



**UNCUYO**  
UNIVERSIDAD  
NACIONAL DE CUYO



FACULTAD DE  
**CIENCIAS  
ECONÓMICAS**

Contador Público Nacional y Perito Partidor

## Trabajo de Investigación

# LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LAS EMPRESAS DE MENDOZA

Alumnos

BARNABÓ, Ignacio Javier, REG. 23666

HERRERA, Gonzalo Martín, reg. 28642

LUQUEZ JOFRE, Agustín Javier, reg. 29326

**Director: Majowka Pablo David**

**Mendoza, 2023**



## RESUMEN TÉCNICO

La información constituye el principal activo de una empresa, es su centro de poder porque se trata de todo lo referente al accionar y funcionamiento de la misma. En la actualidad es fundamental proteger los datos de una organización que circulan cotidianamente en las redes informáticas dado que la fuga de información puede repercutir gravemente y hasta destruir una empresa.

Este proyecto de investigación tiene como objetivo principal indagar los ciberataques, las fallas intrínsecas que permiten la comisión de delitos informáticos a fin de gestionar una adecuada seguridad informática en pymes y organizaciones. Específicamente se pretende descubrir los ataques cibernéticos, gestionar los riesgos y proponer acciones que los mitiguen.

Metodológicamente el presente estudio se trata de una investigación cuantitativa de carácter explicativa, micro social y transversal. Los datos serán recolectados mediante encuestas aplicadas a 15 Pymes y 15 organizaciones de la provincia de Mendoza, en los meses de enero a abril de 2023.

De los resultados extraídos se descubrió que las empresas mendocinas no poseen un departamento de Seguridad Informática y que existe un alto porcentaje de ataques cibernéticos que afectan la administración, los mails y la calificación de los clientes. Lo cual muestra la necesidad de centrar atención al mantenimiento de las computadoras y apuntar a una cultura organizacional sobre seguridad informática.

**Palabras claves:** Sistema de información, seguridad informática, gestión, Pymes y organizaciones.



## ÍNDICE

<b>INTRODUCCIÓN .....</b>	<b>7</b>
<b>CAPÍTULO I</b>	
<b>INFORMÁTICA EN PYMES Y ORGANIZACIONES .....</b>	<b>10</b>
<b>SISTEMAS DE INFORMACIÓN Y SEGURIDAD.....</b>	<b>10</b>
<b>1. PYMES Y ORGANIZACIONES .....</b>	<b>11</b>
<b>1.1 Concepto de pymes.....</b>	<b>11</b>
<b>1.2 Ventajas de las pymes.....</b>	<b>11</b>
<b>1.3 Desventajas de las pymes.....</b>	<b>12</b>
<b>2. DEFINICIÓN DE ORGANIZACIONES.....</b>	<b>12</b>
<b>2.1 Tipos de organizaciones.....</b>	<b>13</b>
<b>3. LA INFORMACIÓN EN UNA EMPRESA .....</b>	<b>13</b>
<b>3.1 Introducción al concepto de información.....</b>	<b>13</b>
<b>3.2 ¿Para qué sirve la información? .....</b>	<b>16</b>
<b>3.3 Atributos relevantes de la información .....</b>	<b>16</b>
<b>3.4 Tipos de información .....</b>	<b>17</b>
3.4.1 Información privilegiada.....	18
3.4.2 Información pública.....	18
3.4.3 Información privada.....	18
<b>4. LOS SISTEMAS DE LA INFORMACIÓN .....</b>	<b>18</b>
<b>4.1 Definición de sistemas de información .....</b>	<b>19</b>
<b>4.2 Funciones del sistema de información.....</b>	<b>20</b>
4.2.1 Buscar y recolectar datos .....	21
4.2.2 Almacenamiento .....	21
4.2.3 Procesamiento de la información .....	22
4.2.4 Distribución o diseminación de la información .....	22
<b>4.3 Objetivo del sistema de información .....</b>	<b>23</b>



<b>4.4 Clasificación de los distintos tipos de sistemas de información.....</b>	<b>23</b>
4.4.1 Los tipos de información en los niveles jerárquicos .....	24
<b>5. SEGURIDAD INFORMÁTICA .....</b>	<b>24</b>
<b>5.1 ¿Qué es la seguridad? .....</b>	<b>24</b>
<b>5.2 Concepto de seguridad informática.....</b>	<b>25</b>
<b>5.3 Áreas de la seguridad informática.....</b>	<b>26</b>
<b>5.4 Objetivos de la seguridad informática .....</b>	<b>26</b>
<b>5.5 Tipos de seguridad informática .....</b>	<b>27</b>
<b>5.6 Necesidad de una cultura de seguridad informática en empresas.....</b>	<b>28</b>
 <b>CAPÍTULO II</b>	
<b>RIESGOS Y GESTIÓN DE SEGURIDAD INFORMÁTICA .....</b>	<b>30</b>
<b>1. AMENAZAS, VULNERABILIDADES Y RIESGOS INFORMÁTICOS .....</b>	<b>31</b>
<b>1.1 Amenazas.....</b>	<b>31</b>
1.1.1 Tipos de amenazas.....	31
<b>1.2 Vulnerabilidad.....</b>	<b>32</b>
1.2.1 Tipos de vulnerabilidad .....	33
1.2.2 ¿Cómo detectar vulnerabilidades en las empresas? .....	36
<b>1.3 ¿Qué son los riesgos? .....</b>	<b>37</b>
1.3.1 Riesgo informático .....	38
<b>2 DELITOS INFORMÁTICOS EN LA EMPRESA .....</b>	<b>39</b>
<b>2.1 Malware .....</b>	<b>39</b>
<b>2.2 Tipos de malware .....</b>	<b>39</b>
<b>2.3 Phising.....</b>	<b>40</b>
<b>2.4 Ataque de inyección SQL .....</b>	<b>41</b>
<b>2.5 Ataque de denegación de servicio .....</b>	<b>41</b>
<b>2.6 Ataque cross-site scripting .....</b>	<b>41</b>
<b>2.7 Ataque bec7eac.....</b>	<b>42</b>
<b>2.8 Robo de identidad .....</b>	<b>43</b>
<b>2.9 Trashing.....</b>	<b>43</b>



<b>3. POLÍTICAS DE SEGURIDAD INFORMÁTICA.....</b>	<b>43</b>
<b>3.1 Definición.....</b>	<b>43</b>
<b>3.2 Aspectos que se consideran en las políticas de seguridad.....</b>	<b>44</b>
<b>3.3 ¿Que protege la seguridad informática?.....</b>	<b>44</b>
<b>3.4 Aspectos que afectan la seguridad.....</b>	<b>47</b>
<b>3.5 Medidas de seguridad informática.....</b>	<b>48</b>
3.5.1 Antivirus.....	48
3.5.2 Cortafuegos.....	48
3.5.3 Actualizar las aplicaciones con los “parches de seguridad”.....	49
3.5.4 Software Legal.....	49
 <b>CAPÍTULO III</b>	
<b>TRABAJO DE CAMPO, ANÁLISIS E INTERPRETACIÓN DE DATOS.....</b>	<b>51</b>
<b>1. INTRODUCCIÓN.....</b>	<b>52</b>
<b>1.1 Universo y muestra.....</b>	<b>52</b>
<b>1.2 Instrumento de medición.....</b>	<b>53</b>
<b>1.3 Resultados e interpretación de datos.....</b>	<b>53</b>
1.3.1 ¿Cuántos años lleva trabajando en la empresa?.....	53
1.3.2 Actualmente en su empresa cuantos dispositivos aproximadamente se conectan.....	54
1.3.3 ¿La empresa posee un departamento para Seguridad Informática?.....	55
1.3.4 ¿La empresa donde Usted trabaja ha tenido ataques cibernéticos?.....	55
1.3.5 ¿Cuántas veces la empresa ha sufrido ataques cibernéticos significativos en los últimos 5 años?.....	56
1.3.6 ¿Cuál fue la estrategia que utilizaron los delincuentes para afectar la seguridad informática? ¿Y cuál fue el estrato de la empresa que fue afectado?.....	57
1.3.7 ¿Después de los ataques se tomaron medidas de seguridad informática? ¿Cuáles?.....	58
1.3.8 ¿Cuáles han sido las vulnerabilidades detectadas en la empresa que propiciaron ataques cibernéticos?.....	60
1.3.9 ¿La empresa utiliza alguna de las siguientes herramientas para mantener segura su red?.....	61
1.3.10 ¿Se realizan mantenimientos periódicos de las computadoras de la empresa?.....	62



1.3.11 ¿Cada cuánto tiempo se realiza el mantenimiento?.....	63
1.3.12 ¿Se realizan pruebas de seguridad en la red? .....	64
<b>CONCLUSIONES.....</b>	<b>67</b>
<b>BIBLIOGRAFÍA.....</b>	<b>68</b>

## INTRODUCCIÓN

Todas las empresas en la actualidad utilizan sistemas informáticos para almacenar su información sensible. El trabajo mismo lleva a los directivos a implementar sistemas de redes interconectadas para funcionar, organizar, procesar, analizar información, obtener mayor visibilidad de los datos, vender o promocionar un producto.

Toda esta información virtual representa un activo elemental para cada empresa y una fuga de información, un ciberataque al sistema podría ocasionar resultados nefastos y hasta podrían destruir la compañía. Teniendo presente esto se debe dar la debida importancia y resguardar la información y gestionar una seguridad informática.

El empleo de la seguridad para proteger la información tiene larga data, ya en la antigüedad, hacia el año 500 a C. se inventó la criptografía, una ciencia que modificaba las representaciones lingüísticas de los mensajes mediante técnicas de cifrado y /o codificado para hacerlos indescifrables a personas no autorizadas. Otro cambio fundamental se produjo en el año 600 a C. donde los griegos inventaron un cifrado por transposición. Se trataba de un cifrado en el que las unidades de texto plano cambiaban de posición siguiendo un esquema bien definido (Muñoz, 2015).

Y a partir de la década de los 80, con la aparición de Internet y las nuevas tecnologías de la información y comunicación se comenzó a utilizar ordenadores interconectados en las empresas para facilitar su funcionamiento. Pero al transcurrir el tiempo se manifestó la vulnerabilidad de esta medida, cuando los sistemas se vieron infectados por virus, los primeros troyanos disfrazados como programas de mejoras. Ante esta emergencia surgió la necesidad de dotar a los sistemas de información, la correspondiente seguridad contra amenazas informáticas, intrusos o programas maliciosos.

La seguridad informática es el área que enfoca la protección de la información que se encuentra computarizada y todo lo relacionado con esta (incluyendo la información contenida), cabe también destacar que estos procesos deben perfeccionarse permanentemente para obtener un adecuado nivel de seguridad (Voutssas, 2010, p. 127-155).

De lo antes expuesto surge la idea de esta investigación que tiene como objetivo principal indagar los ciberataques, las fallas intrínsecas que permiten la comisión de estos delitos y las consecuencias derivadas de los mismos.

En virtud de lo antes dicho se formulan las siguientes preguntas de investigación:

- ¿Cómo impacta la falta de gestión de la seguridad informática en las empresas de la provincia de Mendoza?

- ¿Cuál es el porcentaje de ataques cibernéticos que afectan significativamente a las empresas mendocinas?
- ¿Cuáles son los principales factores que posibilitan la consecución de los ataques?
- ¿Cuáles son los tipos de ataques que sufren las empresas en Mendoza?
- ¿Cómo han gestionado las empresas mendocinas dichos ataques cibernéticos?
- ¿Cuál es el estrato de las empresas que se ven más afectadas por los delitos informáticos?

A continuación, se proponen los siguientes objetivos específicos:

- Determinar el porcentaje de ataques cibernéticos que afectan significativamente a las empresas de Mendoza
- Describir los principales factores que posibilitan la consecución de los ataques
- Enumerar y explicar los tipos de ataque que sufren las empresas de Mendoza
- Obtener de los dueños de las empresas de Mendoza una descripción de las estrategias adoptadas para afrontar los ataques cibernéticos.
- Investigar qué estrato de las empresas se ve más afectado por los delitos informáticos.

Y los supuestos de este trabajo de investigación son:

- El impacto producido por el aumento de ataques a las organizaciones se debe a la falta de gestión en la seguridad informática, en cambio, se observa una disminución de riesgos en las empresas que poseen una fuerte y consolidada gestión de seguridad informática.
- El avance de la tecnología, la creación de nuevas protecciones para los sistemas informáticos, hacen que las vulnerabilidades de las empresas estén relacionadas con los conocimientos y experiencia de los usuarios.

La metodología aplicada en este estudio es de un enfoque cuantitativo, de carácter explicativo. Se aplicarán como instrumento de medición a la muestra, encuestas mediante un cuestionario estructurado con preguntas cerradas a cinco Organizaciones y cinco Pymes de la provincia de Mendoza, los resultados permitirán obtener un mejor conocimiento del actuar y las formas de ataques que se producen en las empresas. Y es explicativa porque busca el porqué de los hechos, considerando la relación causa y efecto, sus conclusiones aportan a un conocimiento más profundo (Hernández Sampieri, Collado & Baptista Lucio, 2006).

Por último, cabe destacar que este proyecto se configura en cuatro capítulos:

En el primer capítulo se introducen los conceptos fundamentales acerca de pymes y organizaciones, sistema de información y la seguridad informática.

En el segundo se explican los conceptos claves que explican los distintos ataques cibernéticos.

En el tercer capítulo se desarrolla la explicación del diseño metodológico.



Y en el cuarto capítulo se tratan los resultados y análisis de las encuestas realizadas en el trabajo de campo, para finalizar en un informe final con las ideas más relevantes y la exposición de los aportes a esta investigación.



**CAPÍTULO I**  
**INFORMÁTICA EN PYMES Y ORGANIZACIONES**  
**SISTEMAS DE INFORMACIÓN Y SEGURIDAD**

En este capítulo se introducen los conceptos fundamentales sobre: Pymes, organizaciones, información, sistemas de información y seguridad informática. Se pretende dar a conocer estos conceptos básicos para luego tener una idea acabada de la importancia y necesidad de la Seguridad informática en las empresas. Para ello se recurre a la consulta de los siguientes autores: Rafael Lapiedra Alcamí, Carlos Devece Carañana y Joaquín Guiral Herrando, Barzanallana Rafael, Hernández Trazabares entre otros.

## **1. PYMES Y ORGANIZACIONES**

### **1.1 Concepto de pymes**

Las PYMES son consideradas en muchos países como el motor de la economía, impulsan la creación de puestos de trabajo y ayudan a incrementar el crecimiento económico.

El término PYME es un acrónimo que hace referencia a una pequeña y mediana empresa, es una empresa mercantil, industrial o de otro tipo que posee pocos trabajadores y que registra ingresos moderados (Definición de, 2022).

También se podría definir como una empresa micro, pequeña o mediana empresa que realiza actividades en Argentina, en los rubros de servicios, comercial, industrial, agropecuario, construcción o minero. Puede estar constituida por una o varias personas y su categoría se establece conforme a la actividad declarada, a los montos de ventas totales anuales o cantidad de empleados (Argentina.gob.ar., s.f.).

El vocablo “Pyme” se puede escribir de dos maneras: PYME o PyME. Este tipo de empresa se caracteriza por tener un número reducido de trabajadores con ingresos moderados, incluye a las unipersonales. Las pymes pueden tener una plantilla de trabajadores de 50 o también reducirse a 5 trabajadores.

No obstante, debido a estas cantidades mínimas de trabajadores, a estas empresas se les dificulta mantenerse en el mercado y competir con grandes corporaciones, en consecuencia, el Estado ha legislado estrategias para estimular su creación y consolidarlas. Las PYMES pueden solicitar créditos para emprendimientos y contar con beneficios fiscales desde el punto de vista impositivo.

### **1.2 Ventajas de las pymes**

Las ventajas que presentan las PYMES son varias, entre ellas se destaca su flexibilidad,

esto les permite cambiar el nicho o modelo de negocios con facilidad. Tienen una relación cercana entre empresario y clientes, condición que crea vínculos fuertes y mayor fidelidad en los trabajadores. Por otra parte, se establecen lazos de simpatía y comunicación fluida con los clientes.

En este tipo de empresas, son más rápidas las decisiones porque la decisión recae sobre una persona o sobre un grupo reducido de personas.

### **1.3 Desventajas de las pymes**

Normalmente las Pymes, tienen dificultades para sostenerse, por ello habitualmente recurren a solicitar una financiación externa, además, por esta razón les resulta difícil competir con otro tipo de empresas.

Por otro lado, les es complicado llegar a un gran número de clientes, porque no puede sostener el costo de publicidad a través de medios masivos y promocionar sus productos. Su condición financiera no les permite tampoco, tener soporte en medio de crisis y fue así que durante la pandemia COVID 19<sup>1</sup> muchas PYMES tuvieron que declararse en quiebra.

Tampoco por su escaso capital tienen poder de negociación con proveedores y clientes y por lo general se ven obligadas a ceder más de lo que quisieran en las negociaciones. Y también se les dificulta acceder a las actualizaciones tecnológicas.

## **2. DEFINICIÓN DE ORGANIZACIONES**

Según Roldán (2017), una organización es definida como: “una asociación de personas que se relacionan entre sí y utilizan recursos de diversas índoles con el fin de lograr determinados objetivos o metas”.

Una organización es una estructura ordenada constituida por un conjunto de personas que tienen responsabilidades y roles distintos orientados a un fin en común, por otro lado, se ajustan a normas y convenciones que regulan la relación de las personas y su rol en la organización (Roldán, Organización, 2017).

---

<sup>1</sup> COVID 19: La COVID-19 es la enfermedad causada por el nuevo coronavirus conocido como SARS-CoV-2. La OMS tuvo noticia por primera vez de la existencia de este nuevo virus el 31 de diciembre de 2019, al ser ¿Definición rescatada de: [https://www.who.int/es/news-room/questions-and-answers/item/coronavirus-disease-covid19#:~:text=La%20COVID%2D19%20es%20la,Wuhan%20\(Rep%C3%BAblica%20Popular%20China\)](https://www.who.int/es/news-room/questions-and-answers/item/coronavirus-disease-covid19#:~:text=La%20COVID%2D19%20es%20la,Wuhan%20(Rep%C3%BAblica%20Popular%20China).).



## 2.1 Tipos de organizaciones

Existen diferentes formas de clasificar las organizaciones, en este estudio se escogen las más relevantes:

- *Según la estructura:* las organizaciones se dividen en formales o informales. La primera son las de rol son más delimitadas que las informales. Las organizaciones informales son más espontáneas surgen de los intereses en común.
- *Según su localización:* pueden ser locales, nacionales e internacionales.
- *Según su tamaño:* pueden ser pequeñas, medianas o grandes organizaciones considerando el número de trabajadores y el ingreso.
- *Según su propiedad:* pueden ser públicas o privadas. Las primeras son empresas cuyo capital pertenece al Estado, pueden ser nacionales, provinciales o municipales. Y las organizaciones privadas son aquellas que son constituidas por particulares.
- *Según su fin:* pueden ser con o sin fines de lucro. Ejemplos: Los bancos tienen fines de lucro mientras hay otras organizaciones que son de ayuda comunitaria.

Ejemplos de organizaciones: Clubes deportivos, partidos políticos, Sindicatos, empresas, organizaciones de ayuda humanitaria.

## 3. LA INFORMACIÓN EN UNA EMPRESA

### 3.1 Introducción al concepto de información

Las personas como las empresas reciben a diario toda clase de datos, pero no todos ellos son relevantes o significativos a sus intereses. Los datos logran un real significado cuando se transforman en información para las empresas y se vuelven útiles para la toma de decisiones.

Los directivos de empresas tienen que planificar, organizar actividades de trabajo, decidir sobre sus negocios, enfrentarse a desafíos, es decir viven en un medio lleno de complejidades e incertidumbres donde es necesario tomar decisiones que lleven a la compañía al éxito. Pero ello, requieren información, las buscan en distintas fuentes, sean formales o informales, devenidas de conversaciones en un café, informes o documentos que reciben. Al recibirlas tienen que analizarlas para luego tomar decisiones, pero no siempre se cuenta con toda la información, aun así, la mayoría toma decisiones sin todos los conocimientos.

Antes de proseguir, es preciso tener en claro tres conceptos claves: Dato, información y conocimiento.

**El dato** es la unidad semántica mínima, es el antecedente preciso para llegar al conocimiento de algo o para inferir las consecuencias de un suceso, dicho de otra forma, es un documento, un fundamento, un testimonio, es la materia prima que en el proceso se convierte en un producto acabado, la información (Bernardi & Dranca, 2020).

**La información:** Etimológicamente el vocablo “información” deriva del sustantivo latino *informatio (-nis)* y del verbo “*informare*” que tiene como significado: dar forma a la mente, disciplinar, enseñar. La palabra latina “*informationis*” es utilizada para indicar un "concepto" o una "idea" (Barzanallana).

La información es un conjunto de datos que han sido procesados y que adquieren un valor significativo para la persona que los ha recibido, aporta un conocimiento, reduce la incertidumbre, y colaboran para la toma de decisiones (Bernardi & Dranca, 2020).

**El conocimiento** es la combinación de contexto, experiencia, interpretación y reflexión (Bernardi & Dranca, 2020). En la siguiente figura se podrá conocer la jerarquía de estos conceptos: dato, información, conocimiento.

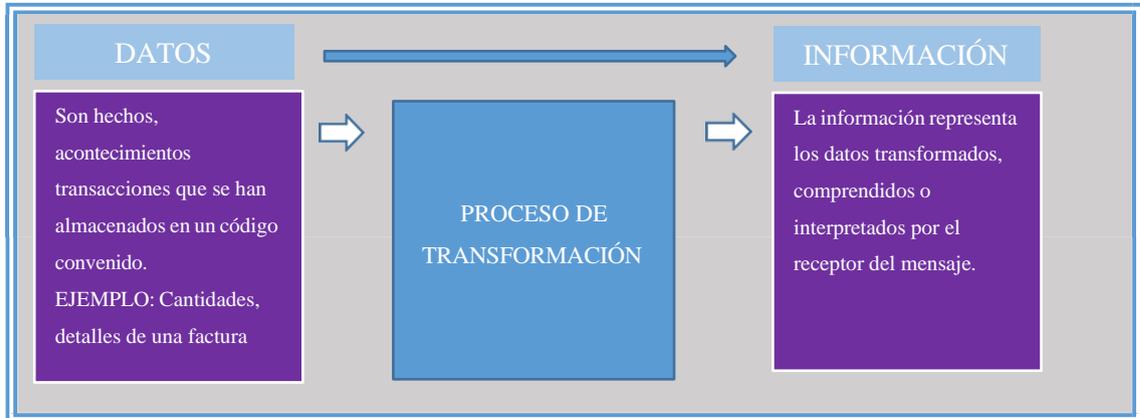
*Ilustración N°1: Dato, información y conocimiento*



Fuente: Elaboración propia.

De acuerdo a (Lapiedra Alcamí, Devece Carañana, & Guiral Herrando, 2011) los datos “son símbolos aleatorios que representan valores de atributos o sucesos” (...) y “la información representa los datos transformados de forma significativa para la persona que los recibe, es decir, tiene un valor real o percibido para sus decisiones y para sus acciones”.

Ilustración 2: Diferencia entre datos e información



Fuente: Elaboración propia.

En la ilustración anterior, se puede notar la diferencia entre datos e información y cómo se produce esa transformación en la mente del receptor. El individuo recibe los datos y hace una reflexión e interpretación personal, le confiere una significación y se forma el mensaje.

La información es un recurso importante para las empresas, así como el capital humano, los recursos materiales, pero sin información no es viable una compañía. También es necesario destacar que el tipo de información se ajustará a los requerimientos del momento, la confiabilidad, el nivel de jerarquía de la persona que la pide, el área de trabajo etc. Inclusive cuando se transfiriere la información, esta puede tener cambios de significados, por ejemplo: en una organización para un individuo algo puede ser información y para la otra que lo recibe solo significar un dato porque no se ajusta al valor de la información que necesita para tomar una decisión, lo que equivale determinar una acción. Esta variación también puede relacionarse con el tiempo, el momento en que se obtiene la información. Sí es a destiempo, se convierte en un dato sin valor. Menguzzato y Renau (1991) citado por (Lapiedra Alcamí, Devecé Carañana, & Guiral Herrando, 2011).

Ilustración 1 Información-toma de decisiones y acción



**INFORMACIÓN** → **TOMA DE DECISIÓN** → **ACCIÓN**

Fuente: Imagen de: <https://www.tipsempresariales.com/tips/plan-de-negocios>

### 3.2 ¿Para qué sirve la información?

La información puede tener diferentes usos y motivaciones para buscarla. La información sirve para: “reducir la incertidumbre o acrecentar el contenido que tiene una determina área, contexto o situación” (Morales, 2020). De allí que para algunas personas tener información es tener poder y conocimientos que otros no lo tienen.

Pero tener mucha información no garantiza el conocimiento acertado, se requiere que la persona que va a procesar los nuevos datos reconozca la información correcta de la incorrecta. La información tiene que servir para aclarar una situación, complementar otros conocimientos y ajustarse para guiar una decisión o acción. Dicho de otra forma, la información es útil cuando es la correcta para un fin determinado.

### 3.3 Atributos relevantes de la información

De acuerdo a Lapiedra Alcamí, Devece Carañana, & Guiral Herrando (2011), una información tiene valor cuando cuenta con las siguientes características:

- **Relevancia:** La información es relevante cuando proporciona conocimientos y disminuye las dudas acerca de un determinado problema. A veces, la información recibida no es clara, tiene partes irrelevantes que dificultan la comprensión y entorpecen su uso y se toman decisiones erróneas. La correcta información es aquella donde no hay sobrecarga de datos, sino que es ajustada y es capaz de resolver un problema.
- **Exactitud:** La información tiene que ajustarse al destino o propósito por el cual ha sido buscada. Dicho en otras palabras, la información tiene que ser precisa, exponer todos los detalles necesarios para comprender su significado, ajustarse a la importancia de la decisión que se intenta tomar y dependerá del rango jerárquico de la persona que va a tomar la determinación.
- **Completa:** Una información es completa cuando abarca los puntos claves del problema a resolver y proporciona toda la información requerida en un momento y para un problema determinado. Cuando no se dispone de la información necesaria, esta no tiene mucha utilidad para resolver un problema.
- **Confianza en la fuente:** Esta confianza o seguridad proviene de las experiencias pasadas con una fuente, de allí que la fuente es calificada como digna de crédito. Los directivos de empresas para tomar decisiones estratégicas, consultan varias fuentes para disminuir los índices de error.
- **Comunicar a la persona correcta:** En toda empresa, los directivos tienen sus funciones y responsabilidades, y en forma continua reciben información para funcionar en su rol. En

ocasiones, esto no funciona como debería ser porque fallan las comunicaciones y no se proporciona la información adecuada a la persona que la necesita o bien se retiene información para obtener mayor poder y hacerse indispensable. Los que administran la información deben hacerla llegar directamente donde es requerida, a la persona correcta.

- **Puntualidad:** En este aspecto, se considera la importancia de brindar la información en el momento que se la precisa para ser utilizada. Se trata aquí de valorar la rapidez en brindar una información. Una información vital que llega a destiempo en una empresa pierde su valor.
- **Detalle:** La información en lo posible para ser más eficaz debe contener la mínima cantidad de detalles. Se tiene que eliminar todo dato superfluo que dificultan su interpretación y ser precisa, acotada. En ocasiones la cantidad de detalles puede variar de acuerdo al nivel de la organización. En organizaciones de alto nivel, se necesita una información más puntual para dirigir la atención a otros aspectos y en niveles más bajas, tiene que ser con más detalles. Con frecuencia se utilizan los informes donde se destacan ítems, muy usados en la técnica contable de control presupuestario esto permite síntesis y realizar la función de control en menor tiempo.
- **Comprensión:** Es justamente esta propiedad mediante la cual los datos se convierten en información. Si no se entienden los datos recibidos no es posible utilizar la información.

Los factores que influyen en la comprensión son:

*La preferencia de los usuarios;* algunos prefieren la información brindada en gráficos o cuadros, otros prefieren textos, estadísticas, otros se inclinan a trabajos de investigación donde pueden ver reflejados comportamientos etc.

*Conocimientos previos.* La comprensión es un resultado de la asociación de memoria con el mensaje recibido.

*Factores ambientales* como el tiempo, la confianza que brinda la fuente.

*El lenguaje.* La información es codificada en señales o mensajes.

### 3.4 Tipos de información

A continuación, se presentan los distintos tipos de información de acuerdo a Morales ( 2020).



### **3.4.1 Información privilegiada**

Este tipo de información solo se encuentra disponible para algunas personas, debido a su contenido el acceso es restringido para evitar que se divulgue. Ejemplo: los datos compartidos en una reunión empresarial.

### **3.4.2 Información pública**

Se trata de una información que es de libre acceso al público en general, se basa en la libertad de expresión, tiene una corta duración. Ejemplo: informes de gobierno, publicidades.

### **3.4.3 Información privada**

Este tipo de información no se divulga, se establece por ley y acceder a esta información puede perjudicar la seguridad personal, profesional, empresarial o de gobierno. Ejemplo: datos de cuenta bancaria.

### **3.4.4 Información externa**

Se trata de aquella información que ingresa a una empresa por distintas vías externas y se utiliza para resolver algún problema. Una compañía recibe todo tipo de información de distintas fuentes externas, se deben evaluar y escoger las que sirven para satisfacer las necesidades de información de la empresa. (Morales, 2020).

## **4 LOS SISTEMAS DE LA INFORMACIÓN**

El mundo de los negocios ha sufrido muchos cambios debido a la globalización, el aumento de la competencia en los mercados y el desarrollo de nuevas tecnologías de la información, aumento de incertidumbres de allí que es importante explicar debidamente lo que son los sistemas de información en el presente.

En la actualidad la mayoría de las organizaciones, empresas dependen de los sistemas de información para gestionar todas sus actividades, desde un simple correo hasta la administración de la base de datos o el manejo de su sitio web.

#### 4.1 Definición de sistemas de información

De acuerdo a La Real Academia Española: Diccionario de la lengua española, versión en línea 2021, <https://www.rae.es/drae2001/sistema>, consultado el 15 de diciembre de 2022, el término “sistema” tiene las siguientes acepciones:

- Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí.
- Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a un determinado objeto.

Para Bernardi & Dranca (2020), en sentido general, un sistema tiene varios elementos interrelacionados que buscan un objetivo en común: proporcionar la información necesaria para tomar las resoluciones pertinentes. Es un mecanismo donde se reciben datos en brutos, se analizan, procesan y se genera la información y se produce una retroalimentación donde una cierta proporción de salida vuelve a dirigirse a la entrada.

Para Laudon & Laudon (2012) un sistema de información es: “un conjunto de componentes interrelacionados que reúne (u obtiene), procesa, almacena y distribuye información para apoyar la toma de decisiones y el control en una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores a analizar problemas, a visualizar asuntos complejos y crear productos nuevos”.

De esta definición se deduce que un sistema de información es un conjunto de componentes interrelacionados que se procesan, almacenan para luego distribuir la información, que puede ser útil para dar solución a un problema complejo, o simplemente tomar decisiones o ejecutar un control estratégico.

Otro aspecto que es necesario aclarar es que un sistema de información no es sinónimo de un sistema informático.

El sistema de información se compone de los siguientes elementos:

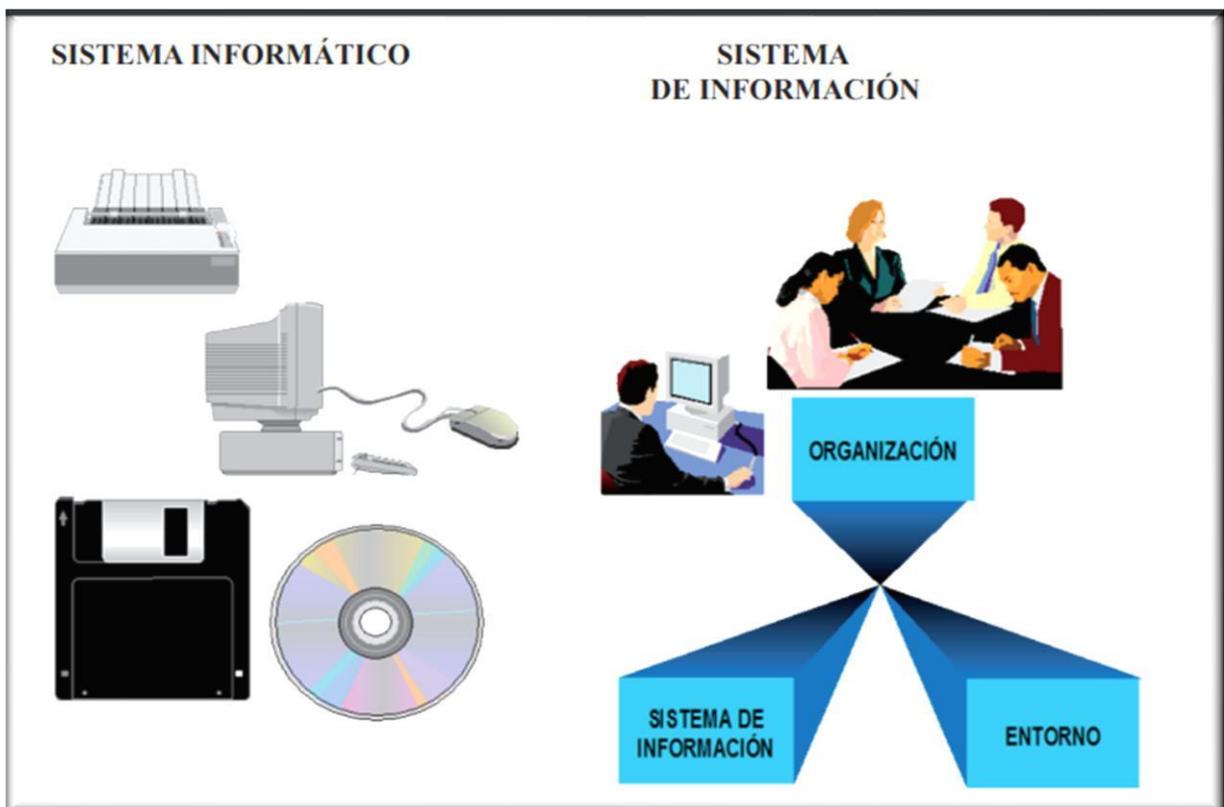
- **Hardware:** una computadora, dispositivos, aparatos, servidores, servicios de Nube, terminales, con los cuales interactúan los usuarios en su uso.
- **Software:** hace referencia a los programas que se utilizan para llevar adelante la administración, el correspondiente procesamiento y análisis. Los programas son parte del software del sistema de información.
- **El recurso humano:** las personas que interactúan con el sistema, alimentándolo de datos o extrayendo información, que lo utilizan para aprovechar sus ventajas y optimizar su trabajo.
- **Bases de datos:** son recursos que se utilizan para organizar datos en tablas y archivos.
- **Telecomunicaciones:** son el hardware y el software que hacen posible la transmisión de

textos, datos, imágenes, informes etc. En la actualidad, los sistemas computarizados están unidas a redes de telecomunicaciones. En una empresa pequeña existen red de computadoras conectadas para hacer más sencillas las comunicaciones entre los trabajadores y compartir datos y trabajar en equipo. Cuando se tratan de empresas de mayor magnitud, se emplean redes de área amplia (Whan) para conectarse con lugares remotos. A través de Internet, la red de redes se pueden ampliar los horizontes de los negocios.

- **Procedimientos:** se tratan de las políticas y reglas que rigen el funcionamiento de la organización y los mecanismos que hacen trabajar las aplicaciones de la computadora.

Mientras que el sistema informático: alude a un sistema computarizado, que sirve para almacenar, procesar y disponer información. En la ilustración siguiente se puede observar el sistema informático y el sistema de información.

*Ilustración N 3: Sistema informático y sistema de información.*



Fuente: imagen extraída de <https://libros.metabiblioteca.org/bitstream/001/193/8/978-84-693-9894-4.pdf> consultada el 16 de diciembre de 2022.

## 4.2 Funciones del sistema de información

Los sistemas de información tienen la tarea de optimizar los recursos y colaborar en el

desempeño de las actividades de la empresa. Sus funciones son:

- Buscar y recolectar los datos.
- Almacenamiento.
- Procesamiento de la información.
- Distribución o disseminación de la información.

Siguiendo a Lapiedra Alcamí, Devece Carañana, & Guiral Herrando (2011) a, continuación se desarrollarán los ítems ya mencionados.

#### **4.2.1 Buscar y recolectar datos**

Esta función tiene que ver con la búsqueda de la información. Quién o quiénes se ocuparán de recolectar los datos depende del tipo de empresa que se trate. Pueden ser compradores o vendedores, autoridades jerárquicas de la compañía o trabajadores que tengan contactos externos que puedan aportar información. Los datos provienen de fuentes externas e internas de la empresa y se envían a los órganos del sistema donde son reagrupados y se eliminan todo tipo información superflua o duplicada.

#### **4.2.2 Almacenamiento**

Acerca de este punto, antes del almacenamiento, la empresa tiene que preguntarse: ¿Cuál será el criterio para el almacenamiento de la información? ¿Qué soporte es el apropiado para guardar la información? ¿Y cómo y a quienes dar el acceso de la información almacenada?

La empresa tiene que considerar el volumen de sus datos, la frecuencia con que se utiliza, por tanto, debe escoger el soporte adecuado para el almacenamiento que puede ser un archivador-clasificador clásico o una base de datos de tratamiento informático entre otros.

Según AMBIT (2020), los dispositivos para almacenamiento pueden ser:

- Discos

**Discos duros:** Discos HDD (Hard Drive Disk) estos dispositivos utilizan el magnetismo para grabar los datos.

**Discos en estado sólido** SSD (Solid State Drive) almacenan la información en Chip con memorias flash interconectas (memorias NAND que mantienen la información cuando se corta el suministro eléctrico) Dentro de él, existen tres tipos según su conexión: SATA, M.2 y PCIe NVME.

- Cintas magnéticas: existen diferentes tipos de cintas de almacenamiento según su composición química o formatos de grabación y tamaño de soporte.
- Almacenamiento en red: las redes actualmente tienen una capacidad de transferencia de al menos 1000 Mbps, en caso de red de fibra óptica, de 10Gbps, esto les permite transmitir mucha información en breve tiempo. Los tipos de almacenamiento en red son SAN (su uso principal es en servidores de aplicaciones o NAS (destinados sobre todo a almacenamiento

de empresas o personal).

- Almacenamiento en la Nube: Se trata de un almacenamiento externo donde es posible almacenar toda la información y acceder en el momento que se la necesite independientemente del sistema operativo, ubicación, dispositivo que se utilice. (s. p.)

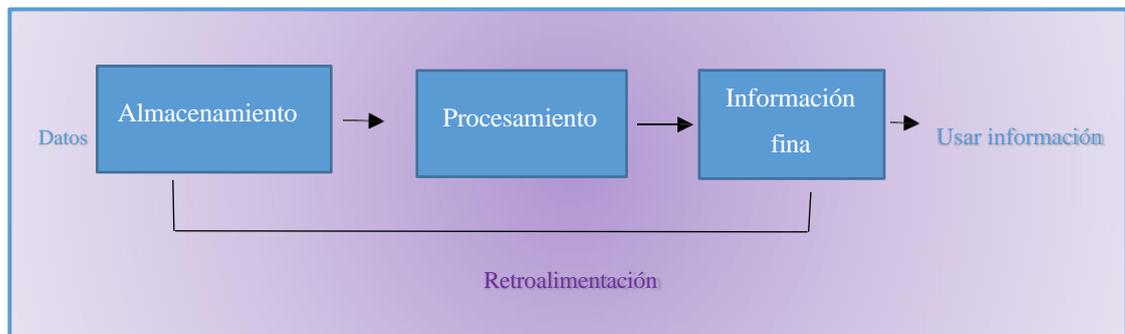
#### 4.2.3 Procesamiento de la información

En esta función el objetivo es transformar la información almacenada en una información útil y significativa para el uso de los usuarios. El tratamiento de la información se realiza a través de un subsistema informático.

#### 4.2.4 Distribución o diseminación de la información

El sistema de información tiene que brindar a los usuarios la información en el momento que la precisan, de forma correcta para que pueda ser interpretada y transmitida a las personas de la empresa. Es necesario para las empresas que la información esté disponible para la resolución de problemas y toma de decisiones. Las unidades más conocidas de salida de un sistema de información son: impresoras, estaciones de trabajo, la voz, cintas magnéticas etc.

*Ilustración N°4: Sistema de información*



Fuente: Elaboración propia.

Los sistemas de información pueden ser de tipo informal o formal. Un sistema de información informal si bien es tenido en cuenta en las empresas, tienen sus limitaciones porque no han sido planificadas, son casuales, no obstante, no se las puede ignorar porque a veces pueden ser efectivas, por ejemplo, un rumor en la empresa puede llegar más rápido que la información que sigue distintos procesos. En cambio, un sistema de información es formal porque responde a reglas preestablecidas y tiene una estructura.

### 4.3 Objetivo del sistema de información

El objetivo en términos generales es contribuir a las actividades administrativas y de gestión con las distintas áreas de la empresa proveyendo una información adecuada y de calidad en el momento oportuno para su uso.

A continuación, se resumen los objetivos principales de acuerdo a la perspectiva de (Hernández Trazobares, 2020):

- *Apoyar la dirección de la empresa, sus objetivos y estrategias:* el sistema de información tiene como responsabilidad transmitir a la compañía toda la información necesaria, tanto para desarrollar las actividades diarias como aquellas que son más complejas para la planificación y desarrollo de decisiones.
- *Brindar información para el control de las actividades globales de la empresa,* para el cumplimiento de los objetivos planteados por la organización.
- *Ajustar la información a la evolución de la compañía:* porque la empresa se desarrolla, las necesidades van cambiando, por tanto, el sistema de información también tiene adaptarse a las nuevas necesidades.
- *Interactuar con las distintas áreas de la empresa* para que cada área sea provista de manera eficaz y rápida de la información que necesiten, esto le otorga al sistema de información una mayor flexibilidad.

De esta manera, un sistema de información para ser efectivo en la transmisión de la información y cumplir con los objetivos determinados por la empresa tiene que evaluar la calidad de los datos que recibe, eliminar toda información superflua, redundancias, almacenar los datos para que puedan estar disponible para los usuarios que la necesiten, evitar toda fuga de información o la divulgación en personas no autorizadas, colaborando en generar información útil en la salida y propiciando la toma de decisiones.

### 4.4 Clasificación de los distintos tipos de sistemas de información

De acuerdo a García Bravo, 2000 y Edwards, Ward y Bythesway (1998) los sistemas de información se clasifican de la siguiente manera:

- **Según el grado de formalidad:** en formales e informales
- **Según la automatización** en; manuales e informáticos.
- **Según la relación con la toma de decisiones:**

\*Estratégicos (alta dirección).

\*Gerencial (nivel intermedio).

\*Operativo (control operativo).

- **Según la funcionalidad:** Gestión comercial, gestión contable, gestión financiera, gestión de recursos humanos y gestión de producción.
- **Según grado de especificación:** específicos y generales.

#### 4.4.1 Los tipos de información en los niveles jerárquicos

La información que se provee en los distintos niveles jerárquicos no son los mismos. En la alta dirección de una empresa, los directivos requieren una información resumida, general, amplia, para tomar decisiones a largo plazo. En los mandos intermedios, se requiere información menos detallada, precisa para tomar decisiones tácticas de medio plazo. En los mandos operativos, se necesitan informaciones detalladas sin resumir, para decisiones de corto plazo.

## 5. SEGURIDAD INFORMÁTICA

Actualmente es una prioridad que las empresas piensen seriamente en resguardar toda su información ya que es un capital esencial para el funcionamiento de la misma, si la información se daña o es foco de ataques cibernéticos pueden ocurrir graves repercusiones como, por ejemplo, que la información confidencial quede expuesta a manos de los competidores, se bloqueen los accesos y no se disponga de la información o puede ser motivo de extorción por parte de delincuentes etc. Todo el arduo de trabajo de años para levantar una compañía puede desplomarse y destruirla.

La informática y las tecnologías aplicadas a las actividades de las empresas tiene grandes ventajas, facilita la comunicación y agiliza procesos, pero requiere contemplar posibles riesgos de allí que se insiste en la importancia de la seguridad y protección de la información.

### 5.1 ¿Qué es la seguridad?

Para la Real Academia Española: Diccionario de la lengua española, versión en línea 2021, rescatado de <https://www.rae.es/drae2001/seguridad>, consultado el 15 de diciembre de 2022, el término “seguridad”, proviene del latín *seguritas*, *atis* que significa cualidad de estar seguro, certeza, fianza de indemnidad a favor de alguien, regularmente en materia de intereses.

La seguridad en términos generales equivale a tener confianza, libertad frente al peligro, a

los adversarios, ausencia de riesgos o peligros, es el objeto de estudio de las ciencias de la seguridad.

El término seguridad es aplicado a diferentes ámbitos, por eso se conocen distintos tipos de seguridad, como: seguridad nacional, seguridad ambiental, seguridad sanitaria, seguridad laboral, seguridad social, seguridad informática entre otras (Editorial Etecé, 2020).

De acuerdo a Romero Castro, y otros (2018) La seguridad propone gestionar, tratar de evitar, prevenir riesgos y brindar estrategias preventivas. La expresión “ausencia de riesgos” engloba cuatro acciones:

- Prevención del riesgo.
- Transferir el riesgo.
- Mitigar el riesgo.
- Aceptar el riesgo.

Estas son las medidas necesarias cuando se trata de seguridad, independientemente de cualquier tipo de seguridad.

## 5.2 Concepto de seguridad informática

La seguridad informática se trata de la seguridad del medio informático, busca proteger todo aquello que almacene información. Según Aguilera, 2011 citado por Romero Castro, y otros, (2018, pág. 14) la seguridad informática es: “Una disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad”.

Para Samaniego Mena & Ponce Ordóñez la seguridad informática es:

Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema ((2021, p. 2).

De estas definiciones se puede inferir que la seguridad informática es una ciencia que se ocupa planificar y establecer normas, procedimientos, técnicas para impedir las operaciones de personas no autorizadas y resguardar la confiabilidad, la integridad de la información de cualquier ataque cibernético, lo que implica dar confianza y seguridad de protección.

Dicho de otra forma, la seguridad informática es la disciplina que se ocupa de proteger sistemas interconectados específicamente la información que contienen estos sistemas. Las medidas de seguridad informática son variadas engloba desde antivirus,

firewall y estrategias sofisticadas que requieren alto conocimiento como activación o desactivación de ciertas funciones de software.

### 5.3 Áreas de la seguridad informática

Retomando a Romero Castro, y otros (2018), la seguridad informática contempla bajo su cuidado tres áreas fundamentales:

**\*Los usuarios:** son considerados el eslabón más frágil de la cadena, porque ellos no pueden ser controlados. Los usuarios en cualquier momento pueden cometer errores, olvidarse de guardar información relevante, utilizar inadecuadamente los programas, borrar contenidos por accidente, todas estas acciones del usuario pueden ocasionar severas consecuencias a la empresa.

**\*La información:** es el principal objetivo de la seguridad informática porque la información es valiosa para toda compañía, tiene que estar a salvo, bien resguardada. Es decir, que no tengan acceso a la información confidencial de la empresa como aspectos administrativos y datos bancarios. Para ello se clasifican los datos y solo se otorga permiso a personas autorizadas. Solo estas personas pueden realizar cambios, los demás pueden ver la información, pero no realizar cambios.

**\*La infraestructura:** si bien, es un medio que puede controlarse, también implica riesgos y amenazas a la información, problemas complejos como acceso de intrusos, personas no autorizadas, robo de equipos, consecuencias de catástrofes naturales como incendios, inundaciones que perjudiquen el material físico del sistema de la empresa.

### 5.4 Objetivos de la seguridad informática

Seguendo a Samaniego Mena & Ponce Ordóñez (2021) los objetivos de la seguridad informática son:

- Planificar y gestionar los riesgos e identificar posibles atentados y amenazas a la seguridad.
- Propiciar el adecuado uso de los recursos y de las aplicaciones del sistema.
- Reducir las pérdidas y recuperar el sistema en caso de sufrir un incidente de seguridad.
- Ajustarse al marco legal y los requerimientos establecidos por los clientes en sus contratos.

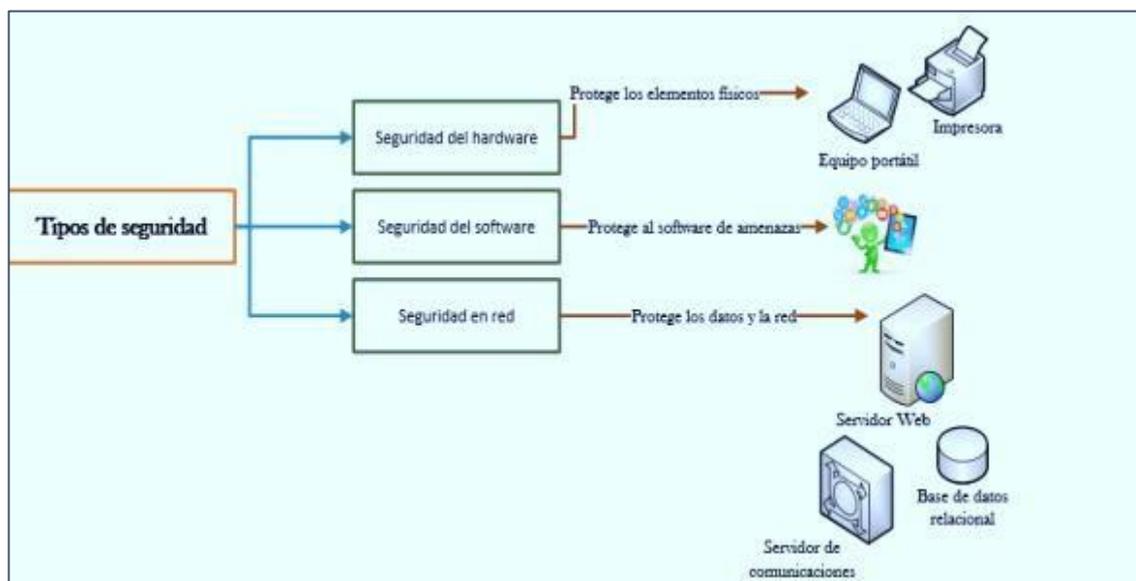
## 5.5 Tipos de seguridad informática

**Seguridad del hardware:** este tipo de seguridad, resguarda los elementos físicos de cualquier perjuicio, brinda una fuerte seguridad los sistemas de alimentación ininterrumpida, los cortafuegos etc. Trata de proteger el Hardware de los problemas de vulnerabilidad, las entrada y salida de datos en la navegación en Internet.

**Seguridad del software:** se trata de proteger el software de los ataques cibernéticos, que atentan a la confidencialidad, integridad y disponibilidad de los datos. Existen distintas formas de perjudicarlo, por ejemplo, falencias de implementación, defectos en el diseño, falta de seguridad en el código, mal manejo de errores, entre otros.

**Seguridad de Red:** Protege los datos y la red, cuida que los datos no sean robados, modificados y en cuanto a la red, cuenta con distintos niveles de seguridad para que si uno es vulnerado otros sigan trabajando. (Samaniego Mena & Ponce Ordóñez, 2021). Protege la red de personas indeseables que vulneran el acceso, para sustraer información, de manera tal que se asigna un administrador que tiene una identificación y contraseña para ingresar al sistema y acceder a los datos y programas bajo su cargo.

*Ilustración N°5: Tipos de seguridad*



Fuente: (Samaniego Mena & Ponce Ordóñez, 2021)

## 5.6 Necesidad de una cultura de seguridad informática en empresas

Los hechos demuestran que, en el presente, las empresas conocen en cierta forma, la posibilidad de ataques cibernéticos, robo de información, fraudes en la red, suplantación de identidad, pero existe muy poca atención en formar en los empleados para una cultura de seguridad informática.

Muchas veces, son los mismos empleados o usuarios los que provocan daños con o sin intención a la seguridad informática de una organización, navegan en la red de forma desprevenida y por esta razón u otras se infiltran intrusos e infectan el sistema y acceden a la información. Por tanto, es necesario implementar y reconocer la necesidad de una cultura de seguridad informática para incorporar nuevas actitudes de cuidado y responsabilidad hacia el manejo de los recursos informáticos.

### 5.6.1 Acciones para una buena cultura de seguridad

A continuación, se describirán algunos aspectos, de los cuales se deberían dar charlas educativas a los empleados de las empresas para fomentar el cuidado y la cultura en seguridad informática:

- 5.6.1.1 **Encontrar una memoria USB:** esta es una forma muy frecuentemente utilizada por los hackers para robar información. Sucede que una persona que encuentra una memoria USB movido por la curiosidad, se pregunta acerca de su contenido y con el fin de satisfacer su inquietud, lleva la memoria USB y la introduce en su ordenador y sin saber con ese hecho está permitiendo que unos posibles hackers ingresen a su ordenador y acceda a su información personal. Alrededor del 60% de las personas que encuentran memorias, deciden abrir al menos un archivo, generalmente quien lo hace no tiene en cuenta que es la puerta para el robo de información.
- 5.6.1.2 **Venta de información confidencial de la empresa:** Los empleados de una organización que trabajan en el área informática, tienen conocimiento del valor de la información, pero las personas que no se sienten involucradas, identificadas con su empresa o no se sienten valoradas, pueden incurrir en el error de intercambiar documentos, vender información.
- 5.6.1.3 **Dar la debida importancia sobre la seguridad antes que la comodidad:** En cuanto a este punto, es necesario cumplir con todos protocolos de autorización de los sistemas operativos, no saltarse pasos. A veces los empleados para terminar con rapidez el trabajo, no respetan las actualizaciones y esto puede traer como consecuencia que los sistemas de

seguridad informática no funcionen adecuadamente lo que deja una oportunidad para los hackers.

5.6.1.4 **La desprotección en descargas:** Regularmente gran parte de los empleados, que no conocen las tecnologías no toman los recaudos necesarios al realizar descargas varias de documentos, videos, informes etc. no tienen presente la seguridad, estos pueden venir infectados por virus.

5.6.1.5 **No reportar incidentes de ciberseguridad:** Suele suceder que en muchas oportunidades los empleados no reportan incidentes a nivel tecnológico o informático, infiltración de algún virus, dar permiso para ingreso de malware en su ordenador etc. Esto ocurre quizás, por el temor de ser despedidos de la empresa. Lo cierto es que estos códigos malignos pueden acceder fácilmente a los servidores de la compañía y causar cuantiosos daños (Bustamente, 2020).

Es importante tener presente estos sucesos para contrarrestarlos y desarrollar una correcta actitud frente los ataques a la seguridad informática.

En resumen, en toda pyme u organización, la información es un recurso importante, sin información no es viable una compañía. La información tiene que ajustarse a los requerimientos del momento, la confiabilidad, el nivel de jerarquía de la persona que la pide, el área de trabajo etc., Para Laudon & Laudon (2012) un sistema de información es un conjunto de componentes interrelacionados que reúne, procesa, almacena y distribuye información para apoyar la toma de decisiones y el control en una organización. Una fuga de información puede generar la quiebra de una empresa por ello se hace indispensable establecer un cuidado específico mediante una seguridad informática. Para ello, la seguridad informática tiene que planificar y gestionar los riesgos, identificar las amenazas y propiciar el uso adecuado de recursos para reducir pérdidas.



## **CAPÍTULO II**

# **RIESGOS Y GESTIÓN DE SEGURIDAD INFORMÁTICA**

El presente capítulo se inicia con conceptos claves como amenazas, vulnerabilidades y riesgos informáticos, para luego exponer y explicar los diversos ataques y delitos informáticos a los que se ven expuestas las empresas y de esta forma conocer los peligros que presentan las redes informáticas, cómo en la actualidad, los ciber delincuentes se han especializado para infiltrarse en ordenadores, robar datos, información y causar daños a las empresas. Sabiendo esto, se desarrolla como implementar políticas de seguridad, su importancia y explicar mecanismos de protección de la seguridad informática. Para ello se consultarán los siguientes autores: Cardona Arboleda, Omar Darío, Briceño Huaygua, Cristhian Abijail, entre otros.

## 1. AMENAZAS, VULNERABILIDADES Y RIESGOS INFORMÁTICOS

### 1.1 Amenazas

De acuerdo a Cardona Arboleda (2001) el término amenaza, puede ser entendido como: “la probabilidad de ocurrencia de un suceso potencialmente desastroso durante un cierto período de tiempo en un sitio dado” (...) “estar propenso a o ser susceptible de sufrir daño o perjuicio”.

La amenaza supone una advertencia de un daño, un presagio, una probabilidad de un posible daño, sugiere la idea de peligro latente, peligrosidad. Este concepto enfocado a la seguridad informática, es entendido como toda acción que aprovecha una vulnerabilidad para invadir el sistema informático y provocar daños, estos ataques pueden ser externos o internos como, por ejemplo, robo de información o uso inapropiado de los sistemas informáticos.

#### 1.1.1 Tipos de amenazas

Las amenazas que atentan contra la información pueden atentar contra la confiabilidad, la integridad y disponibilidad, los pilares de la seguridad informática. Si alguno de estos aspectos se encuentra débil, la organización o empresa puede hallarse expuesta a ataques cibernéticos.

**La confiabilidad** se produce porque se mantiene la información oculta, secreta. Esto es muy importante cuando se trata de información sensible, para cuidar la seguridad de la misma, se establece que solo personas autorizadas pueden acceder a la información y con tal propósito disponen de recursos como: autenticación de usuarios que tiene como objetivo identificar qué,

quién accede a la información, la manera en cómo, tendrán autorización, encriptación etc.

Las situaciones que pueden hacer vulnerables la información son: cuando la información se halla almacenada en un sistema de cómputo, cuando la información está moviéndose hacia otro sistema o cuando la información se encuentra en cintas de respaldo.

**Integridad**, este otro pilar de la seguridad, se trata de cuidar que la información no se pierda o adultere o sea manipulada, porque eso significaría causar una cadena de errores sucesivos lo cual llevaría obviamente a decisiones equivocadas. Para que esto no ocurra, se debe contemplar el monitoreo del tráfico de red para detectar posibles amenazas, accesos no autorizados, auditar los sistemas para determinar quién ingresa al sistema, en qué momento lo hace y con qué información y disponibilidad, por otra parte, establecer un sistema para reeditar información y corregir errores y otro recurso es tener copias de respaldo de toda la información valiosa de la empresa.

**Disponibilidad:** hace alusión a la disponibilidad de la información. Es preciso que la información y los servicios estén disponibles cuando se los necesite, y que llegar a la información, no sea un paso complicado. Por ejemplo, un ataque distribuido de denegación de servicio o DDoS puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar.

Existen dos tipos de amenazas Arroba system (2021):

- *Aquellas que no se pueden controlar:* como los desastres naturales como dañarse el Hardware por el uso, por sismos u otras catástrofes inesperadas, fallas eléctricas o por errores humanos como enviar un correo con información confidencial a un destinatario equivocado, eliminar información de manera involuntaria de un servidor.
- *Y las que son voluntarias:* son producidas de manera intencional por piratas informáticos que acceden a las computadoras, dispositivos y/o servidores con el fin de obtener claves de las tarjetas de créditos de las víctimas, robar información confidencial, colgarse de Internet, acceder a información bancaria o infectar la computadora.

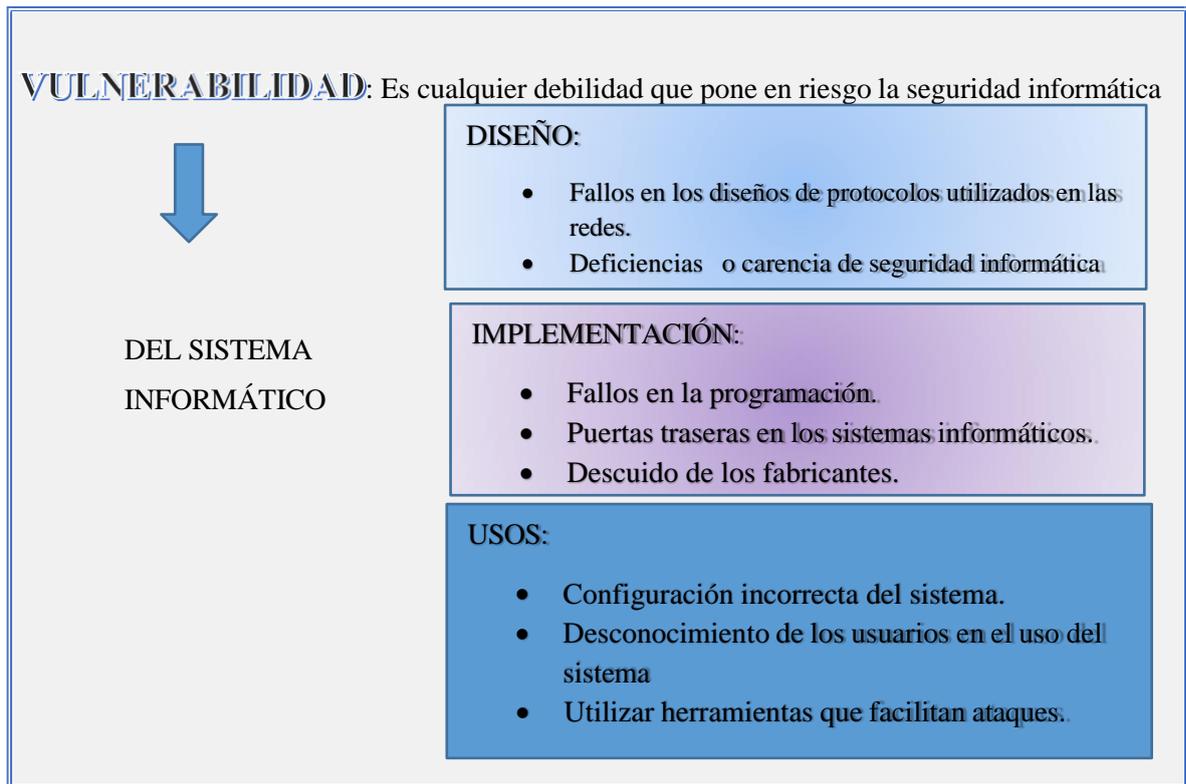
## 1.2 Vulnerabilidad

De acuerdo a Castro Romero, y otros (2018), las vulnerabilidades son fallos de diseño, de procedimientos o de recursos. Los fallos de un sistema suceden cuando este se encuentra obsoleto, o está mal configurado. También se producen vulnerabilidades por una deficiente gestión de recursos, errores a la hora de validar la información cargadas en base de datos, fallos voluntarios o involuntarios de los usuarios, carencia de rigor en los accesos y permisos otorgados.

Dicho en otras palabras, “una vulnerabilidad es una debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confiabilidad, integridad,

disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones” (Marker, 2020). Por otra parte, Marker afirma que las vulnerabilidades “se tratan de partes del código fuente del programa que no han sido concienzudamente escritas teniendo en cuenta la seguridad global de una aplicación”, por tanto, es una oportunidad para que un hacker o una persona con altos conocimientos aproveche la situación para atacarlo y robar información o manipular el sistema a su conveniencia.

Ilustración N°6: Las vulnerabilidades del sistema informático



Fuente: Elaboración propia.

### 1.2.1 Tipos de vulnerabilidad

Existen distintas formas de clasificar las vulnerabilidades, en este estudio se menciona la clasificación de (Castro Romero, y otros, 2018). Para estos autores, las vulnerabilidades se dividen en lógicas y físicas:

*Las vulnerabilidades lógicas* son las que afectan la infraestructura: la configuración, actualización y desarrollo. *Las vulnerabilidades de la configuración* son fallos muy comunes. Pueden devenir de un defecto del sistema o de algunas aplicaciones del servidor o de algunos firewalls, que no hayan sido gestionado correctamente. Por ejemplo, los password por default, password débiles, usuarios con demasiados privilegios e inclusive la utilización de protocolos de encriptación obsoletos.

*En cuanto a la actualización*, las vulnerabilidades se presentan cuando no se actualizan los sistemas, por ejemplo, el caso de los sistemas operativos XP de Windows no tienen soportes y allí comienzan sus vulnerabilidades. También las vulnerabilidades pueden provenir de algún protocolo de SSH que no se haya parchado o actualizado.

*Con respecto a las vulnerabilidades de desarrollo* se pueden nombrar las inyecciones de código en SQL, Cross Site Scripting, lo que depende del tipo de aplicación y la validación de los datos.

*Las vulnerabilidades físicas* son la infraestructura física provocadas por desastres naturales, que afecten la disponibilidad del servicio, como inundaciones, sismos etc. También, se trata de los controles de acceso, en algunos casos, se logra tener los accesos a la infraestructura crítica y no se tiene los accesos pertinentes, cualquier empleado de la empresa podría abrir una puerta, podría entrar sin problemas, lo que se convierte en un gran riesgo porque cualquier persona puede ingresar a la oficina y utilizar un USB y copiar información y de igual manera infectar la misma infraestructura (Castro Romero, y otros, 2018). El tema de las vulnerabilidades ha sido investigado por muchas empresas a fin de encontrar los fallos y poder solucionarlos. De estos estudios se concluye que las vulnerabilidades se pueden clasificar en: Vulnerabilidades críticas, importantes, moderadas y de bajo impacto.

Tabla N°1: Tipos de vulnerabilidades

TIPOS DE VULNERABILIDADES			
CRÍTICAS	IMPORTANTES	MODERADA	BAJA
Este tipo de vulnerabilidad, provee la propagación de amenazas sin intervención del usuario.	Este tipo de vulnerabilidad puede poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios,	Este es uno de los tipos de vulnerabilidades más sencillas de combatir, ya que el riesgo que presenta se puede disminuir	Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta

	como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga.	con medidas tales como configuraciones predeterminadas, auditorías y demás. Aparte, las vulnerabilidades moderadas no son aprovechables en todo su potencial ya que no afecta a una gran masa de usuarios.	a una gran masa de usuarios.
--	--	--	------------------------------

Fuente: Elaboración propia basada en datos de (Marker, 2020).

En opinión de Castro Romero, y otros (2018), las vulnerabilidades también pueden producirse por el desbordamiento de buffer, esto es un error de software, sucede cuando no se controla la cantidad de datos que se copian en una memoria reservada a tal efecto (buffer). Los autores mencionados sostienen que cuando esto ocurre:

Algún intruso puede introducir su propio código en ese espacio de memoria y la máquina lo va a ejecutar antes que cualquier otra tarea, por ejemplo, eso normalmente se da mucho con los payloads, en los cuales se inyectan cierta cantidad de memoria o inclusive dentro de los backdoor o puerta trasera, los cuales inyectan en la memoria RAM un cierto o una cierta cantidad de código, el cual se arranca antes, inclusive de arrancar toda la parte del sistema operativo o de algunos de los archivos dentro del mismo sistema que se utilizan para arrancar de manera normal. (Castro Romero, y otros, 2018, p. 43)

### 1.2.2 Tipos de ataques cibernéticos devenidas de vulnerabilidades

A continuación, se muestra los tipos de ataques maliciosos que se realizan cuando se presentan vulnerabilidades.

Tabla N 2- ATAQUES Y CONSECUENCIAS CUANDO EXISTEN VULNERABILIDADES

VULNERABILIDADES	
TIPOS DE ATAQUES	DAÑOS QUE SE PRODUCEN
<b>Interrupción</b>	El daño que produce es la interrupción de servicio de red y la información no estará disponible para los usuarios.
<b>Intercepción</b>	La intercepción posibilita al atacante que acceda fácilmente al sistema, a la información almacenada o que se esté transmitiendo por la red a otros usuarios.
<b>Modificación</b>	El propósito de un ataque de modificación es interceptar y manipular la información sin estar autorizado, lo que produce enormes daños a la empresa dado que el usuario está trabajando con datos que son falsos.
<b>Fabricación</b>	Este tipo de ataque es uno de los más peligrosos, ya que ha sido diseñado para engañar al usuario cuando accede a un sitio web que cree legítimo. En este caso se crea una página web idéntica a una original, por ejemplo, el sitio de un banco, por lo cual el usuario ingresa datos personales y confidenciales que luego le son sustraídos con fines delictivos.

Fuente: (Marker, 2020).

### 1.2.3 ¿Cómo detectar vulnerabilidades en las empresas?

Siguiendo a Castro Romero, y otros (2018), una de las formas para detectar vulnerabilidades en el sistema es utilizar:

*Escáneres de vulnerabilidades*, existen algunos que son gratuitos y otros pagos. Estas son herramientas (software que realizan pruebas de caja negra) para evaluar el estado de programas y equipos informáticos con el fin de encontrar falencias de seguridad. Una vez encontradas los fallos, se clasifican para establecer un orden de prioridad teniendo presente la gravedad del asunto, la extensión del tiempo y los accesos no autorizados, para luego resolver el problema. Es preciso

destacar que estos escáneres solo otorgan información básica de los fallos del sistema, para gestionar y solucionar estas vulnerabilidades se deben buscar otros medios.

Algunos ejemplos de escáneres:

- **Acunetix:** estos se suelen aplicar para la web, muchos de ellos trabajan con proxy y a partir de ellos se realizan capturas y se pueden lograr modificaciones. Otros Acunetix están fabricados para hallar “agujeros de seguridad” en las aplicaciones web.
- **Netsparker** es un escáner pago, permite en algunos casos exportar en herramientas como Metasploit en su versión pro o exprés y a partir de ahí tener un vector de ataque más puntual.
- **ProxyStrike** este es un escáner gratuito, permite identificar inyecciones de SQL Y Cross Site Scripting.
- **LanGuard** utilizar el escáner sin tener credenciales o con las credenciales del administrador.
- **Grendel- Scan:** es una herramienta bastante completa para realizar testeos de aplicaciones web, desarrollada en Java apropiada para Windows, Linux y Mac Os. Permite encontrar fallas de inyección, SQL, XSS, CSRF, defectos de lógica y diseño.
- **Vega:** esta herramienta es de código libre de escaneo y testeos de la seguridad de aplicaciones web, permite encontrar SQL, injection, header injection, directory listing entre otras. Apropia para Mac, Linux y Windows.

Estas herramientas automáticas para hallar fallos son muy útiles, muy potentes para encontrar vulnerabilidades conocidos, además brindan muestran los niveles de riesgos y posibles exploit comunes, pero no son útiles para encontrar vulnerabilidades desconocidas, contraseñas débiles o errores de configuración, por ello las empresas usan la búsqueda manual de fallos.

**2. Búsqueda manual de vulnerabilidades:** se utiliza para encontrar fallos que no son detectadas mediante los escáneres automáticos. Sirve, por ejemplo, para las vulnerabilidades de día cero o los errores de configuración, o buscar vulnerabilidades específicas. Se realiza por medio de un ejercicio de laboratorio, este procedimiento se puede aplicar de diferentes formas. Para utilizar esta práctica se debe tener autorización del dueño del sistema. El hacking ético, relee todas las tareas que podría llegar a ejecutar un hacker malicioso, para descubrir los fallos del sistema, como paso seguido realiza un reporte sobre las fallas encontradas y los métodos que se han aplicado. La diferencia entre el hacking ético y el malicioso es que el primero es una persona contratada por la empresa y autorizado para acceder al sistema, mientras que el hacker no tiene autorización y busca robar información.

### 1.3 ¿Qué son los riesgos?

Para comprender y tener claridad sobre el concepto de riesgo, a continuación, se expondrán

algunas definiciones:

De acuerdo a la Real Academia Española (2022), el término riesgo en sentido general, supone un peligro. “Contingencia o proximidad de un daño”. Es sinónimo de fortuna, eventualidad.

Para Fernando Izquierdo Duarte: “El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos” (Izquierdo, 2005 citado por Cevallos & Naranjo Sánchez, 2021)

El riesgo implica dos elementos:

- *Incertidumbre*: es decir el suceso puede o no ocurrir.
- *Pérdida Potencial*: significa fallos, deficiencias en los sistemas derivadas de errores en el procesamiento de operaciones (Briceño Huaygua, 2019).

En conclusión, se podría decir que el riesgo en sentido general alude a un suceso que puede ocurrir o no, pero que persiste como una probabilidad a tener en cuenta porque puede afectar el futuro con consecuencias positivas o negativas puede repercutir en el cumplimiento de objetivos propuestos.

Al hablar de riesgos, existen distintos tipos de riesgos depende desde qué perspectiva se observe el fenómeno, entre ellos: riesgos laborales, riesgos políticos, financieros, informáticos etc.

### 1.3.1 Riesgo informático

En el presente, la tecnología ha ganado protagonismo en todas las áreas de la vida, en el trabajo, en el hogar, en el estilo de vida otorgando valor a todas las actividades del ser humano. Tiene una amplia utilidad: informar, entretener, intervenir en las actividades diarias. Y aunque sean herramientas muy provechosas, también, en este ámbito surgen riesgos, donde pueden ocurrir delitos informáticos. Antes de proseguir el tema, es preciso definir lo que es el riesgo informático.

El riesgo informático: “es un proceso que comprende identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentra expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia” (Giraldo García, 2016)

Cuando se trata de un riesgo informático, se refiere a la probabilidad de que ocurran sucesos que puedan dañar los activos informáticos. Los elementos que lo componen son:

1. Activos de información.
2. Amenazas.
3. Vulnerabilidades

Por lo tanto, es preciso realizar un análisis de los riesgos producidos en la empresa, a fin de gestionar adecuadamente los riesgos, y en base a los informes obtenidos aplicar las estrategias de seguridad correspondientes, eliminarlos, mitigarlos, ignorarlos o controlarlos. Pero es esencial conocer primero los distintos delitos informáticos que pueden ocurrir en una empresa.

## **2 DELITOS INFORMÁTICOS EN LA EMPRESA**

El delito informático es una actividad fraudulenta que se ejecuta en medios informáticos. En la actualidad resulta atractivo para los delincuentes infiltrarse en las redes porque la generalidad de las personas se encuentra conectados a Internet, una buena alternativa para crear negocios, extenderse a otros niveles etc. De allí que los ciber-delincuentes, se especializan en como ingresar a los ordenadores para robar información valiosa, obtener números de tarjetas o lograr transferencias bancarias a su favor. A continuación, se explicarán los delitos informáticos más frecuentes siguiendo a López Vargas y Torres Granados (2010), (Castro Romero, y otros, 2018), (Gamboa Suárez, 2020), (Briceño Huaygua, 2019)

### **2.1 Malware**

De acuerdo a López Vargas & Torres Granados (2010), algunas de las amenazas que se pueden mencionar son las siguientes:

- *Malware*: Es un software o cualquier programa o código malicioso que puede dañar el sistema. Cuando un malware entra al ordenador puede tomar el control del equipo, monitorear acciones de la empresa, vender información confiable a otras personas. Una de las formas más comunes de ingresar a una computadora es a través de archivos adjuntos de correos electrónicos no deseados o a través de descargas en línea de sitios aparentemente fiables. Los signos de estar infectado por malware se manifiestan de distintas formas: la computadora se vuelve lenta, la pantalla se llena de publicidades, anuncios que dicen; “en hora buena ha ganado una sesión gratuita con la vidente...”, los recursos del sistema funcionan anormalmente, el ventilador funciona más rápido de lo normal esto sucede porque el malware se ha apropiado de los recursos del sistema.

### **2.2 Tipos de malware**

Existen una gran variedad de malware:

- *Virus*: Según Vieites (2013) citado por Castro Romero, y otros define al virus informático,

como:

“un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o auto replicación, el cual trata de reproducirse de forma acelerada para extender su alcance” (2018, p. 15).

Existen distintos tipos de virus: Virus de sector de arranque (BOOT). Virus de archivos ejecutables. Virus de macros. Virus de lenguajes de Script. Malware.

Los virus son programas informativos maliciosos cuyo fin es alterar el funcionamiento de un computador: infectar archivos del sistema para destruir de manera intencionada datos almacenados en un equipo o red. un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático.

- **Troyanos:** un tipo de malware que se disfraza como software legítimo. Se trata de un programa o fragmento de código que tiene apariencia de legítimo. Los cibercriminales o hacker suelen emplear los troyanos para intentar acceder a los sistemas de los usuarios. Una vez activados estos malware pueden realizar varias acciones como: eliminar, bloquear, modificar, copiar datos, interrumpir el funcionamiento de la computadora o red de computadoras.
- **Spyware:** software malicioso que registra y reúne información de una computadora o red, para luego transmitirla a otro sistema externo o hacer uso de la información sin la autorización de dueño de la misma. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.
- **Ransomware:** Es programa o software malicioso extorsivo, proviene del término en inglés “ransom” que significa “rescate”. Su objetivo es impedirte usar tu computadora hasta que hayas pagado un rescate. Existen dos tipos de Ransomware: los de bloqueo, estos afectan las funciones básicas del equipo. Y los de cifrado: cifra archivos cifrados.
- **Adware:** software no deseado que muestra constantemente anuncios publicitarios en la pantalla del ordenador. Son tan molestos que impiden la navegación. También puede robar información personal, registrar sitios que el usuario visita. El fin de este software es producir ganancias a los proveedores de anuncios mostrados. Es necesario destacar que los anuncios persisten aún, cambiando de navegador porque los adwares se encuentran instalado en el sistema y esto ocurre porque vienen junto a programas que se descargan gratuitamente.
- **Botnets:** nombre genérico que denomina a cualquier grupo de ordenadores o redes de computadoras con infección de malware controlados por un atacante o grupo de cibercriminales de manera remota para realizar tareas en línea sin el permiso del usuario (Gamboa Suárez, 2020).

## 2.3 Phising

**Phising:** Es un programa malicioso enviado a víctimas, mediante correos que simulan

contener notificaciones oficiales de empresas conocidas como bancos, energía eléctrica, etc. con la mera intención de robar información, datos personales. El procedimiento de estafa o engaño consiste en que los correos enviados por estas personas contienen enlaces que se redirigen a un sitio web exclusivamente preparado por los delincuentes para solicitar de la víctima a introducir datos personales, estos correos son enviados de forma masiva para multiplicar las víctimas y exponerlos a los hackers. Estos ataques dependen en su mayoría de la curiosidad y los impulsos humanos, por lo tanto, serán difíciles de detener. Para combatir este tipo de ataques, es esencial comprender la importancia de verificar los remitentes de correo electrónico, archivos adjuntos y enlaces.

## **2.4 Ataque de inyección SQL**

**Ataque de inyección SQL** es: “un código malicioso con un lenguaje de programación de consulta estructurado, utilizado para comunicarse con las bases de datos de los servidores que almacenan información crítica para sitios web y de servicios” (Gamboa Suárez, 2020).

Su finalidad es el control y extraer datos privados tales como: nombres de usuario y contraseña, datos bancarios, números de tarjeta de crédito, entre otros. Los atacantes aprovechan las vulnerabilidades de las aplicaciones para insertar código malicioso en una base de datos mediante una instrucción SQL maliciosa, lo que le da acceso a la información confidencial contenida en la base de datos.

## **2.5 Ataque de denegación de servicio**

**Ataque de denegación de servicio:** Es un ciberataque donde el actor malicioso impide que el ordenador esté disponible para los usuarios, mediante un funcionamiento anormal. Consiste en sobrecargar o inundar la computadora con solicitudes al punto que el tráfico normal es incapaz de ser procesado. En algunos casos, estos ataques se aplican a varias computadoras al mismo tiempo. Son muy difíciles descubrir porque el atacante aparece con diferentes direcciones IP en todo el mundo (López Vargas & Torres Granados, 2010).

## **2.6 Ataque cross-site scripting**

**Ataque Cross-Site Scripting:** Este tipo de ataque persigue al usuario y no al servidor, aprovecha las carencias de seguridad en sitio web y permite que el atacante implante un script malicioso para que se pueda ejecutar automáticamente en el navegador cuando el usuario acceda a

la web, con el fin de robar credenciales (López Vargas & Torres Granados, 2010).

## 2.7 Ataque bec7eac

**Ataque BEC/EAC:** Este ataque se trata de una estafa sofisticada que se dirige a empresas y usuarios que envían solicitudes legítimas de transferencia de fondos. El intruso crea cuentas de correos con dominios similares al de las personas o enmascara su correo como legítimo con el fin de realizar transferencias de fondos no autorizadas. Aunque no siempre está asociada con una solicitud de transferencia de fondos, sino solicitar otro tipo de información sensible, como datos personales. Aunque existen varias formas para realizar este tipo de ataque, entre los más comunes se pueden mencionar:

- Mensajes de redes sociales como Twitter y Facebook.
- Archivos adjuntos en los mensajes de correos electrónicos.
- Insertar USBs, DVDs, o CDs con software maliciosos.
- Sitios Web sospechosos.
- Descargar aplicaciones o programas de internet.
- Anuncios publicitarios falsos. De acuerdo a lo anteriormente dicho, una vez que es enviado el programa malicioso el proceso de infección más común del ordenador o red es:
- El usuario descarga u un programa infectado en su computador.
- El archivo malicioso se aloja en la memoria ram de la computadora, aún si no se termina de instalar.
- El archivo malicioso infecta los archivos y programas en ejecución en ese momento.
- Al reiniciar la computadora, programa malicioso se carga nuevamente en la memoria ram y toma control del sistema operativo, lo cual hace más fácil su replicación para contaminar cualquier archivo que encuentre a su paso.

Ya instalado y propagado en el computador o red del sistema un programa malicioso puede causar grandes daños o efectos negativos en la información del usuario como:

- *Ataque de contraseña:* se trata de una prueba metódica de contraseñas y así encontrar el acceso al sistema, este ataque puede ser efectuado mediante: 1- el uso de diccionario de palabras, esta forma se trata de probar una y otra vez recurriendo a palabras de diccionario, 2- por fuerza bruta, esta forma aplica combinaciones de letras, números y símbolos para encontrar la contraseña del usuario.
- *Fraude informático:* se trata del perjuicio económico hacia una víctima a través de un sistema informático, introduciendo datos incorrectos o verdaderos que pueda engañar la seguridad del

sistema.

- *Acceso a información confidencial.* Esto puede ocurrir cuando el personal autorizado deja involuntariamente copias de información confidencial en las impresoras y son documentos que pueden llegar a manos de personas de limpieza u otras personas no autorizadas.
- *Daños físicos al equipamiento.* Estos daños se producen por actitudes intencionales, errores de los usuarios, por ejemplo, derrames de líquidos, por caídas etc. por tanto se debe resguardar el equipo, colocarlos en lugares seguros y no donde hay mucho movimiento y pueda ser rosado al pasar (López Vargas & Torres Granados, 2010).

## 2.8 Robo de identidad

*Robo de identidad:* esto ocurre cuando los intrusos utilizan la identidad de otras personas, para utilizar sus tarjetas de crédito, acceder a información bancaria y cometer sus fraudes

## 2.9 Trashing

*Trashing:* se trata de buscar información en la papelera de reciclaje. La información relevante que no se elimina de la papelera puede ser fácilmente hallada por otras personas y esto representa una amenaza para la empresa (Briceño Huaygua, 2019).

# 3. POLÍTICAS DE SEGURIDAD INFORMÁTICA

## 3.1 Definición

De acuerdo a Caurín (2014) Las políticas de seguridad: “son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa” (s. pág.). Se trata del diseño de una planeación para eliminar todos los riesgos que sufre una empresa u organización.

Para la Organización Inca, una política de seguridad informática es:

Una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización. No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el porqué de ellos, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal. (2020, p. 5).

De las definiciones expuestas se podría decir que las políticas de seguridad informática un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa, son mecanismos que tienen como principal objetivo proteger la información y concientizar a los usuarios de su importancia.

### 3.2 Aspectos que se consideran en las políticas de seguridad

Al momento de formular las políticas de seguridad informática se debe tener presente lo siguiente:

- **Realizar un análisis de riesgos informáticos** y ajustar las políticas a la realidad de la empresa y el valor de los activos.
- **Reunirse con los departamentos dueños de los recursos** para determinar el alcance y definir las violaciones a las prácticas.
- **Comunicar a todo el personal sobre el desarrollo de las políticas**, incluyendo los beneficios, riesgos relacionados con los recursos, bienes, y elementos de seguridad.
- **Determinar la persona que tendrá la autoridad para tomar decisiones en cada departamento**, pues son ellos los interesados en salvaguardar los activos críticos de su área.
- **Monitorear periódicamente los procedimientos y operaciones de la empresa**, con el fin de que las políticas puedan estar siempre actualizadas.
- **Determinar el alcance de las políticas** con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas (Caurín, 2014).

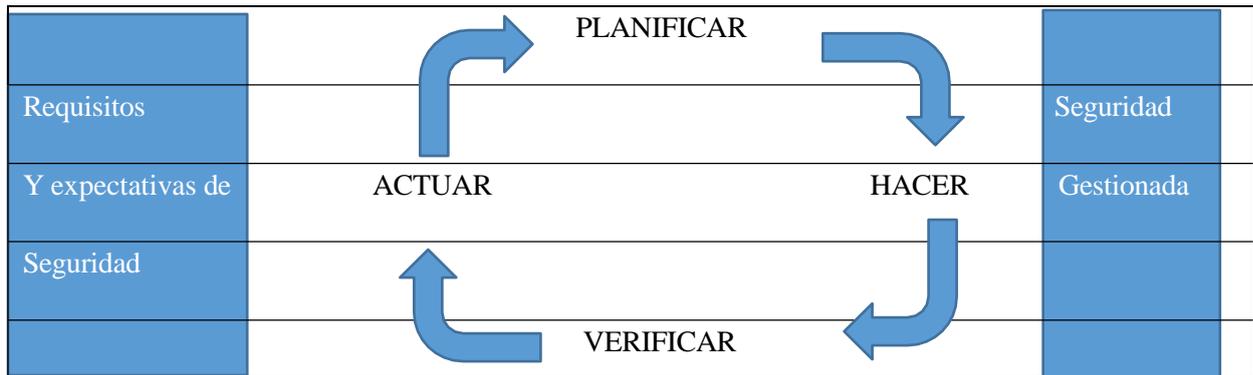
### 3.3 ¿Que protege la seguridad informática?

El objetivo principal de esta tarea es impedir la manipulación de datos y de los sistemas informáticos por terceras personas no autorizadas o sea proteger toda la tecnología y sus datos dentro de las empresas contra daños y amenazas.

¿Cómo se establece un sistema de seguridad informática?

Continúa en pág. siguiente...

Ilustración N°7 Organizar de la Seguridad informática



Fuente: (Metodología para la gestión de la seguridad informática, 2013)

- **Planificar:** Son procesos de seguridad necesarios para evitar riesgos y obtener mejoras en el área de seguridad, logrando así los resultados esperados.
- **Hacer:** De esta forma se garantiza una correcta aplicación de los controles.
- **Verificar:** Significa evaluar, verificar los distintos procesos, y reportar los resultados, para su verificación.
- **Actuar:** Son las acciones correctivas y preventivas propias de toda Gestión de Seguridad, en base a los datos obtenidos por el sistema de verificación y así lograr una mejora continua.

Toda política de seguridad informática tiene como objetivo proporcionar apoyo y orientación a los directivos para obtener seguridad en sus empresas respetando las regulaciones y leyes vigentes.

Toda política de Seguridad va a definir: qué es lo que debe ser protegido, qué es lo más importante y más prioritario para la empresa y qué es lo que no está permitido. También tiene en cuenta las correcciones a realizar para obtener una mejora continua en el sistema de Gestión.

Toda política de seguridad debe considerarse como una estrategia central dentro de la empresa, no se debe conceder medidas o procedimientos que no respondan a esta política, cada medida que se tome por la empresa, así como cada procedimiento debe estar inmerso dentro de la política de seguridad.

Afectando no solamente los procesos sino también el capital humano que se requiera para llevar a cabo dicho propósito, es por ello que es conveniente tener un nivel de autoridad dentro de la empresa para control y seguimiento de todo el proceso incluyendo el personal.

Es por ello que toda política de seguridad debe estar avalada por la máxima autoridad, para que por ello tenga facultad tanto para implementar como para hacer cumplir dicha política (Metodología para la gestión de la seguridad informática, 2013).

Toda buena política de seguridad debe:

- 1- Definir las áreas de responsabilidad de todos los usuarios, incluidos los administrativos y directores.
- 2- Contar con herramientas necesarias que respalden las exigencias de las normativas a cumplir, y llegado el caso si es necesario aplicar sanciones correspondientes.
- 3- Implementar las distintas medidas de prevención y procedimientos por medio de publicaciones, utilizando todos los medios disponibles para ese fin.

Toda política de seguridad debe dar respuesta a los posibles interrogantes que se presentarán:

- ¿Qué estrategia se utilizará para lograr la seguridad informática?
- ¿Quiénes podrán hacer uso de los recursos informáticos?
- ¿Quién es la persona autorizada para permitir acceso al recurso informático?
- ¿Cómo sé que estoy haciendo un uso correcto del recurso informático?
- Derechos y responsabilidades de los usuarios.
- Información clasificada ¿Qué hacer con ella?, ¿Quiénes pueden tener libre acceso a ella?
- ¿Cómo actuar frente a un incidente de seguridad informática?

Toda información que se procesa y almacena en la empresa estarán custodiados por los directores o coordinadores, quienes utilizan dicha información. Aun cuando ellos puedan delegar, a personal idóneo y de confianza su uso, nunca dejaran de ser los máximos responsables de su utilización frente a la empresa.

Dicha asignación de responsabilidad de la información debe estar debidamente documentada, y es muy saludable y práctico contar con un acuerdo de confidencialidad y de no divulgación con el objetivo de salvaguardar la información de valor que la empresa maneja.

Es menester que dicho acuerdo sea firmado por todo personal involucrado en el manejo del sistema informático con el objetivo de obtener mayor capacitación, mejor asesoramiento y de intercambio de experiencia muchas veces es necesario el contactarse con otras empresas u organismo que realice similar tarea, y que también cuenten con personal especializado para lograr un excelente intercambio de información sobre el tema. De esa manera se provee al personal involucrado de una continua capacitación, a través de foros, eventos, reuniones, etc. (Metodología para la gestión de la seguridad informática, 2013)

En caso de contar con personal que trabajen a distancia utilizando dispositivos móviles (laptop, notebooks, tabletas, teléfonos celulares y otros.), y que dichos dispositivos deben contar con información sensible, deben tales dispositivos contar con medidas de seguridad adecuada, para evitar toda filtración de datos sensibles por medio de manipulaciones maliciosas, o en caso de

hurto.

Procedimiento que garantizan el cuidado de información sensible:

- Contar con un sistema de anulación de cualquier software malicioso.
- Cifrar las comunicaciones sensibles impidiendo su libre acceso.
- Contar con una central quien monitoree toda información que se está consultando en el momento.
- Contar con un mecanismo que en caso de robo /hurto, se le impida el acceso a información de privilegio.
- El poseedor del dispositivo en cuestión, debe contar con un sistema de alerta inmediata a la central para el bloqueo total de dicho dispositivo.
- Es conveniente notificar a todo el grupo de tarea del incidente ocurrido.
- Siempre es conveniente realizar auditoria o monitoreo de las actividades realizadas por cada dispositivo.

Pautas a tener en cuenta para el personal que trabaje a distancia.

- Su trabajo a distancia debe estar lo más claramente especificado por sus superiores, ya sea tema a tratar, horarios, información necesaria de consultar, y el tipo de información al cual se le es permitido acceder.
- Determinar si terceras personas están autorizadas a dar uso de su dispositivo.
- Cuando finalice su tarea debe reintegrar el dispositivo para su examinación/auditoria.

### **3.4 Aspectos que afectan la seguridad**

Muchas veces las medidas de seguridad se ven afectadas por:

- Falta de mantenimiento en el software de tus equipos informáticos.
- Los empleados: el factor humano en una empresa es uno de los puntos más débiles dentro de los delitos informáticos.
- Las contraseñas: estas deben ser seguras, combinaciones de mayúsculas y minúsculas, números y símbolos, etc.
- Hacer uso del modo incognito: evita que se guarden contraseñas e historial de navegación.
- Diferentes contraseñas para diferentes áreas de navegación.

Es por ello que siempre se aconseja:

- Evaluar en forma constante el estado de la seguridad informática.

- Continua evaluación de riesgos.
- Contar con un buen plan de seguridad informática.
- Concientizar a los empleados.
- Encriptar los datos.
- Realizar copias de seguridad.
- Contar con antivirus y cortafuegos actualizados.

### **3.5 Medidas de seguridad informática**

De acuerdo a Martínez Sánchez, la seguridad informática es una necesidad en la actualidad para protegerse de los frecuentes ataques informáticos. El autor sostiene:

La protección de la información tiene que ser una de las prioridades de cualquier departamento de TI. Sin embargo, hay indicios que muestran que las organizaciones no se están protegiendo de la manera adecuada. De acuerdo con los datos compilados por Kaspersky Lab y por la agencia B2B International, el 82% de las compañías ha implementado protección de malware. Así mismo, el 80% tienen instaladas medidas contra el spam. Pero solo dos de cada cinco organizaciones usan tecnologías verdaderamente eficientes para protegerse contra las amenazas corporativas (2021, p. 2).

A continuación, siguiendo a este autor, se explicarán las medidas de seguridad que una empresa debería tener.

#### **3.5.1 Antivirus**

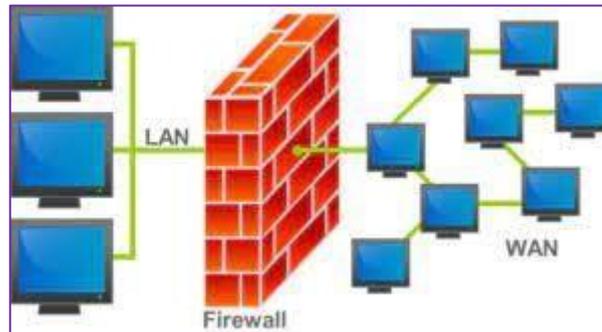
Una de las primeras medidas que se conocen para resguardar la seguridad de un ordenador es la instalación de un antivirus. Este es un tipo de software que se utiliza para evitar, detectar y eliminar virus, una vez instalado se ejecutan automáticamente en segundo plano o bien utilizarlo periódicamente para revisar y desinfectar la PC. Es preciso que siempre el programa se encuentre actualizado, dado que cada día aparecen nuevos virus.

El antivirus ayuda a resguardar archivos de Hardware de malware, como troyanos, gusanos, programas maliciosos, además proteger al sistema de bloqueos de sitios web.

#### **3.5.2 Cortafuegos**

Un cortafuego o “firewall” en inglés, es un software destinado a bloquear accesos no autorizados a un ordenador, garantizar la seguridad en las comunicaciones vía Internet y restringir la salida de información.

Ilustración N°8 Cortafuego



Fuente: <https://www.islabit.com/105707/cortafuegos-de-hardware-y-software-estas-son-las-diferencias.html>

Existen dos tipos de matabuegos: Los firewalls de hardware y los Firewall de software o combinación de ellos. Los primeros requieren se encuentran incluidos en algunos enrutadores, tienen poca o ninguna configuración, estos se ocupan de monitorear el tráfico de todas las computadoras y dispositivos conectados a la red de dicho enrutador, protege al sistema de amenazas externas. El firewall de software es más completo, examina más profundamente los datos y bloquea el envío de programas específicos. Se recomienda utilizar ambos firewalls para una completa seguridad.

### 3.5.3 Actualizar las aplicaciones con los “parches de seguridad”

Son frecuentes que en las empresas se presenten vulnerabilidades en los programas informáticos más utilizados (navegadores de Internet, procesadores de texto, programas de correo, etc.) lo cual produce una oportunidad de ataque por parte de los creadores de virus. Para evitarlo, se tienen que actualizar las aplicaciones para restaurar el sistema y dar mejoras en su funcionamiento.

### 3.5.4 Software Legal

Es sumamente importante que se instale un software legal, proveniente de una fuente conocida y fiable, Además de transgredir la Ley, pueden contener virus, spyware o archivos de sistema incompatibles con los de su ordenador, lo cual provocará inestabilidad en su equipo. También es necesario no confiar en los archivos gratuitos que se descargan de sitios Web



desconocidos, ya que estos pueden ser una vía de propagación de virus. En cualquier caso, debe analizar con el antivirus.

En resumen, toda empresa tiene que tener en cuenta la importancia de tener una buena seguridad informática que resguarde los activos de la misma. Tener conocimiento de cuáles pueden ser las amenazas a las que pueden estar expuestos, las vulnerabilidades y los riesgos que se presentan en la red. Para luego hacer un diagnóstico de las amenazas y planear una seguridad informática que contemple los problemas informáticos que atenten contra la compañía.



**CAPÍTULO III**  
**TRABAJO DE CAMPO, ANÁLISIS E INTERPRETACIÓN**  
**DE DATOS**

## 1. INTRODUCCIÓN

El presente capítulo refleja el trabajo de campo realizado y los datos recolectados que son analizados e interpretados a fin de conocer la situación de las empresas mendocinas con respecto a la seguridad informática y su gestión.

### 1.1 Universo y muestra

Para iniciar este desarrollo es conveniente considerar algunos conceptos como universo y muestra. De acuerdo a Hernández Sampieri, Collado, & Baptista Lucio (2006), el universo se refiere al conjunto total de elementos, individuos, objetos, eventos relevantes para la investigación y que posea una o más características en común. En otras palabras, el universo es el conjunto completo de todas las unidades de análisis que se consideran en la investigación y que cumplen con los criterios de inclusión establecidos.

Y la muestra se refiere a una parte o subconjunto del universo o población de interés que se selecciona para ser estudiada en la investigación. Dicho de otra forma, la muestra es un grupo de individuos, objetos, eventos o unidades de análisis que se consideran representativos del universo y que se utiliza para hacer inferencias sobre el mismo (Hernández Sampieri, Collado, & Baptista Lucio, 2006). Para el siguiente trabajo de campo se tuvo presente un universo de 34.665 pymes, datos extraídos del Ministerio de la Producción de la Nación de la provincia de Mendoza. Y para seleccionar la muestra se escogió un muestreo no probabilístico por conveniencia.

Como resultado, la muestra elegida quedó constituida por 30 empresas de la ciudad de Mendoza para la investigación de los siguientes objetivos planteados:

- Determinar el porcentaje de ataques cibernéticos que afectan significativamente a las empresas de Mendoza
- Describir los principales factores que posibilitan la consecución de los ataques.
- Enumerar y explicar los tipos de ataque que sufren las empresas de Mendoza.
- Obtener de los dueños de las empresas de Mendoza una descripción de las estrategias adoptadas para afrontar los ataques cibernéticos.
- Investigar qué estrato de las empresas se ve más afectado por los delitos informáticos.

## 1.2 Instrumento de medición

Para reunir los datos estadísticos se emplea como instrumento de medición una encuesta semiestructurada constituida por preguntas en su mayoría cerradas y algunas abiertas. La investigación se realizó en los meses de enero a abril de 2023, en la ciudad de Mendoza, Argentina. Cabe destacar que en primer momento se eligieron 40 empresas pymes para realizar la investigación, pero no hubo respuesta positiva, por tanto, se redujo el número a 30 empresas disponibles.

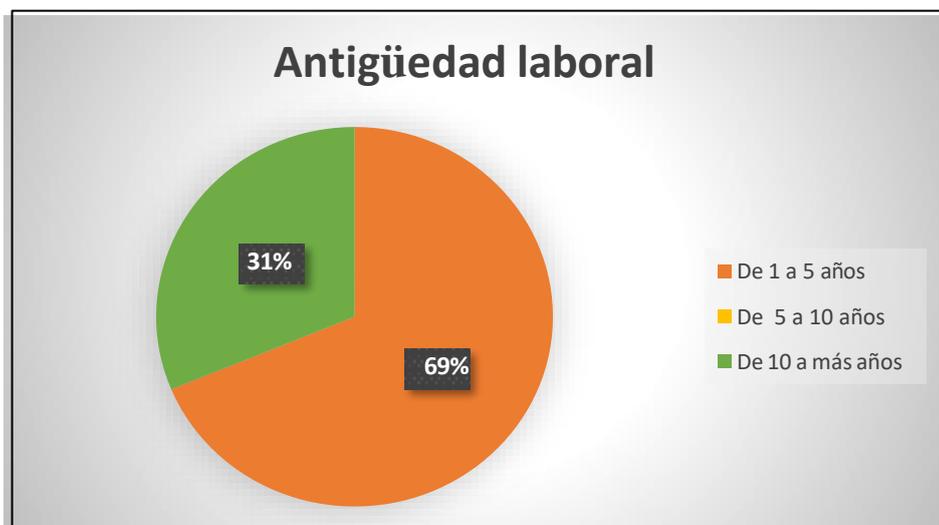
## 1.3 Resultados e interpretación de datos

### 1.3.1 ¿Cuántos años lleva trabajando en la empresa?

Tabla N°1: Antigüedad laboral

ANTIGÜEDAD LABORAL	EMPRESAS CONSULTADAS	PORCENTAJE
De 1 a 5 años	22	69 %
De 5 a 10 años	0	0 %
De 10 a más años	8	31%
<b>TOTAL</b>	<b>30</b>	<b>100 %</b>

Gráfico N°1: Años de trabajo en la empresa.



De los datos recolectados, el gráfico demuestra que el 69% de los encuestados tienen entre

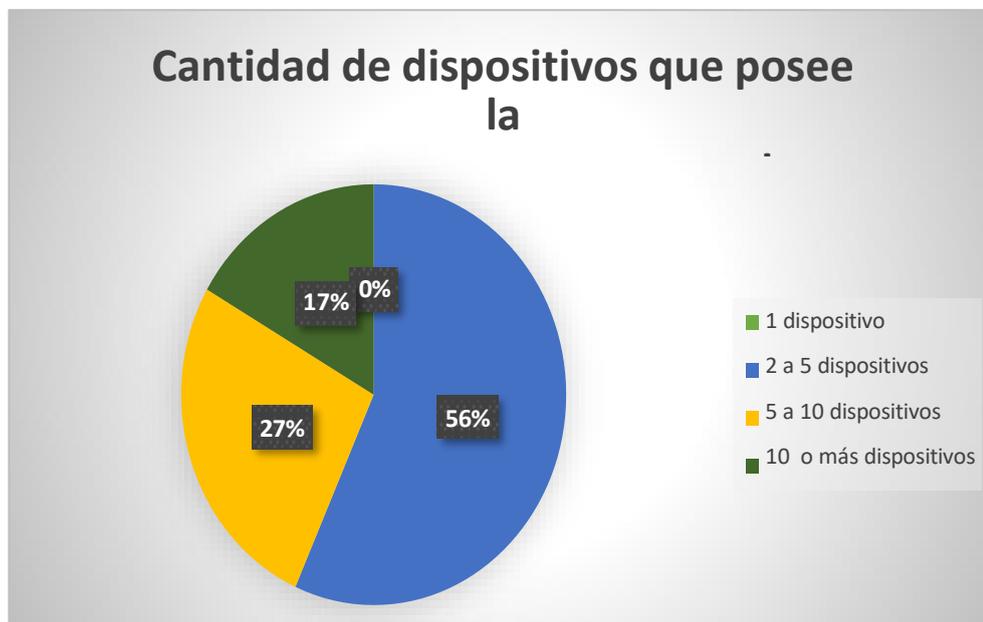
1 a 5 años de antigüedad y un 31 % tiene de 10 a más años.

### 1.3.2 Actualmente en su empresa cuantos dispositivos aproximadamente se conectan

Tabla N°2: Cuántos dispositivos se conectan en la red.

DISPOSITIVOS QUE SE CONECTAN A LA RED EN LA EMPRESA	EMPRESAS CONSULTADAS	PORCENTAJES
1 dispositivo	0	0 %
2 a 5 dispositivos	17	56 %
5 a 10 dispositivos	8	27 %
10 a más dispositivos	7	17 %
<b>Total</b>	<b>30</b>	<b>100</b>

Gráfico N°2: Dispositivos que se conectan a la red en la empresa



De los datos recolectados se supo que el 56 % de las empresas poseen entre 2 a 5 dispositivos, un 27 % de las empresas tienen entre 5 a 10 dispositivos, un 17 % de las empresas entre 10 o más dispositivos conectados a la red.

### 1.3.3 ¿La empresa posee un departamento para Seguridad Informática?

Tabla N°3: ¿La empresa posee un departamento de Seguridad Informática?

¿LA EMPRESA POSEE UN DEPARTAMENTO PARA SEGURIDAD INFORMATIVA	EMPRESAS CONSULTADAS	PORCENTAJE
No	24	80 %
Sí	6	20 %
Total	30	100 %

Gráfico N°3: ¿La empresa posee un departamento de Seguridad Informática?



De acuerdo a la recolección de los datos se supo que el 80 % de las empresas consultadas no posee un departamento de Seguridad Informática y 20 % de ellas, sí los tiene.

### 1.3.4 ¿La empresa donde Usted trabaja ha tenido ataques cibernéticos?

Tabla N°4: ¿La empresa donde trabaja Ud. ha tenido ataques cibernéticos?

¿LA EMPRESA DONDE TRABAJA UD. HA TENIDO ATAQUES CIBERNÉTICOS?	EMPRESAS CONSULTADAS	PORCENTAJES
Sí	22	73 %

No	8	27 %
<b>Total</b>	<b>30</b>	<b>100%</b>

Gráfico N°4: ¿Su empresa ha tenido ataques cibernéticos?



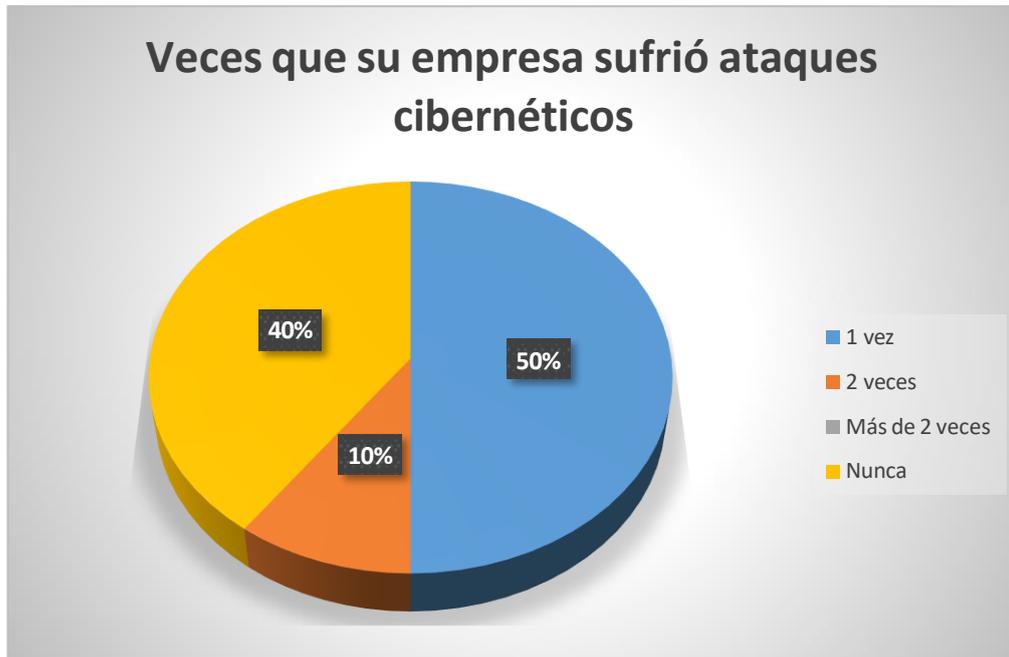
De los datos recolectados se conoció que un 73 % de las empresas encuestadas ha tenido ataques cibernéticos y un 27 % no los tuvo.

### 1.3.5 ¿Cuántas veces la empresa ha sufrido ataques cibernéticos significativos en los últimos 5 años?

Tabla N°5: Cantidad de veces que la empresa ha sufrido ataques cibernéticos en los últimos 5 años

CANTIDAD DE VECES QUE LA EMPRESA HA SUFRIDO ATAQUES CIBERNÉTICOS EN LOS ÚLTIMOS 5 AÑOS	EMPRESAS CONSULTADAS	PORCENTAJES
1 vez.	15	50 %
2 veces	3	10 %
Más de 2 veces	0	0 %
Nunca	12	40 %
<b>TOTAL</b>	<b>30</b>	<b>100 %</b>

Gráfico N°5: Cantidad de veces que la empresa ha sufrido ataques cibernéticos en los últimos 5 años.



De los datos recolectados se supo que el 50 % de las empresas encuestadas tuvo 1 ataque cibernético significativos en los últimos 5 años, un 40 % de las empresas mencionó que no tuvo ataques cibernéticos en los últimos años, y un 10 % de las empresas sostienen que solo 2 veces tuvieron un ataque cibernético significativo.

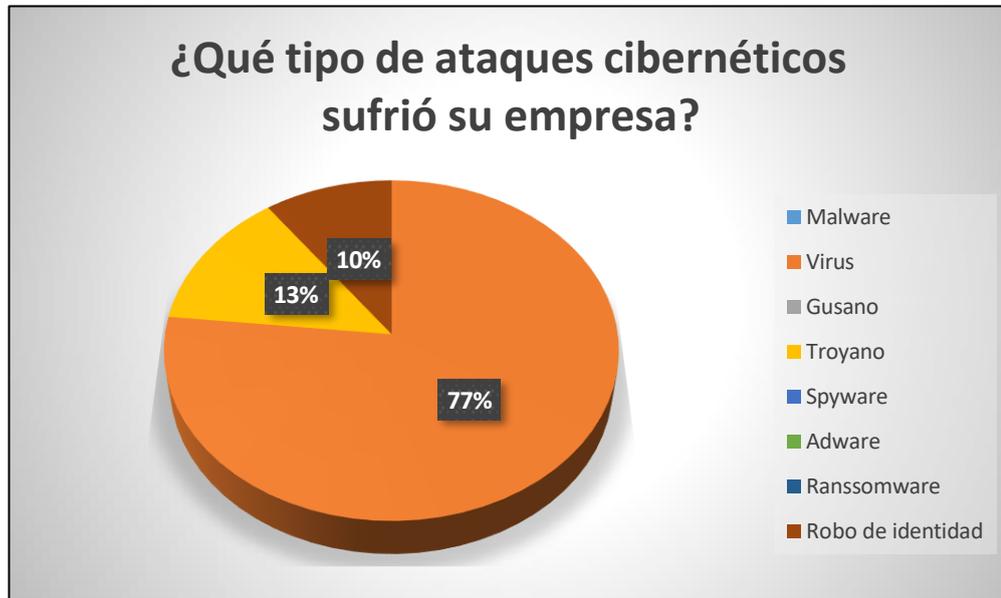
**1.3.6 ¿Cuál fue la estrategia que utilizaron los delincuentes para afectar la seguridad informática? ¿Y cuál fue el estrato de la empresa que fue afectado?**

Tabla N°6: Tipo de ataque que sufrió su empresa

TIPO DE ATAQUE QUE SUFRIÓ SU EMPRESA	EMPRESAS CONSULTADAS	PORCENTAJES
Malware	0	21 %
Virus	23	60 %
Gusano	0	0 %
Troyano	4	11 %
Spyware	0	0 %
Adware	0	0%
Ranssonware	0	0%

Robo de identidad	3	8 %
<b>TOTAL</b>	<b>30</b>	<b>100%</b>

Gráfico N°6: Tipo de ataque que sufrió su empresa



De acuerdo al gráfico, se supo que el 60% de las empresas encuestadas fueron atacadas por virus, un 21 % por malware, 11 % por troyanos y un 8 % de las empresas hubo robo de identidad.

En la segunda pregunta de este Ítem, de tipo abierta, donde se indaga que extracto de la empresa es afectado las respuestas se colocan en orden teniendo en cuenta su prevalencia y coincidencia:

- El área afectada fue la administrativa.
- La dirección mails.
- La calificación de la empresa por parte de los clientes.

**1.3.7 ¿Después de los ataques se tomaron medidas de seguridad informática? ¿Cuáles?**

Tabla 7: Medidas de prevención

¿SE TOMARON MEDIDAS DE PREVENCIÓN?	EMPRESAS CONSULTADAS	PORCENTAJES

Sí	16	53%
No	14	47%
TOTAL	30	100%

Gráfico N°7: ¿Se tomaron medidas de prevención?



De acuerdo a los datos recolectados se supo que el 53% de las empresas encuestadas tomaron prevención, pero se puede observar que un alto porcentaje, un 47% de las empresas no tomó medidas al respecto.

La segunda pregunta realizada en este ítem, es de tipo abierta. Las respuestas se colocan según prevalencia y coincidencia:

- Backup externo, cortafuegos, contraseñas
- Ninguna
- No se
- Se educó a los empleados en materia de ciberseguridad y para actuar en contra de las amenazas online, incluyendo la utilización de contraseñas unipersonales y seguras. No insertar más pen drives en las computadoras, solo descargamos archivos por correo electrónico.

Gráfico N°7: ¿Se tomaron medidas de prevención?



De acuerdo a los datos recolectados se supo que el 53% de las empresas encuestadas tomaron prevención, pero se puede observar que un alto porcentaje, un 47% de las empresas no tomó medidas al respecto.

La segunda pregunta realizada en este ítem, es de tipo abierta. Las respuestas se colocan según prevalencia y coincidencia:

- Backup externo, cortafuegos, contraseñas
- Ninguna
- No se
- Se educó a los empleados en materia de ciberseguridad y para actuar en contra de las amenazas online, incluyendo la utilización de contraseñas unipersonales y seguras. No insertar más pen drives en las computadoras, solo descargamos archivos por correo electrónico.

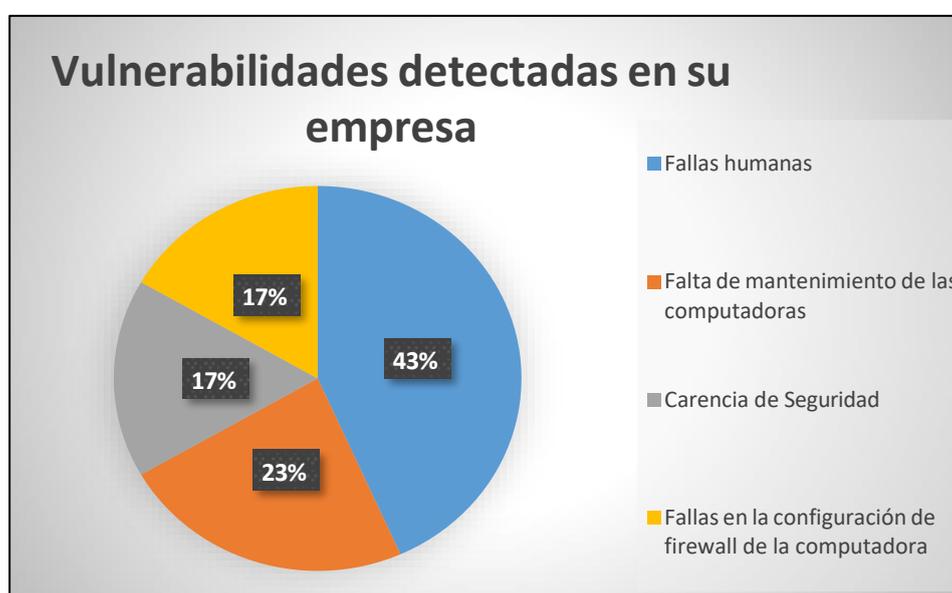
### 1.3.8 ¿Cuáles han sido las vulnerabilidades detectadas en la empresa que propiciaron ataques cibernéticos?

Tabla N°8: Vulnerabilidades de la empresa que propiciaron los ataques cibernéticos

VULNERABILIDADES DE LA EMPRESA QUE PROPICIARON LOS ATAQUES CIBERNÉTICOS	EMPRESAS CONSULTADAS	PORCENTAJES
---	----------------------	-------------

Fallas humanas	13	43 %
Falta de mantenimiento de las computadoras	7	23 %
Carencia de Seguridad	5	17%
Fallas en la configuración de firewall de la computadora	5	17%
<b>TOTAL</b>	<b>30</b>	<b>100%</b>

Gráfico N°8: Vulnerabilidades de la empresa que propiciaron los ataques cibernéticos



De la recolección de los datos se supo que hubo varias vulnerabilidades que propiciaron los ataques cibernéticos: el 43 % de las empresas encuestadas mencionaron que fueron las fallas humanas, un 23 % de las empresas mencionó falta de mantenimiento de las computadoras, un 17 % la carencia de Seguridad Informática, un 17 % la falta de fueron las fallas en la configuración del firewall de la computadora.

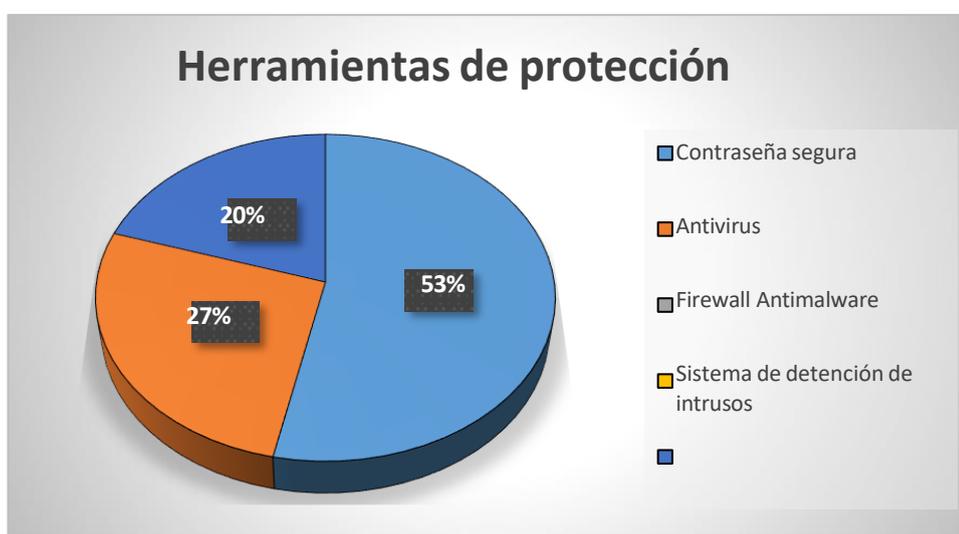
### 1.3.9 ¿La empresa utiliza alguna de las siguientes herramientas para mantener segura su red?

Tabla N°9: Herramientas de protección

HERRAMIENTAS DE PROTECCIÓN	EMPRESAS CONSULTADAS	PORCENTAJES
Contraseña segura	16	53 %

Antivirus	8	27 %
Antispyware	0	0 %
Antimalware	0	0 %
Sistema de detención de intrusos.	6	20 %
Otro	0	0%
<b>TOTAL</b>	<b>30</b>	<b>100%</b>

Gráfico N°9: Herramientas de protección



De los datos recolectados, se supo que el 53% de las empresas encuestadas utilizan contraseñas seguras, el 27 % de las empresas menciona que emplea como herramienta de protección un antivirus y un 20 % utiliza un sistema de detención de intrusos.

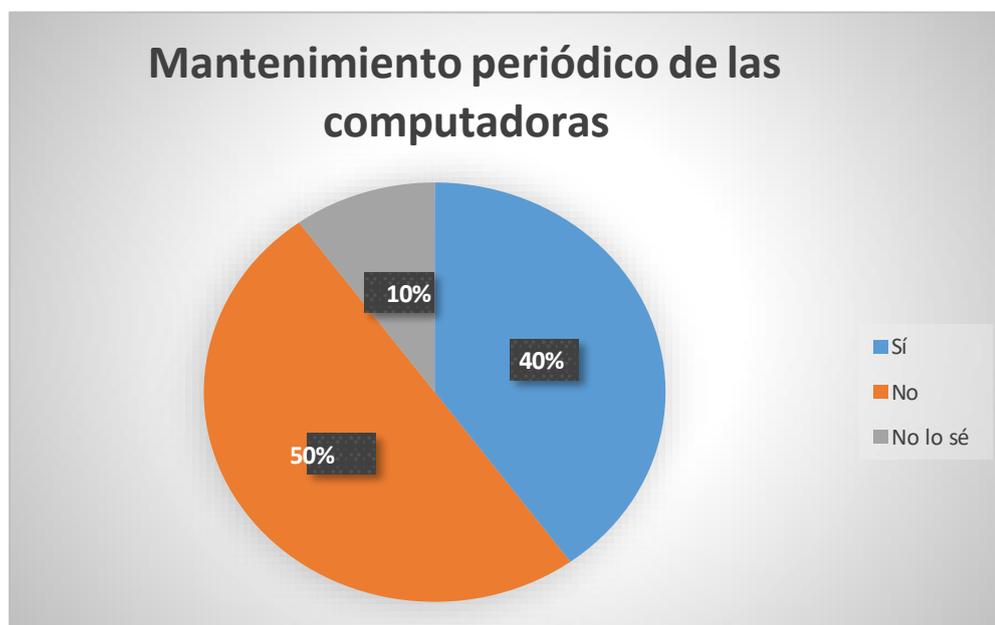
### 1.3.10 ¿Se realizan mantenimientos periódicos de las computadoras de la empresa?

Tabla N°10: Mantenimientos periódicos de las computadoras

MANTENIMIENTO PERIÓDICOS DE LAS COMPUTADORAS	EMPRESAS CONSULTADAS	PORCENTAJES
Sí	12	40 %
No	15	50 %

No lo sé	3	10 %
<b>TOTAL</b>	<b>30</b>	<b>100%</b>

Gráfico N°10: Mantenimientos periódicos de las computadoras



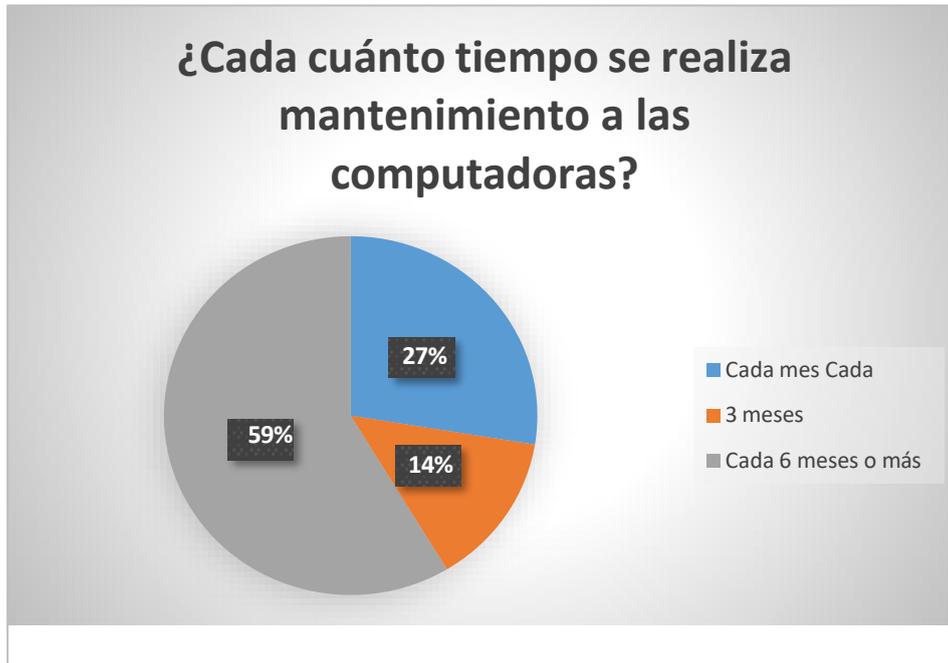
De la recolección de los datos, se supo que el 50 % de las empresas consultadas han respondido que realizan mantenimientos periódicos de sus computadoras, el 40 % no los realiza periódicamente y el 10 % de las empresas consultadas respondieron que no lo saben.

### 1.3.11 ¿Cada cuánto tiempo se realiza el mantenimiento?

Tabla N°11: ¿Cada cuánto tiempo se realiza el mantenimiento?

¿CADA CUÁNTO TIEMPO REALIZA EL MANTENIMIENTO DE LAS COMPUTADORAS?	EMPRESAS CONSULTADAS	PORCENTAJES
Cada mes	8	27 %
Cada 3 meses	5	14 %
Cada 6 meses o más	17	59 %
<b>TOTAL</b>	<b>30</b>	<b>100%</b>

Gráfico N°11: ¿Cada cuánto tiempo se realiza el mantenimiento?



De los datos recolectados se supo que las empresas consultadas, el 59 % de ellas realiza el mantenimiento cada 6 meses o más, que 27 % lo realiza cada mes y un 14 % lo lleva a cabo cada 3 meses.

### 1.3.12 ¿Se realizan pruebas de seguridad en la red?

Tabla N°12; Pruebas de seguridad informática en la red

¿SE REALIZAN PRUEBAS DE SEGURIDAD INFORMÁTICA EN LA RED?	EMPRESAS CONSULTADAS	PORCENTAJES
Sí	12	43 %
No	16	57 %
No lo sé	0	0 %

TOTAL	30	100%
-------	----	------

Gráfico N°12: Pruebas de seguridad en la red.



De acuerdo al gráfico se supo que el 57 % de las empresas encuestadas, no se realizan pruebas de seguridad en la red, y solo un 43 % realiza pruebas de seguridad en la red.

#### ACCIONES PREVENTIVAS A CONSIDERAR

Teniendo en cuenta los resultados extraídos de los datos se recomienda implementar y reconocer la necesidad de una cultura de seguridad informática para incorporar nuevas actitudes de cuidado y responsabilidad hacia el manejo de los recursos informáticos. Y con este propósito, realizar charlas educativas al respecto al menos dos veces al año y afianzar la responsabilidad y fidelidad de los empleados a la empresa, evitando de esta manera, que se conviertan en cómplices de aquellos delincuentes que busquen ingresar al sistema para robar información o datos de importancia. Considerar temas que instruyan a los empleados sobre los posibles peligros que surgen de no mantener copias de seguridad, los nuevos virus y métodos que surgen para violar la seguridad informática, la necesidad de mantener actualizados los antivirus,

Por otra parte, para tener mayor resguardo de la seguridad informática es muy preciso



invertir fondos para incorporar un departamento de seguridad informática, que se ocupe de implementar una buena política de seguridad, determine las áreas de responsabilidad de los usuarios, incluyendo a administrativos y directores, proporcionar herramientas necesarias para el cumplimiento de las normativas a cumplir y pueda definir medidas de prevención y realizar los debidos controles.

Otras de las acciones que suelen ser muy provechosas suelen ser exponer cartelerías que motiven a los empleados al cuidado y responsabilidad en el uso de recursos informáticos.

## CONCLUSIONES

En la actualidad, la mayoría de las empresas utilizan sistemas informáticos para almacenar su información sensible y para ello se emplean sistemas de redes interconectadas para funcionar, organizar, procesar, analizar información, obtener mayor visibilidad de los datos, vender o promocionar un producto. De allí que resulta sumamente importante resguardar la información y gestionar debidamente una seguridad informática.

En el presente estudio, después de haber ejecutado el correspondiente relevamiento de los datos se concluye que las empresas consultadas en su mayoría no cuentan con un departamento de Seguridad Informática y el porcentaje de los ataques cibernéticos a las empresas mendocinas son bastante altos, un 73 %.

Así mismo se ha descubierto que los tipos de ataques que son frecuentes en la mayoría de empresas son: infección de virus, troyanos y robo de identidad, los factores que posibilitan estos ataques, provienen mayoritariamente de fallas humanas, lo cual refleja una escasa concientización acerca de las medidas de prevención.

Para una organización o entidad, la información es vital, una fuga de ella puede causar la destrucción de la misma, esto requiere no solo de charlas sino lograr una cultura organizacional que fundamente y sostenga una política de seguridad informática. Por otro lado, las empresas descuidan el mantenimiento de las computadoras y se registraron fallas en la configuración del firewall.

También se supo que las áreas más afectadas por los ataques cibernéticos son la parte administrativa, los mails y la calificación de los clientes. Lo alarmante de esta situación radica que las medidas de prevención son mínimas como, por ejemplo, empleo de antivirus, contraseñas seguras y en muy pocas empresas recurren a la educación de los empleados sobre seguridad informática.

De esta manera, se comprueba que el impacto de los ataques a las organizaciones se debe a la falta de una buena gestión de seguridad informática y también se observa que hay disminución de riesgos en empresas que concientizan a su personal del cuidado de la información y gestión de seguridad.

Resta mencionar que frente a los avances de las tecnologías y nuevas formas de estafas se necesita estar siempre informados y tener conocimientos sobre las nuevas estrategias de los delincuentes para contrarrestar sus ataques.

## BIBLIOGRAFÍA

- Samaniego Mena, E., & Ponce Ordóñez, J. (2021). *Fundamentos de Seguridad Informática*. Guayaquil: Grupo Compás
- AMBIT. (2020). *¿Conoces todos los sistemas de almacenamiento de datos?* AMBIT. consultores en tecnología. <https://www.ambit-bst.com/blog/conoces-todos-los-sistemas-de-almacenamiento-de-datos#:~:text=El%20almacenamiento%20de%20datos%20es,otra%20informaci%C3%B3n%20en%20formato%20digital>.
- Argentina, gob, ar. (s.f.). *PYME*. <https://www.argentina.gob.ar/produccion/registrar-una-pyme/que-es-una-pyme>
- Arroba system. (2021). *¿Qué son las amenazas informáticas y cómo protegerte de ellas?* Blog Arroba System. <https://arrobasystem.com/blogs/blog/que-son-las-amenazas-informaticas-y-como-protegerte-de-ellas>
- Barzanallana, R. (s.f.). *Gestión de la seguridad en sistemas de la información*. UMU. <https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf>
- Bernardi, S., & Dranca, L. (2020). *Sistema de Información para la Dirección*. Zaragoza: Edelvives Talleres Gráficos.
- Briceño Huaygua, C. (2019). *Aplicación de la metodología Magerit para la elaboración de un plan de seguridad de los activos de información de la zona especial de desarrollo*. Zed Paita. Tesis de grado, UNIVERSIDAD NACIONAL DE PIURA Piura, Perú
- Bustamente, M. (2020). *Cultura en Seguridad Informática*. CEUPE - Centro Europeo de Postgrado. <https://posgradosadistancia.com.ar/cultura-en-seguridad-informatica/>
- Cardona Arboleda, O. (2001). ESTIMACIÓN HOLÍSTICA DEL RIESGO SÍSMICO UTILIZANDO SISTEMAS DINÁMICOS COMPLEJOS. Tesis doctoral UNIVERSITAT POLITÈCNICA DE CATALUNYA- Cap 2.
- Castro Romero, M. et al (2018). *Introducción a la Seguridad Informática y el análisis de las vulnerabilidades*. Editorial Área de Innovación y Desarrollo, S. L. <https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf>
- Caurín, J. (2014). *Políticas de Seguridad*. Emprende Pyme. <https://emprendepyme.net/politicas-de-seguridad.html>
- Cevallos, J. D., & Naranjo Sánchez, B. (2021). *ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN DE UNA EMPRESA DEL SECTOR INFORMÁTICO*.

- <https://www.coursehero.com/file/97295533/35-Administraci%C3%B3n-de-Riesgos-de-TIpdf/>  
Definición de. (2022). *PYME*. <https://definicion.de/pyme/>
- Editorial Etecé. (s.f.). *Seguridad*. En Editorial Etecé, última edición. Recuperado el 30 de septiembre 2020. <https://concepto.de/seguridad/>
- Gamboa Suárez, J. (agosto de 2020). *Importancia de la Seguridad informática y ciberseguridad en el mundo actual*. Tesis de la Universidad Piloto de Colombia. <http://repository.unipiloto.edu.co/handle/20.500.12277/8668>
- Giraldo García, Y. M. (2016). *¿Qué es el riesgo informático?* <https://prezi.com/cyw-1ww070o8/que-es-el-riesgo-informatico/>
- Hernández Sampieri, R., Collado, C., & Baptista Lucio, M. (2006). *Metodología de la investigación*. Mc Graw Hill.
- Hernández Trazobares, A. (2020). *Los sistemas de información: evolución y desarrollo*. Revista científica Dialnet, págs. 149-165. Recuperado el día 10 de noviembre de 2020.
- Lapiedra Alcamí, R., Devece Carañana, C., & Guiral Herrando, J. (2011). *Introducción a la gestión de sistemas de información en la empresa*. <https://libros.metabiblioteca.org/bitstream/001/193/8/978-84-693-9894-4.pdf>
- Laudon, K., & Laudon, J. (2012). *Management information systems*. New York: Pearson.
- López Vargas, J., & Torres Granados, M. (2010). *Problemática del Delito Informático: hacia una necesaria regulación internacional*. Tesis de la Universidad de Costa Rica. Costa Rica.
- Marker, G. (2020). *Vulnerabilidades informáticas*. Blog Tecnología informática. [https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/#%C2%BFQu%C3%A9\\_es\\_una\\_vulnerabilidad?](https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/#%C2%BFQu%C3%A9_es_una_vulnerabilidad?)
- Martinez Sanchez, R. (2021). *Seguridad informática en empresas*. Portal académico Academia: [https://www.academia.edu/31713009/Seguridad\\_Informatica\\_En\\_Empresas](https://www.academia.edu/31713009/Seguridad_Informatica_En_Empresas)
- Metodología para la gestión de la seguridad informática*. (2013). Proyecto. <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVA>.
- Morales, A. (2020). *Información*. Blog, herramienta educativa. TODO MATERIA. <https://www.todamateria.com/informacion/>
- Muñoz, D. (2015). *Antecedentes de la Seguridad Informática*. <https://prezi.com/rawao1zpujn1/antecedentes-de-la-seguridad-informatica/>
- Organización Inca. (2020). *Políticas de seguridad informática*. Organización Inca: [https://www.centroinca.com/centro\\_inca/documentos/politica\\_seguridad\\_informatica.pdf](https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf)
- Roldán, P. (2017). *Organización*. <https://economipedia.com/definiciones/organizacion.html>
- Roldán, P. (7 de enero de 2017). *Organización*. <https://economipedia.com/definiciones/organizacion.html>
- Romero Castro et al. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*.



Alicante, España.

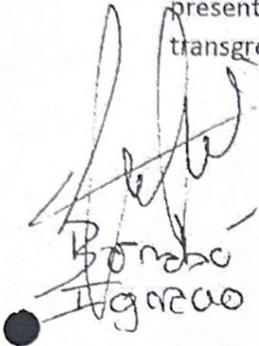
Santos Chaves, J. (2022). *Vulnerabilidad informática: Qué es y cómo protegerse*.

<https://www.deltaprotect.com/blog/vulnerabilidad-informatica>

Voutssas, M. (2010). *Preservación documental digital y seguridad informática*. Investigación bibliográfica. [https://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0187-358X2010000100008](https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008)

### DECLARACIÓN JURADA RESOLUCIÓN 212/99 CD

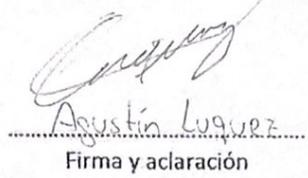
El autor de este trabajo declara que fue elaborado sin utilizar ningún otro material que no haya dado a conocer en las referencias que nunca fue presentado para su evaluación en carreras universitarias y que no transgrede o afecta los derechos de terceros.

  
Hecece Gonzalo

Bog 23666

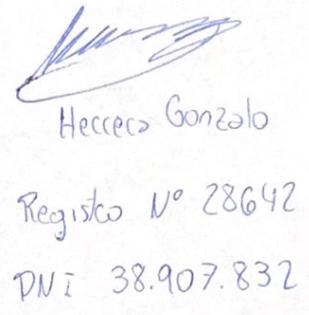
DNI 31285622

Mendoza, 6 de septiembre de 2023

  
Agustín Luquez  
Firma y aclaración

29326  
Número de registro

39.235.949  
DNI

  
Hecece Gonzalo  
Registro N° 28642  
DNI 38.907.832