-121*, URI: https://revistas.pascualbravo.edu.co/index.php/cintex/article/view/33 (nueva versión 2020).

Contero Ramos, V. (2019). Design of an information security policy based on ISO 27002: 2013, for the system of a private company. *Repositorio Institucional UniSEK [tesis de Maestría]*, URI: https://repositorio.uisek.edu.ec/handle/123456789/3345.

Cotino Hueso, L. (2020). Artificial intelligence, big data and applications against Covid-19, and privacy and data protection. *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política, Número 31, pp. 332-351*, URI: https://dialnet.unirioja.es/servlet/articulo?codigo=7633148.

Del Canto, E., Mega L., G. A., Guerra R., M., & Capobianco M., J. P. (2018). Nuevas tecnologías y sistemas de información gerencial en la actualidad venezolana. *Ingeniería Industrial. Actualidad y Nuevas Tendencias: Volumen 21, número 21, pp. 111-130*, URI: https://www.redalyc.org/journal/2150/215058535008/215058535008.pdf.

Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, B., & Saltos Gómez, J. (2021). Informatic security and information security. *Polo del Conocimiento: Revista Científico-Académica Multidisciplinaria: Volumen 21, número 86, pp. 431-451*, URI: https://polodelconocimiento.com/ojs/index.php/es/article/view/420.

Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, C., & Saltos Gómez, J. (2019). La seguridad informática y la seguridad de la información. *Polo del Conocimiento: Volumen 25, número 34, pp. 681-695*, DOI: 10.23857/pc.v2i12.420.

Galindo, J., & Riaño, M. (2019). Evolución de los Sistemas de Información: Antecedentes y Desarrollo. *Tecnología e Innovación: Volumen 4, número 1*, pp. 50-62.

Grishaeva, S., & Borzov, V. (2020). Information security risk management. *International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), pp. 96-98*, DOI: 10.1109/ITQMIS51053.2020.9322901.

Herrera, E., Casas, A., & Riaño, L. (2021). What are the pillars of information security? *Docusign México: Information Security*, en línea: docusign.mx/blog/seguridad-de-la-informacion [consultado el 13 de agosto de 2022].

Lewis, F., Arthur, N., & Cerma, L. (2021). Digital Security: Strategies to Protect Important Data in a Customer Management Company through a CRM System. *Journal of Science and Research EFI: Volumen 402, número 77, pp. 1322-1381*, URI: https://dialnet.unirioja.es/servlet/articulo?codigo=3287944.

Limón Sánchez, M. L., & De la Garza Cárdenas, M. H. (2018). Tecnologías de información y desempeño organizacional de las pymes del noreste de México. *Revista Venezolana de Gerencia: Volumen 23, número 82, pp. 298-313*, URI: https://www.redalyc.org/journal/290/29056115004/29056115004.pdf.

Lundgren, M., & Bergström, E. (2019). Security-related stress: A perspective on information security risk management. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, DOI: 10.1109/CyberSecPODS.2019.8884877.

Melgarejo, C., & Olarte, M. (2020). Ventajas de la Implementación de Sistemas de Información. *Procesos Efectivos: Volumen 101, número 1*, pp. 87-106.

Moreno Cevallos, J., & Dueñas Holguín, B. (2018). Sistemas de información empresarial: la información como recurso estratégico. *Dominio de las Ciencias: Volumen 4, número 1, pp. 204-217*, DOI: http://dx.doi.org/10.23857/dc.v4i1.728.

Moreno, M., Morales, J., & Denis, G. (2021). Pérdida de datos para las empresas ¿Cómo solucionarlo? *BE Services: Asesoría en Protección Digital de Datos*, en línea: https://www.beservices.es/perdida-datos-empresas-n-5356-es [consultado el 13 de agosto de 2022].

Pava, H., & Amortegui, S. (2019). Pérdida de Información Empresarial: Causas y Consecuencias. *Industria 4.0 de los Datos: Volumen 12, número 1*, pp. 87-99.

Pinzón Riaño, M., & Contreras Mejía, J. D. (2019). Desarrollo Empresarial: Avance tecnológico y digital para los nuevos métodos de trabajo - Sistemas de Información. *Gerencia y Salud Laboral: Volumen 16, número 5*, pp. 51-63.

Proaño Castro, M., O. C., & Martillo Pazmiño, O. (2018). Information systems and their importance in the digital transformation of the current company. *Revista Científica Espacios: Volumen 39, número 45, pp. 3-15*, URI: http://es.revistaespacios.com/a18v39n45/18394503.html.

Rodríguez García, A. M., Fuentes Cabrera, A., & Moreno Guerrero, A. J. (2020). Competencia digital docente para la búsqueda, selección, evaluación y almacenamiento de la información. *Revista Interuniversitaria de Formación del Profesorado [tesis de pregrado de la Universidad de Granada]*, URI: http://hdl.handle.net/10481/59955.

Rojas Amado, J., & Escobar Ávila, M. (2021). Benefits of Using Digital Technologies in External Auditing: a Literature Review. *Revista Facultad de Ciencias Económicas: Investigación y Reflexión: Volumen 29, Número 2, pp. 106-132*, DOI: https://doi.org/10.18359/rfce.5170 .

Ruiz, A. (2021). Los casos más graves de pérdida de información. *Data Recovery Serman: México*, en línea: https://serman.com/blog-recuperacion-datos/los-casos-mas-graves-de-perdida-de-informacion/ [consultado el 13 de agosto de 2022].

Ruiz, F. (2017). Sistemas de Información Gerencial: Introducción y Generalidades. *Innovar: Volumen 41, número 18, pp. 71-94*, URI: http://www.scielo.org.co/sci0121-50512018000300099.

Sánchez, F. (2019). ¿Por qué es importante la información y su correcto almacenamiento para las empresas? *Innovación Europea: Volumen 3, número 1, pp. 12-23*, URI: https://www.redalyc.org/pdf/342/418346009.pdf.

Sánchez, H. (2017). El fraude en la información empresarial en el marco de las relaciones financieras. *Revista de Fomento Social, Volumen 276, número 1, pp. 247-281*, DOI: https://doi.org/10.32418/rfs.2014.276.1595.

Tejena Macías, M. (2018). Análisis de riesgos en seguridad de la información. *Polo de Conocimiento: Volumen 17, número 84, pp.541-566*, URI: https://polodelconocimiento.com/ojs/index.php/es/article/view/809.

Terreros, D. (2022). Sistemas de Información Empresarial: Tipos de información para un gestión eficiente organizacional. *Marketing Exitoso: Volumen 1, número, 1, pp. 1-22*, URI: https://blog.hubspot.es/marketing/sistemas-de-informacion-empresas.

Torres, G., & Garzón, M. (2021). Evolución de los Sistemas de Información: Tecnologías de Información. *Tecnologías de Información: Edición 4 recurso web*, en línea: https://www.tecnologias-informacion.com/evolucionsistemas.html [consultado el 31 de julio de 2022].

Vivar Astudillo, A., Erazo Álvarez, J., & Narváez Zurita, C. (2019). Management and Treatment of Information: Competitive Advantages. *CompartirIgual 4.0 Internacional: Volumen 204, número 161, pp. 1287-1291*, DOI: https://doi.org/10.35381/r.k.v6i10.686l/.