| Logo instituto sin fondo | **INSTITUTO SUPERIOR DE FORMACIÓN TÉCNICA N° 93**  **CARRERA**: Tecnicatura superior en análisis, desarrollo y programación de aplicaciones  **ESPACIO CURRICULAR**: Metodologia de Investigacion  **CURSO**: 1 AÑO B  **CICLO LECTIVO**: 2024  **PROFESORA**: Sciaca Carolina  **ALUMNO**: Nicolás Sandoval.  **CANTIDAD DE HOJAS**: |
| --- | --- |

**La Ciberseguridad en**

**las redes sociales**

# Introducción

Las redes sociales han comenzado a generar un gran impacto alrededor del mundo a partir de los últimos años del segundo milenio, ganando exponencialmente una gran cantidad de suscriptores a través de aplicaciones web. Como consecuencia, algunos usuarios vieron que podían introducir sus intenciones maliciosas para lograr un objetivo muy claro, el cual sería el aprovechamiento de la ignorancia que tienen las personas hacia algo nuevo y masivo que estaba llegando, que hasta el día hoy es muy difícil poder contrarrestar.

Estas intenciones maliciosas son mejor conocidas como Cibertaques Informáticos, que pueden ser de muchas formas posibles, entre ellas está el robo de datos personales o empresariales, como los números de identidad y las claves bancarias, las estafas a personas adultas con bajos conocimientos en el manejo de internet, a través de mensajes con enlaces de descarga de programas informáticos que podrían llegar a ocasionar múltiples problemas a los equipos que estamos manipulando.

A partir de lo antes visto, es de donde vamos a plantear nuestro objetivo, este será identificar las formas de contrarrestar, prevenir y repeler los ciberataques a las personas vulnerables que son atrapadas en las redes sociales que tanto entretenimiento tienen para dar. Pero para poder realizarlo se tiene que saber que es la ciberseguridad y las maneras que tiene para poder lograrlo.

Entonces ¿Qué es la ciberseguridad? ¿Qué tan importante es? ¿Cómo ayuda a contrarrestar los ataques? ¿Cuáles son sus métodos de prevención? ¿Puede repeler estos ataques de alguna manera?

Estas cuestiones serán desarrolladas y nos servirán de hilo conductor durante todo el estudio de investigación para comprender ante lo que nos enfrentamos, intentando alcanzar la problemática que planteamos.

# ¿Qué es la ciberseguridad?

Es el método desarrollado por las personas científicas especializadas en la informática para combatir las malas intenciones de usuarios ajenos a los primeros sistemas que se establecieron.

Estos surgieron hace ya más de 50 años, cuando se empezaron a conectar las computadoras mediante una red y modems. Esto quiere decir que antes solo se podía piratear una computadora únicamente de manera física, frente al monitor de la misma. Pero ese delito aun no se lo consideraba como un ciberataque, solo se lo caratulaba como violacion de la privacidad. Así fue como en la década de 1960 comenzó lo que hoy conocemos con esta forma de red.

La ciberseguridad intenta proteger equipos, redes, aplicaciones, sistemas de alta complejidad y principalmente los datos de personas ante las amenazas digitales que muchos escucharon pero que pocas saben cómo enfrentar.

Las organizaciones utilizan medidas y herramientas para proteger los datos confidenciales, como también los accesos no autorizados, para evitar interrupciones en los sistemas bancarios u otros sistemas de alta complejidad como lo es el transporte.

La ciberseguridad implementa la defensa en las organizaciones mundiales mediante leyes y estatutos como los hay en Europa, que deben cumplir el Reglamento General de Protección de Datos (GDPR).

Además de lo antes dicho, está la ciberseguridad en el tema que queremos abordar, que es la que se encuentra en las redes sociales. Las medidas tomadas acá son muchas e incluyen el uso de contraseñas fuertes, que contienen letras minúsculas, mayúsculas, números y caracteres especiales, la autenticación en dos pasos, que consiste en el envío de código a teléfonos para confirmar antes de un tiempo determinado, o también un dispositivo con sistemas biométricos y reconocimiento facial.

Además estas aplicaciones sociales ofrecen vigilancia constante de las actividades en la cuenta y notificación de posibles incidentes, la implementación de políticas de seguridad para los empleados y usuarios, y por último, el monitoreo y respuesta rápida a posibles incidentes de seguridad.

Como podemos observar, cuando comenzó el auge de las redes sociales, todas estas implementaciones, aún no estaban impuestas, solo se necesitaba un correo electrónico, un pequeño formulario y una contraseña sin estándares para poder suscribirse a una página web de chat online. Comenzar a ser un usuario más de estas redes no era tarea difícil, cualquier persona con acceso a internet podía hacerlos en menos de dos minutos.