# Seguridad

Luis Jaramillo

2024-08-11

# Table of contents

# 1 Seguridad Informática

**Bienvenidos al fascinante y desafiante mundo de la seguridad informática**

**Autor: Luis Enrique Jaramillo Montaño**

Es un placer presentarles esta guía introductoria, especialmente diseñada para ser una compañera confiable en su viaje hacia la comprensión de los aspectos fundamentales de la ciberseguridad. Hoy en día, el entorno digital no es solo un lugar donde almacenamos información, trabajamos, o nos comunicamos; también es un campo en constante evolución, lleno de amenazas que requieren conocimiento, habilidades y atención.

Esta pequeña guía está pensada para proporcionar una base sólida que les permitirá entender y enfrentar algunos de los ataques informáticos más comunes y actuales. A lo largo de sus páginas, exploraremos métodos de ataque que, aunque frecuentemente utilizados, son cada vez más sofisticados y sutiles. Con una estructura clara y ejemplos prácticos, nuestro objetivo es que puedan identificar estos riesgos y, más importante aún, que desarrollen una mentalidad proactiva y crítica para protegerse a sí mismos, a sus entornos de trabajo, y a sus proyectos personales en el vasto universo digital.

Sabemos que, para algunos, este campo puede parecer intimidante; sin embargo, no subestimen su capacidad para aprender y dominar estos temas. Con dedicación, curiosidad, y un enfoque práctico, estarán listos para comprender mejor el complejo pero fascinante panorama de la ciberseguridad.

Estamos convencidos de que el conocimiento sobre seguridad informática es una herramienta esencial y que todos deberían tener acceso a una comprensión básica de cómo protegerse en el ámbito digital. Esperamos que esta guía sea el comienzo de una nueva etapa en su vida, una etapa donde el conocimiento y la conciencia serán sus mejores defensas frente a los desafíos digitales.

¡Bienvenidos y que disfruten cada capítulo, cada técnica, y cada consejo que hemos recopilado para ustedes en esta guía de seguridad!

# Part I

# ¿Qué es la ciberseguridad?

# 2 Definición de Ciberseguridad.

**¿Qué es la Ciberseguridad?**

En un mundo cada vez más conectado, donde la mayoría de nuestras actividades cotidianas y profesionales se desarrollan en el ámbito digital, la ciberseguridad se ha convertido en una disciplina fundamental. Ciberseguridad no es solo un conjunto de prácticas para proteger dispositivos y redes; es una mentalidad que nos prepara para enfrentar y prevenir riesgos en el mundo digital, donde la información personal, financiera y organizacional puede estar en juego

La ciberseguridad es el conjunto de prácticas, técnicas y tecnologías diseñadas para proteger sistemas, redes y datos contra accesos no autorizados, ataques, daños o destrucción. Aunque la ciberseguridad tiene como objetivo general salvaguardar la confidencialidad, integridad y disponibilidad de la información, esta disciplina adopta un enfoque adaptado según el entorno en el que se aplica.

Ciberseguridad en Tecnologías de la Información (TI) En el ámbito de TI, la ciberseguridad se basa en los principios fundamentales de la CIA:

Confidencialidad: Garantizar que solo los usuarios autorizados tengan acceso a la información. Integridad: Proteger la precisión y consistencia de los datos, evitando modificaciones no autorizadas. Disponibilidad: Asegurar que los datos y sistemas estén accesibles cuando sean necesarios. Ciberseguridad en Tecnologías Operativas (OT) Cuando se trata de redes OT, como en entornos industriales y sistemas críticos de infraestructura (por ejemplo, redes de energía, plantas de manufactura o transporte), se añaden dos pilares adicionales esenciales para cubrir las necesidades de seguridad específicas:

Seguridad de las Personas: Prioriza la protección física y la seguridad de los operadores y personal involucrado en el manejo de sistemas OT, especialmente en entornos de alto riesgo. Resiliencia: Se enfoca en asegurar que los sistemas OT puedan continuar operando de manera segura y confiable, incluso en situaciones de falla o bajo ataque, para evitar interrupciones críticas en los servicios. Estos pilares adicionales reflejan la naturaleza crítica y física de los sistemas OT, donde un fallo en la seguridad no solo representa un riesgo para la información, sino que también puede impactar directamente en la seguridad de las personas y en la continuidad de operaciones esenciales.

## 2.1 Importancia de la Ciberseguridad.

La ciberseguridad es vital para proteger los sistemas digitales y la información que se maneja en ellos, ya que cada aspecto de nuestras vidas y operaciones industriales se encuentra conectado al entorno digital. Sin la protección adecuada, las organizaciones, los servicios críticos y los individuos están expuestos a una variedad de amenazas que pueden afectar la continuidad de las operaciones, la privacidad de los datos y, en algunos casos, incluso la seguridad física de las personas.

Ejemplos Claves para Comprender su Impacto Robo de Datos Personales:

- Ejemplo: En el sector bancario, la filtración de datos personales, como números de cuenta y contraseñas, expone a los usuarios al riesgo de fraude. En 2017, el ataque masivo a Equifax comprometió la información personal de 147 millones de personas, exponiendo datos sensibles como números de seguridad social y tarjetas de crédito, con un costo multimillonario para la empresa y un impacto significativo en la confianza de los consumidores. Impacto: La ciberseguridad es crucial para proteger la privacidad y mantener la confianza en los servicios financieros. Paralización de Infraestructuras Críticas:

- Ejemplo: Un ciberataque a una planta de energía eléctrica o a una red de distribución de agua puede afectar a miles de personas. En 2021, el ataque de ransomware a Colonial Pipeline, la principal red de distribución de gasolina en la costa este de los EE. UU., obligó a cerrar las operaciones durante varios días, provocando escasez y aumentos en los precios del combustible. Impacto: La resiliencia y la disponibilidad de los sistemas son esenciales en OT para evitar una disrupción significativa en infraestructuras críticas que pueden afectar directamente a la población. Amenaza a la Seguridad Física:

- Ejemplo: En una planta de manufactura automatizada, un ataque a los sistemas de control industrial (ICS) puede manipular el funcionamiento de la maquinaria, comprometiendo la seguridad de los operarios. Un ejemplo de ello fue el ataque a una planta de tratamiento de agua en Oldsmar, Florida, donde un ciberdelincuente intentó elevar peligrosamente los niveles de una sustancia química en el agua, poniendo en riesgo la salud de la población. Impacto: En sistemas OT, la ciberseguridad no solo protege datos, sino también la integridad física de los operadores y el público en general. Riesgo Financiero para las Empresas:

- Ejemplo: El ransomware es uno de los ataques más comunes y costosos para las empresas. En 2020, el fabricante de automóviles Honda fue víctima de un ataque de ransomware que paralizó sus sistemas en múltiples plantas de producción alrededor del mundo. Esto provocó retrasos significativos en la cadena de producción y generó pérdidas millonarias. Impacto: La ciberseguridad protege a las empresas de costos significativos por interrupciones operativas, pérdida de productividad y daño a su reputación. Amenazas a la Confidencialidad en el Sector Salud:

- Ejemplo: Los ataques a hospitales y sistemas de salud pueden filtrar información médica confidencial y, en algunos casos, poner en riesgo la vida de los pacientes. En 2017, el ataque de ransomware WannaCry afectó a hospitales en el Reino Unido, bloqueando el acceso a expedientes médicos y forzando la cancelación de citas y cirugías. Impacto: La ciberseguridad es crucial en sectores como el de la salud, donde la confidencialidad y la disponibilidad de los datos son fundamentales para la atención segura y efectiva de los pacientes.

# Part II

# Ataques