UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y AUTOMATISMO

TEMA:

Estudio de ciberseguridad en sistemas SCADA y sistemas informáticos como respuesta a la industria 4.0 en el Ecuador

AUTOR:

Véliz García, David Daniel

Trabajo de titulación previo a la obtención del título de

INGENIERO ELECTRÓNICO EN CONTROL Y AUTOMATISMO

TUTOR:

Ing. Romero Rosero, Carlos Bolívar

Guayaquil, Ecuador

14 de septiembre del 2022

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y AUTOMATISMO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Veliz García, David Daniel** como requerimiento para la obtención del título de **INGENIERO ELECTRÓNICO EN CONTROL Y AUTOMATISMO**.

TUTOR

_____

M. Sc. Romero Rosero, Carlos Bolívar

DIRECTOR DE CARRERA

_____

M. Sc. Bohórquez Escobar, Celso Bayardo

Guayaquil, a los 14 días del mes de septiembre del año 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y AUTOMATISMO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **David Daniel Véliz García**

DECLARO QUE:

El trabajo de titulación: **Estudio de ciberseguridad en sistemas SCADA y sistemas informáticos como respuesta a la industria 4.0 en el Ecuador,** previo a la obtención del Título de **Ingeniero en Electrónica en control y automatismo**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 14 días del mes de septiembre del año 2022

EL AUTOR

_____

Véliz García, David Daniel

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA ELÉCTRONICA EN CONTROL Y AUTOMATISMO

AUTORIZACIÓN

Yo, **Véliz García, David Daniel**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **Estudio de ciberseguridad en sistemas SCADA y sistemas informáticos como respuesta a la industria 4.0 en el Ecuador**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

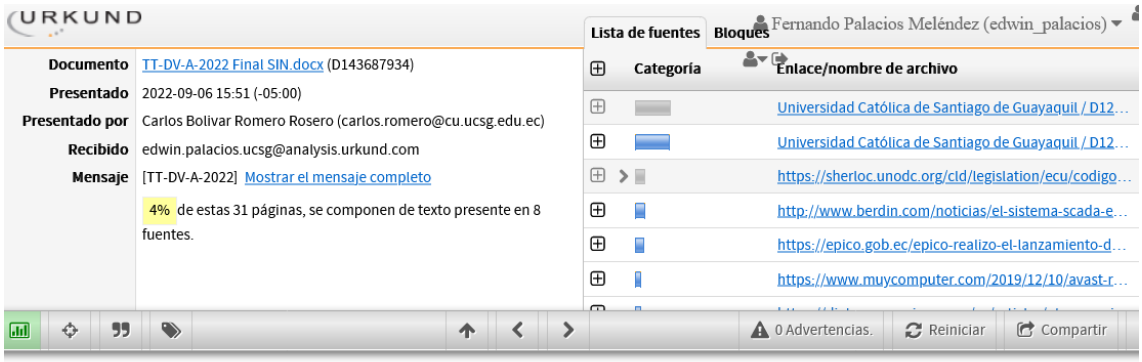
Guayaquil, a los 14 días del mes de septiembre del año 2022

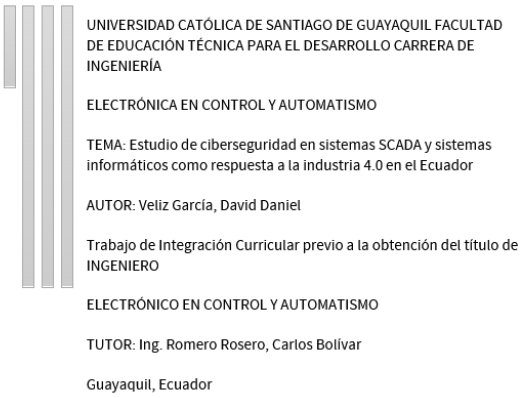
EL AUTOR

Véliz García, David Daniel

REPORTE DE URKUND

Informe del Trabajo de Titulación de la Carrera de Electrónica en Control y Automatismo, con **4 %** de coincidencias perteneciente al estudiante VELIZ GARCIA, DAVID DANIEL**.**





Atentamente,

Ing. Carlos Romero Rosero.
Profesor Titular Principal
TUTOR

DEDICATORIA

Dedicado a mi Madre Angela García y mi Padre Segundo Veliz los cuales me apoyaron a lo largo de mi formación tanto académica como persona, mis hermanos y hermanas los cuales siempre estuvieron para apoyarme y darme consejos.

EL AUTOR

Véliz García, David Daniel

AGRADECIMIENTOS

Al concluir una etapa maravillosa de mi vida quiero extender un profundo agradecimiento a mi madre Ángela García Patricia Chang y a mi padre Telmo Segundo Veliz Mendoza por todo el esfuerzo que hicieron para que pueda estudiar y salir adelante, mis hermanos y hermanas Juan Carlos Veliz García y Andrés Veliz García, Carolina Veliz García y Leyla Veliz los cuales me brindaron consejos y estuvieron para ayudarme y apoyarme a lo largo de mi vida.

A mi enamorada Gabriela Barzola, por estar a mi lado brindándome apoyo y amor para seguir adelante.

A mis amigos: Adriana Velasco, Anthony Guijarro, Luis Zamora, Carlos Racines, María del Carmen García, Víctor Espinoza, Mauricio Martínez los cuales me apoyaron incondicionalmente.

A mis conocidos y compañeros de trabajo los cuales recibí consejos de vida y grandes enseñanzas que me han servido a lo largo de mi formación como profesional.

Y a mis docentes por todas las enseñanzas brindadas a lo largo de mi carrera profesional en especial al Ing. Carlos Romero por orientarme en mi trabajo de titulación.

EL AUTOR

Véliz García, David Daniel

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y AUTOMATISMO

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. BOHORQUEZ ESCOBAR CELSO BAYARDO

DIRECTOR DE CARRERA

f. _____

M. Sc. VELEZ TACURI EFRAIN OLIVERO

COORDINADOR DEL ÁREA

f. _____

ING. BRAVO GAME LUIS HELIODORO

OPONENTE

VIII

Índice General

Índice de Figuras

Capítulo 2

Capítulo 3

Índice de Tablas

Capítulo 3

Resumen

El presente trabajo de titulación consiste en un estudio de ciberseguridad en sistemas informáticos y sistemas SCADA como respuesta a la industria 4.0 en el Ecuador con el fin de dar una respuesta y dar a conocer la calidad de conocimiento que cumplen los Ingenieros que trabajan en estas áreas se realizó una encuesta en la cual se efectuó el análisis de cada pregunta y respuesta para así evaluar a los encuestados sobre que tanto conocen sobre ciberseguridad.

En el capítulo 1 se abordó sobre ¿Como incide la ciberseguridad en los sistemas informáticos y sistemas SCADA actualmente en el Ecuador? Siendo ésta el problema a investigar, además se plantearon los objetivos para así de esta manera llevar a cabo la investigación.

En el capítulo 2 se abordó el marco teórico en el cual se hizo referencia hacia las herramientas que utilizan los ciberdelincuentes, maneras de evitar ataques cibernéticos mediante antivirus, buscadores seguros y sobre todo conocer las leyes que existen en caso de sufrir un ataque cibernético. Las personas suelen mal utilizar términos como hacker y cracker puesto que, en este trabajo, se explicará la manera correcta en la cual se conoce a estos ciberdelincuentes.

Se abordarán temas de cómo lidiar con malwares, troyanos y adware, los cuales pueden abrir una brecha e irrumpir en los softwares de programación

Además de esto en el trabajo se muestra ataques cibernéticos en empresas e industrias fuera del país. Las cuales hicieron que corra peligro la vida del ser humano.

Palabras clave: SCADA, CIBERDELINCUENTE, HACKER, MALWARES, TROYANOS, ADWARE, SOFTWARE

Capítulo 1: Descripción General del Trabajo de Titulación

En este capítulo, se presenta la descripción general del trabajo de titulación.

1.1. Introducción.

En el presente trabajo se observa como el internet se ha adaptado a la industria implementándola en diferentes áreas de trabajo, mejorando la producción y el desempeño del área de trabajo, hoy en día la informática y el internet de las cosas forma parte del diario vivir de las personas en su lugar de trabajo, obligando de esta manera que el empleador se capacite con algún curso informático.

Las proliferaciones de las nuevas tecnologías inteligentes han influido mucho en los sistemas industriales y en los sistemas SCADA de tal manera que un proceso industrial o un proceso de planta puede ser monitorizado de manera remota.

Sin embargo, esto trae consigo el aumento de descuidos en ciberseguridad, así como la tecnología mejora para el bien, otros la utilizan para el mal. Se debe considerar que un ciberdelincuente no necesita de un gran computador para poder realizar ataques informáticos.

En el siguiente estudio se postularán breves recomendaciones con la finalidad de reducir o prevenir dichos ciberataques en los sistemas informáticos de las industrias.

Con el siguiente estudio se logrará identificar y prevenir las diferentes vulnerabilidades que puede presentar un computador lógico programable más conocido como PLC, sistemas como LabVIEW y los diferentes programas informáticos en la educación 4.0

La ciberdelincuencia es algo que siempre estará presente, es un tema delicado debido que en ciertos casos se utilizan a hackers para brindar seguridad en alguna empresa o en alguna industria.

1.2. Antecedentes.

Según (Abril, 2021) El último informe anual de Kaspersky revela que en Ecuador existe un crecimiento del 75% en cuanto a los ataques informáticos, es decir, hay alrededor de 89 ataques por minuto. Según los expertos, esto afecta no solo a las grandes empresas o a los bancos, como ocurría en el pasado, sino que cada vez hay más interés por la información de pequeñas y medianas empresas.

Lo citado de (Onofa, 2022) Ecuador se suma como uno de los países de Latinoamérica más golpeados por los delitos informáticos, principalmente códigos maliciosos (malware). Según el último Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, agencia de la Organización de las Naciones Unidas, Ecuador se encuentra en el puesto 119 de 182 países en vulnerabilidad por ataques cibernéticos.

Según (Nicholas R. Rodofile, 2019) los sistemas de infraestructura crítica basados en SCADA dependen de tecnologías basadas en TI, lo que permite a las empresas de servicios públicos proporcionar infraestructura y servicios esenciales a la sociedad; debido a la dependencia de las infraestructuras críticas en los sistemas basados en TI, los ciberataques que alguna vez se usaron contra los sistemas de TI tradicionales ahora son capaces de atacar la infraestructura crítica. Como resultado, la seguridad cibernética para la infraestructura crítica es una preocupación para los proveedores de servicios públicos. Los servicios de infraestructura crítica incluyen transporte, tratamiento de agua, generación de energía y fabricación. En el pasado, los investigadores se han centrado en ataques aislados en sistemas de control, o en varios tipos de ataques a protocolos de comunicación. Alternativamente, investigaciones anteriores clasificaron los ataques basados en tres partes: hardware, redes y software, lo que proporcionó a la investigación de ciberseguridad un panorama de ataques más amplio.

Los ataques informáticos fueron tomando más relevancia en el país a raíz de la pandemia del COVID-19 debido que un sin número de personas y empresas optaron por la virtualidad, de esta manera los ciberdelincuentes se

valieron de este suceso para cometer delitos, personas que trabajaban en empresas o en industrias eran un blanco fácil para los ciberdelincuentes.

1.3. Definición del Problema.

A raíz de la pandemia del COVID-19 se implementó el teletrabajo, de esta manera las personas que trabajan en industrias, fabricas migraron a la modalidad virtual desde casa, los sistemas SCADA permiten verificar y modificar datos de manera remota de tal manera que al utilizar una maquina personal para controlar dichos procesos, los datos de las empresas o fabricas quedan expuestos a posibles ataques informáticos.

¿Como incide la ciberseguridad en los sistemas informáticos y sistemas SCADA actualmente en el Ecuador?

1.4. Justificación del Problema.

Con la siguiente investigación se enfocará en un plan de formación de procedimiento de ciberseguridad en sistemas informáticos y sistemas SCADA en instituciones superiores académicas como la Universidad católica de Santiago de Guayaquil en la facultad de educación técnica para el desarrollo, para formar a los futuros ingenieros de las carreras técnicas sobre cómo manejar y tratar los riesgos cibernéticos.

Se vive en una época en la cual la información personal o de una empresa se encuentra en una computadora o en el correo electrónico, la mayoría de las personas no sabe cómo protegerse ante ciberataques, depende la situación un antivirus no basta, además de esto muchos utilizan antivirus los cuales son crackeados entonces allí existe una brecha de seguridad logrando que la información sea accesible para cualquier persona.

1.5. Objetivos del Problema de Investigación.

1.5.1. Objetivo General.

Estudiar el impacto de ciberseguridad en sistemas SCADA y sistemas informáticos como respuesta a la industria 4.0 en el Ecuador mediante investigación y análisis de ciberataques en otras empresas internacionales.

1.5.2. Objetivos Específicos.

1. Fundamentar las teorías de la ciberseguridad y descripción de los sitios de estudio.
2. Identificar las vulnerabilidades y las herramientas utilizadas por los ciberdelincuentes.
3. Establecer métodos de protección en los sistemas informáticos para el Ecuador.
4. Planificar y tomar medidas para la protección y prevención de los ciberataques en la industria 4.0.

1.6. Hipótesis.

El presente trabajo dará a conocer a la Universidad católica de Santiago de Guayaquil y a la Facultad de Educación Técnica para el Desarrollo la importancia sobre los ciberataques en la actualidad en dispositivos informáticos utilizados en la industria 4.0

1.7. Metodología de Investigación.

El tipo de investigación a emplear en el presente trabajo de titulación es expositivo y documental. De la manera expositiva permita describir como la industria 4.0 puede verse afectada por ciberataques y como la seguridad informática puede ser de gran ayuda para prevenirlos además de esto la manera en la cual puede influir estas prácticas hacia la educación en las aplicaciones educativas superior.

De igual manera la metodología de trabajo será documental ya que estará guiada por la recopilación de diferentes fuentes bibliográficas para

realizar los respectivos análisis con la finalidad de proporcionar los mejores métodos de protección de datos.

Se realizará un estudio de la realidad actual sobre los riesgos expuestos a la seguridad de los sistemas, además de esto se determinarán las mejores técnicas para la recopilación de datos utilizando artículos científicos, libros y fuentes bibliográficas variadas.

Capítulo 2: Fundamentación Teórica

En el siguiente capítulo se expondrá los fundamentos teóricos los cuales brindaran soporte, lógica y sentido a los diferentes aspectos de la ciberseguridad en los sistemas de la industria 4.0 y sistemas informáticos. Se abordará las diferentes características de los ciberataques y como prevenirlos, los mecanismos y las maneras por las cuales se puede ser víctima de un ataque cibernético y las diferentes políticas de seguridad. También se tratará sobre los incidentes que estos ataques causan en la industria y como estar preparado para prevenir con anticipación algún ciberataque.

2.1. Introducción de un ciberataque.

El termino ciberseguridad se utiliza con la finalidad de detallar los diferentes tipos de eventos en internet desde protestas en línea, robos de secretos informáticos y hasta sabotaje cibernético de la investigación de armas. Por lo que, para adaptar un concepto más apropiado, se debe conocer ampliamente sus características, para a su vez poder clasificar los ciberataques de otras eventualidades informáticas de menor relevancia.

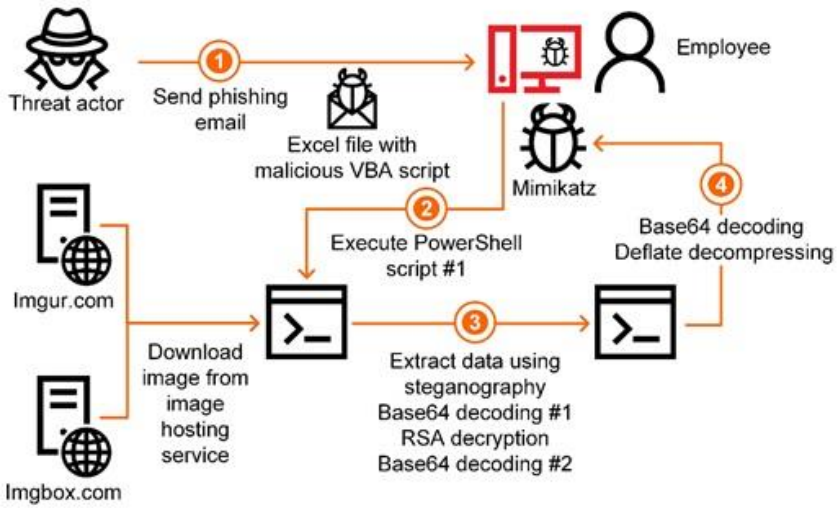


Figura 2. 1: *Proceso de un ciberataque*.

Fuente: (Kaspersky, 2020).

En la figura 2.1 se puede observar la manera en la cual un usuario envía un correo con un correo phishing con un documento malicioso hacia un empleado, la persona a la que le llego el correo abre este documento y de manera oculta se ejecuta el Windows PowerShell, entonces el empleado vera

un documento con información falsa incluidos logos y este al digitar cualquier tecla, será enviada hacia la persona que realizo el ataque, proporcionándole de esta manera usuarios, contraseñas y demás accesos.

2.2. Características de un ciberataque.

Se denomina como intento de desactivar dispositivos informáticos, hurto de datos o de información, existen diferentes maneras de realizar un ciberataque utilizando malwares, phishing u otros métodos como la utilización de un rubber ducky. Los ciberataques son cada vez más comunes y este término es más utilizado para definir cualquier tipo de evento en internet desde robos o protestas.

Para ser víctima de un ciberataque solo basta con ingresar a paginas equivocadas en línea o la descarga de algún archivo peligroso. Estos ataques se caracterizan por ser silenciosos, esto quiere decir que un ataque puede ser efectivo y el usuario no lo notara, son muy comunes en dispositivos que no cuentan con protección ya sea con antivirus o con conocimientos informáticos básicos para evitar ser víctima de estos.

Figura 2. 2: *ventana emergente mostrando un adware*.

Fuente: (Kiguolis, 2019).

En la figura 2.2 se puede observar un adware, el cual muestra de manera automatizada mensajes engañosos o publicidad falsa con la finalidad que algún usuario inocente seleccione alguna opción de allí. Este tipo de

ciberataque tiene como característica aparecer de manera inmediata y llenar de publicidad la pantalla, es uno de los más comunes.

Las maneras en las que este adware se instala en algún dispositivo que tiene acceso a internet es por medio de aplicaciones gratuitas o alguna página web infectada, la mayoría de los usuario no prestan mucha atención a estos mensajes, lo que se desconoce es que al tener instalado dicho adware en la computadora o celular este tiene acceso a contraseñas y demás datos personales, este cuenta con dos funciones de ataque la primera es visualizar anuncios y la segunda es recopilar información personal.

Es importante conocer que no todos los adwares son maliciosos, una gran cantidad de software incluyen adware los cuales son legítimos un ejemplo claro son las aplicaciones gratuitas, existen algunas las cuales piden consentimiento del usuario para mostrar publicidad a cambio que este pueda utilizar la aplicación. También existen adware del tipo maliciosos los cuales pueden instalar malwares o spyware (virus espía) en estos casos el usuario no autoriza la instalación de estos, aun que de igual forma este puede instalarlo por error.

2.2.1. Malwares consecuentes en un ciberataque

El malware es sumamente común es un término en el cual describe un programa o código malicioso el cual afecta a los sistemas informáticos o sistemas de computación. Su función principal es invadir y deshabilitar dispositivos o sistemas informáticos, estos pueden atacar cualquier dispositivo ya sea una computadora, laptop, celular o Tablet.

Cabe destacar que el malware solo puede afectar al software, pero no puede dañar el hardware, este virus informático además de esto puede hurtar dinero, cifrar datos, alterar información hasta incluso espiar la actividad del ordenador incluyendo el pulsado de las teclas.

Formas de detectar este virus, ralentización de la computadora o dispositivo, ya sea navegación por internet o incluso la interacción con el computador, en la pantalla del dispositivo pueden aparecer anuncios inesperados este malware es conocido como adware del inglés ad que significa publicidad, entonces estos actúan en conjunto, al aparecer el adware

y darle click, se descargara algún archivo en el cual se encuentra el malware y de esta manera el dispositivo estará infectado. Otros avisos para saber que el dispositivo cuenta con un malware es que los enlaces de páginas comunes que el usuario tiene guardados al momento de dar click este lo redirige a otra página, además de esto puede producir pantallazos azules al dispositivo.

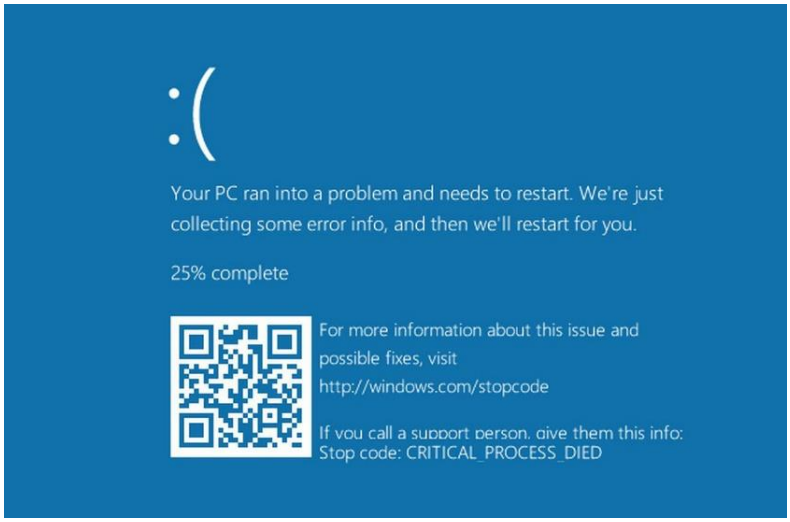


Figura 2. 3: *pantallazo azul de Windows.*

Fuente: (Buxton, 2020).

En la figura 2.3 se puede observar un inconveniente común en la mayoría de los dispositivos, se lo conoce como pantallazo azul de la muerte o pantallazo azul, este problema se suele presentar por alguna mala actualización, algún driver mal instalado, algún error de código interno pero también lo suelen causar los malwares, al momento en que se presenta este inconveniente Microsoft proporciona un código QR en la pantalla en la cual otorgara información sobre el problema y como poder solucionarlo.

Ahora el caso está en que si un malware proporciona o simula un pantallazo azul y otorgue un código QR, sería un peligro escanearlo ya que de esta manera este malware atacaría el dispositivo móvil, es muy común este tipo de ataques en los cuales el usuario escanea dicho código y lo redirecciona hacia otra página en la cual se podrá descargar algún archivo con la supuesta solución al problema del pantallazo azul, de esta manera es en la que el malware ataca varios dispositivos.

2.2.2. Rubber Ducky

El USB rubber ducky se trata de una herramienta de hacking muy común, esta se puede obtener por medio de internet o se puede modificar una memoria y por medio de un código realizado en Python para programarlo.

según (Jimenez, 2022) este dispositivo permite el acceso y control total de un sistema ya que son scripts preconfigurados. Entonces básicamente dicho dispositivo permite el control de manera remota de esta manera este dispositivo cuenta con la opción de registrar pulsaciones, en el mundo informático este término es conocido como keylogger, la manera en la cual este dispositivo ingresa al sistema es de manera física, debido que físicamente tiene la apariencia de un pendrive común y corriente.

La interfaz de dicho dispositivo se conoce como HID (Human Interface Device) debido que es un dispositivo de entrada y salida, estos dispositivos al momento de conectarlos a alguna computadora ya sea que cuente con Windows, Linux, OSX este será detectado como un teclado común y corriente.

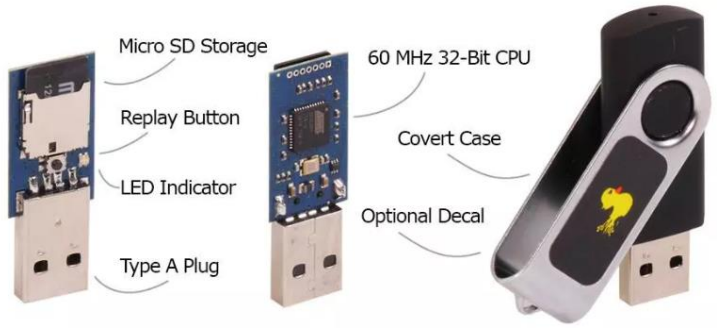


Figura 2. 4: *vista de un rubber ducky sin carcasa*.

Fuente: (Jimenez, 2022).

En la figura 2.4 se puede observar de manera interna un rubber ducky y se puede verificar que físicamente es como una memoria USB común y corriente, para utilizar este dispositivo basta que una persona lo conecte en el computador de otro usuario, incluso se puede programar este dispositivo para que al momento en que se conecte copie todos los archivos que cuenta la máquina.

Entonces este dispositivo al ser capaz de copiar documentos y controlar el computador, se comprende que un PLC (controlador lógico

programable) es vulnerable ante este dispositivo, debido que puede ser controlado a distancia por otro usuario y casuar estragos en el dispositivo.

2.2.3. Ransomware

Este virus es conocido como un programa de secuestro de datos que tal y como su nombre lo indica mantendrá como rehén los archivos o datos hasta que el usuario o dueño de estos archivos pague un rescate, la función de este virus es encriptar dicho contenido de manera total o parcial de modo que no se pueda acceder sin tener la clave de acceso.

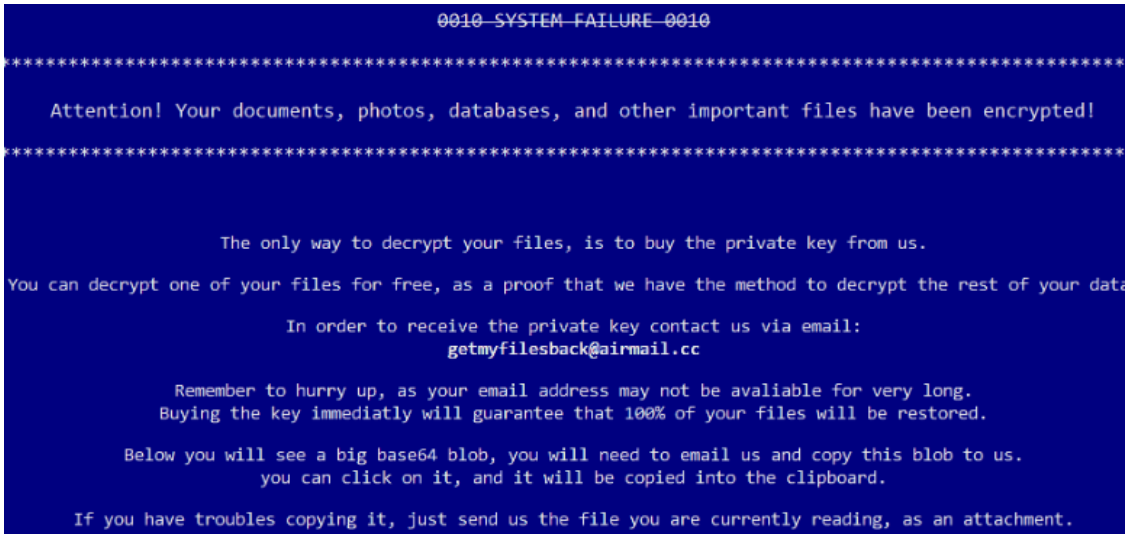


Figura 2. 5: *Nota de rescate de una versión anterior del ransomware Maze.*

Fuente: (Kuskov, 2020).

En la figura 2.5 se puede observar uno de los ejemplos de un ransomware es el virus Maze el cual es una de las más actuales, este cuenta con la peculiar nota de rescate que cuenta con el título “0010 System Failure 0010”, con el pasar del tiempo las versión de dicho troyano utilizaban un sitio web para las víctimas en lugar de un correo electrónico, la táctica de este consiste en infecciones mediante kits de exploits y de spam con archivos adjuntos maliciosos (Kuskov, 2020).

Según (Haran, 2021), el ransomware continuó siendo unas de las amenazas informáticas más peligrosas durante 2021 y registró mayor cantidad de grupos en actividad, mayor cantidad de ataques y pagos más elevados.

Para evitar y prevenir la infección con este tipo de virus es recomendable mantener el sistema operativo actualizado y las aplicaciones parchadas, además de capacitar a los empleados sobre tácticas de ciberseguridad, utilizar conexiones seguras y conocidas y por último utilizar antivirus.

2.2.4. Spyware

Son programas que tal y como lo dice su nombre son virus espías, este se instala sin permiso del usuario para poder recopilar información, supervisar actividades y comportamiento, este puede instalar programas sin necesidad del permiso del usuario, a su vez puede comportarse como un adware además de esto la finalidad de este virus es enviar información al atacante, en el caso de las industrias este es utilizado para atacar a algún empleador para tener acceso a contraseñas y enviarlas al atacante.

Figura 2. 6: *Spyware diseñado para permanecer oculto en los dispositivos.*

Fuente: (Seguin, 2022).

En la figura 2.6 se puede observar una representación gráfica sobre como funcionaria un virus espía, este virus puede estar oculto durante bastante tiempo y puede decidir cuándo atacar. Existen formas de saber si alguna maquina está infectada, pero cabe destacar que el spyware está completamente diseñado para ser indetectable e irrastreable, algunas de las señales para comprobar la infección pueden ser las siguientes:

- El dispositivo se comporta extraño o se ralentiza.
- El ordenador se bloquea o se traba frecuentemente.
- Aparición de ventanas emergentes.
- Aparición de iconos nuevos.
- Al momento de abrir una página web se redirige a otra.

Para prevenir la infección es recomendable tener las actualizaciones más recientes del sistema operativo, verificar que se encuentra en una página segura observando que cuente con https o con un candado y por último tener instalado un antivirus de confianza.

2.2.5. Rootkit

Un rootkit es un software malicioso diseñado para permitir la conexión no autorizada a un dispositivo o a otro software. Esto quiere decir que se conecta remotamente para obtener el control de un dispositivo y robar los datos, al momento en que el dispositivo se infecta el hacker tiene control total del equipo incluido a archivos con privilegio, de esta manera antivirus y software de seguridad no logran rastrear este virus volviéndose así completamente invisible.

Este virus puede realizar las mismas configuraciones que un administrador, de esta manera puede manipular o desactivar programas de seguridad, ocultar e instalar otros malwares, robar datos, crear una brecha de seguridad para que el atacante logre conectarse en cualquier momento y al tener permisos de administrador este puede activar micrófonos con la finalidad de espiar otra de las acciones que realiza es la de un keylogger al español un registrador de teclas. (Burdova, 2022).

Los hackers empaquetan los rootkits junto con dos programas asociados, el dropper y el loader, que colaboran para instalar el rootkit. Estos tres elementos de malware componen una amenaza combinada. Vamos a analizar con más detalle las herramientas utilizadas por los rootkits para instalarse:

- Dropper: Su función es importar el rootkit en el dispositivo de la víctima, una vez activada este activara el loader.

- Loader: Instala el rootlink en el sistema operativo causando un desbordamiento de bufer. Este es un exploit el cual abrirá paso a los hackers para introducir códigos en áreas inaccesibles del dispositivo.

Figura 2. 7: *Representación gráfica de un loader y un dropper para realizar un ataque*.

Fuente: (Burdova, 2022) .

En la Figura 2.7 se puede observar una representación gráfica de la acción que generaría un loader y un dropper al momento de atacar un dispositivo, el insecto representaría el virus el cual está siendo depositado mediante una garra la cual sería el dropper y el loader sería el camión el cual se encargará de instalar el virus el cual abrirá paso a atacantes cibernéticos

2.3. Protección de la información y datos.

Para prevenir ciberataques se necesita estar protegido a toda costa, por lo que se emplea el uso de antivirus, estos se deben configurar bien y debe cumplir con las necesidades de la empresa, persona o industria.

Existen diferentes tipos de antivirus, pero uno de los más utilizados por la industria y por empresas son Sophos, Checkpoint, Kaspersky, Azure Defender.

Es importante conocer que las versiones gratuitas de antivirus tienen severos problemas de seguridad como lo es por ejemplo el Avast, se conocieron casos en los cuales estas versiones gratis de este antivirus el proceso que realizaba era vender datos a empresas de publicidad. Los datos

de los 400 millones de usuarios de Avast son recolectados desde hace años para luego venderlos a empresas dedicadas a la publicidad. Eso es al menos lo que ha reconocido Ondrej Vlcek, jefe ejecutivo de la empresa de ciberseguridad checa Avast Software, en una entrevista que ha mantenido con el conocido medio Forbes. (Medina, 2019).

Figura 2. 8: *Protección de la información cibernética.*

Fuente: (ITtrends, 2022).

2.3.1. CheckPoint.

Este antivirus también conocido como Harmony Protect es uno de los líderes en ciberseguridad a nivel mundial, una de sus principales características es de fomentar la formación en seguridad debido que este antivirus protege al usuario advirtiéndole se encuentra en un sitio malicioso y además de esto al momento en que la persona que utiliza la misma contraseña para varios sitios o páginas web, el antivirus se lo advertirá, además de esto al momento de abrir correos electrónicos este determinara si contiene o no phishing. Este antivirus lo que hará será encriptar todo el disco duro de la máquina y al momento en que alguien aparte de él quiera utilizar la maquina aparecerán varias maneras de iniciar sesión, además de esto el antivirus comentara las veces que alguien ha tratado de ingresar a la máquina y además de esto bloquea los puertos USB del dispositivo para que no exista el robo de información.

Entre sus ventajas contamos con: la generación de contraseñas más seguras para el usuario, vigilar la transferencia de data, examinar proveedores externos, control de acceso a hardware, nube privada, autentificación avanzada

En general, en 2021, las organizaciones experimentaron un 50 % más de ciberataques semanales que en 2020. Con los 1605 ataques semanales del sector de Educación/Investigación a la cabeza (75% de aumento). Le siguió Gobierno/Militar con 1136 ataques semanales (aumento del 47 %) y Comunicaciones con 1079 ataques semanales (aumento del 51%). Los proveedores de software experimentaron el mayor crecimiento interanual (146 %), lo que va de la mano con la tendencia cada vez mayor de los ataques a la cadena de suministro de software observados en 2021. Este último año también se han producido ataques en evolución en dispositivos móviles, un aumento de las principales vulnerabilidades de los servicios en la nube y el regreso de la notoria red de Bots Emotet. (Carlos, 2022).

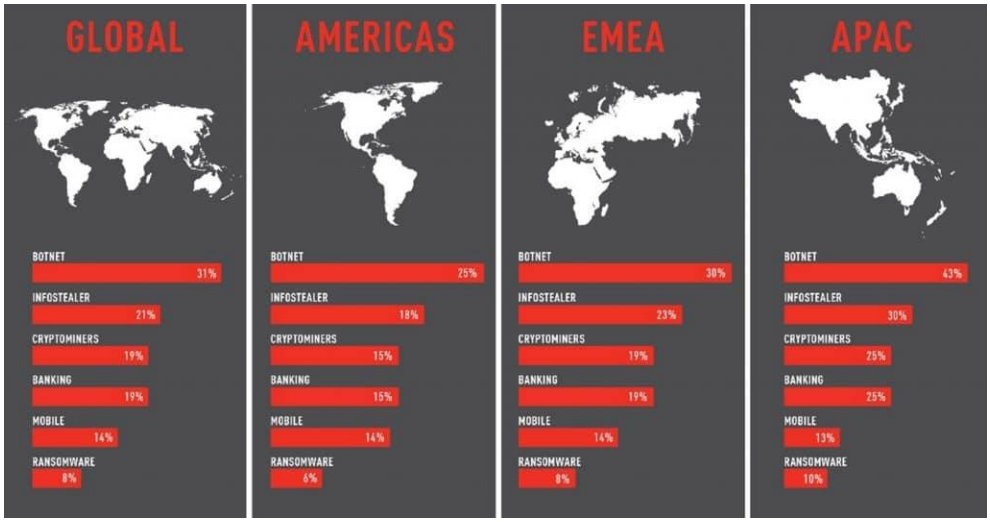


Figura 2. 9: *Categorías de ataques cibernéticos por región 2021*.

Fuente: (Carlos, 2022)

2.3.2. Kaspersky.

Este antivirus cuenta con un modo en el cual se encuentra desarrollado específicamente para infraestructuras y equipamiento industrial, con la finalidad de proteger combina rangos de seguridad tecnológicas como

protecciones contra malwares además de detectar conexiones no autorizadas hacia los sistemas de control.

Con la finalidad de mantener la industria protegida ante filtraciones o robo de información es posible restringir el acceso hacia las conexiones USB, además de esto es posible implementar limites, esto quiere decir que se puede configurar el dispositivo para que un usuario pueda guardar ciertas cosas de carpetas en específico.

El apartado de ciberseguridad industrial que destaca este antivirus es la de monitorear por medio de código ciberataques, anomalías o errores que causan los empleados dentro de la red industrial.

El nombre de la versión industrial es Kaspersky Industrial CyberSecurity la cual cuenta con una consola vía web la cual brinda herramientas de visualización de incidentes para observar a más detalle las amenazas, el operador tendrá la posibilidad de agregar nuevos equipos de manera eficaz a la plataforma hacia nuevos equipos industriales y agregar conectores a diferentes sistemas ya sea SIE, firewall o SCADA mediante la APIREST. (Granados, 2021).

Según comenta (Strelkov, 2021) “La protección adecuada de los entornos OT puede requerir un ajuste cuidadoso y muchos pasos manuales. Nuestro objetivo en esta actualización era simplificar esta tarea para los equipos de seguridad de TI: hacer más cómoda la gestión de la seguridad, mejorar la cobertura de los equipos y automatizar las funciones. La gestión de vulnerabilidades que se incorpora también simplifica esta tarea tradicionalmente complicada. En efecto, a diferencia de los dispositivos de TI, los OT no siempre pueden actualizarse con un clic del ratón y sin consecuencias para los sistemas vecinos. Pero sigue siendo importante encontrar formas de parchar o mitigar, y Kaspersky Industrial CyberSecurity for Networks colabora ahora a ello “.

Figura 2. 10: *Servicios y productos que ofrece Kaspersky Industrial CyberSecurity.*

Fuente: (Kaspersky, 2020).

En la Figura 2.10 se puede observar mediante un esquema a detalle los diferentes productos y servicios que brinda este antivirus en el ambito industrial, entre los productos se cuenta con proteccion endpoint industrial, deteccion de anomalias industriales y se cuenta conn un centro de monitoreo en tiempo real.

2.3.3. Azure Defender

Este software se encarga de proteger identidades, equipos y dispositivos, aplicaciones en la nube, archivos y correos electrónicos. Cuenta con un firewall de alta precisión y se mantiene actualizado de manera continua.

Es una plataforma de servicios en la nube pública que admite una amplia selección de sistemas operativos, lenguajes de programación, plataformas, herramientas, bases de datos y dispositivos. Puede ejecutar contenedores de Linux con integración de Docker, compilar aplicaciones con JavaScript, Python, .NET, PHP, Java, Node.js y crear back-end para dispositivos iOS, Android y Windows. (Terry Lanfear, 2022).

La infraestructura de Azure se encuentra diseñada desde la instalación hasta las aplicaciones para hospedar millones de clientes simultáneamente, y proporciona una base en el cual las empresas puedan mantener a salvo la información de los empleadores.

2.4. Definición y partes de un sistema SCADA.

Los sistemas de control y adquisición de datos o como comúnmente se lo conoce sistemas SCADA el cual permite monitorear, controlar verificar y supervisar procesos de manera remota en cualquier tipo de área, este ayuda a controlar los procesos automáticos y recopilar datos para llevar un registro de las operaciones. Esto lo realiza mediante sensores los cuales registran y capturan parámetros de operación y los transmiten con unidades remotas también conocidas como RTU hacia un centro de control en los cuales estos datos serán almacenados e interpretados con la ayuda de una interfaz hombre maquina (HMI, como lo indican sus siglas en ingles).

Estos sistemas dan paso al usuario a operar sistemas de tuberías, yacimiento de petróleos, sistemas de riego o un complejo de generación de energía hidroeléctrica a realizar modificaciones en el centro de configuración en controladores de procesos distantes como cerrar y abrir válvulas, controlar alarmas y recopilar información de medición. (Boyer, 2016).

En base lo mencionado anteriormente, se puede decir que los componentes principales de un sistema SCADA son los siguientes:

- Las múltiples unidades terminales remotas para los dispositivos como sensores o actuadores.
- Varias estaciones de control y monitoreo en las que se utilizan los aplicativos de HMI.
- Una infraestructura de comunicación puede ser en una red de área local (LAN, como lo indican sus siglas en inglés) o una red de área amplia (WAN, como lo indican sus siglas en ingles)

Dichos sistemas por lo general son una combinación de software y hardware como por ejemplo los PLC (Controladores Lógicos Programables) y las RTU (Unidades Terminales Remotas), dichos dispositivos se comunican con las maquinas, los sensores y demás equipos que se encuentran en una planta. Al momento de recopilar datos estos serán llevados a una sala de operaciones donde intervendrá el interfaz humano maquina más conocidas

como HMI las cuales van en conjunto los sistemas SCADA para poder visualizar los datos y comunicarse con el sistema.

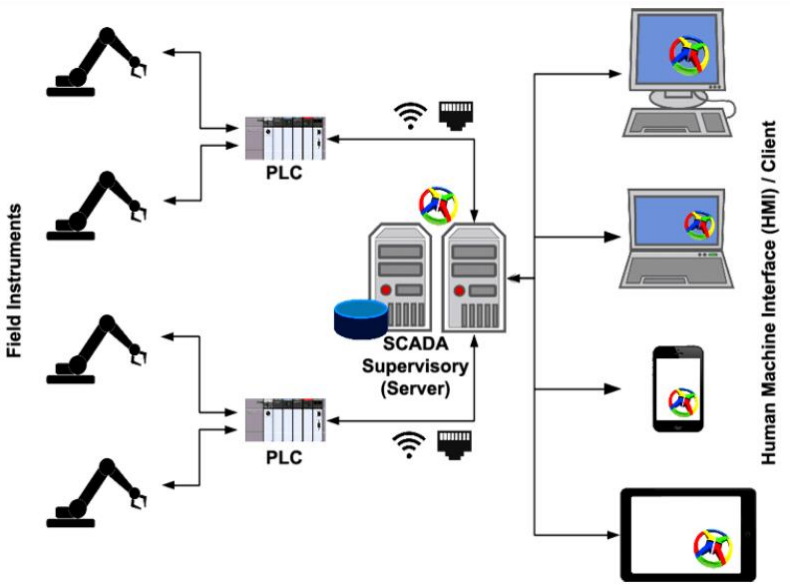


Figura 2. 11: *Estructura de un sistema SCADA.*

Fuente: (Boyer, 2016).

En la Figura 2.11 se puede observar la estructura de un sistema SCADA la cual básicamente se puede monitorear el proceso desde una laptop, celular o tableta entonces esta accede al SCADA y este luego hacia el PLC el cual finalmente llega al brazo mecánico.

El sistema de automatización mediante SCADA es un medio con el propósito de llegar a un meta debido que maximiza rendimientos a través de las operaciones tanto para los fabricantes como de las organizaciones. Aumentar la productividad de una manera eficiente y con calidad es lo que más destaca de este sistema.

Los sistemas SCADA consisten en:

- Una central de operación computarizada los cuales también son llamados como estación o terminal master la cual controla todo el sistema y a su vez informa al operador que todo el sistema funciona correctamente.

- Unidades de control remoto o también conocidos como controladores lógicos programables los cuales interactúan con todo el campo de actuadores, válvulas sistemas analógicos.
- Su sistema de comunicación es utilizado para transferir los datos del dispositivo hacia un host el cual puede ser un sistema telefónico, radio o satélite.
- El software soporta sistemas enteros mediante una conexión de software la cual implementa comunicaciones en Las unidades terminales remotas o como sus siglas lo indican RTU y principalmente en su host central el cual puede ser una computadora la cual proporcionara a los operadores una interfaz gráfica capaz de representar datos y este actúa como un centro de control. Estos dispositivos ya son conocidos como sistemas de interfaz hombre maquina o HMI.

El desempeño de estos sistemas es factible aplicándolos a procesos de áreas de planta, son sencillos de operar, controlar y supervisar, dichos sistemas no necesitan una asistencia frecuente por parte del usuario para poder funcionar.

Estos sistemas pueden ser utilizados en:

- Redes de transmisión eléctrica, las cuales cuentan con miles de kilómetros cuadrados, al momento de realizar algún cambio de carga en las líneas es indispensable que exista el control de interruptores de manera inmediata.
- Plantas energéticas que cuentan con funcionalidad hidráulica, estas dependiendo de la respuesta de la demanda pueden encenderse o apagarse, por lo general su ubicación es en lugares alejados y son controladas de manera remota para la apertura de válvulas y cierre de tuberías, es indispensable que en estos casos sea supervisado de manera frecuente y debe tener una respuesta inmediata.
- Redes de tubería, pueden transportar gases, fluidos químicos o petróleo o incluso agua, cuentan con sensores los cuales se encuentran ubicados en diferentes

segmentos respecto al punto de control, la función en estos casos es de la apertura y cierre de válvulas, encendidos y apagados de bombas, deben responder de manera inmediata debido que pueden llegar a ser peligrosos o inestables ya que suelen ser sustancias sensibles.

Estos sistemas han evolucionado con el pasar de los avances tecnológicos y han sido instalados exitosamente demostrando un gran desempeño respecto a la supervisión y control.

2.4.1. Process Field Bus

El Process Field bus o como se lo conoce comúnmente PROFIBUS este es un bus de campo abierto el cual se lo utiliza en procesos de fabricación y automatización. Es utilizado como medio de transferencia de datos y cuenta con todas las características de una red de comunicación industrial.

Este bus de campo permite la interacción entre controladores, actuadores y sensores en ambientes industriales, este reemplaza el cableado en las líneas de producción reduciendo costes de diseño e instalación y otorga un mejor control mejorando el sistema para mejorar la productividad. (Profiworks, 2022).

Entre sus principales usos es en aplicaciones como calefacción, refrigeración, control de bombas, automatización de industrias y automatización de procesos.

Figura 2. 12: *Siemens Scalance M804PB conectado a cables ethernet y Profibus /MPI.*

Fuente: (Siemens, 2018).

En la Figura 2.12 se puede observar un Profibus conectado a un router industrial, al utilizar este cable simplifican la conexión.

El funcionamiento de este dispositivo integra TIA portal cloud connector el cual facilita a los usuarios conectarse de manera sencilla a los Profibus existentes hacia herramientas de software industriales.

Figura 2. 13: *Tablero de control conectado por Profibus.*

Fuente: El Autor

2.4.2. Protocolos de comunicación de un SCADA

La arquitectura de estos sistemas consiste en un host centrar, en el cual opera el software HMI y diversos RTUs los cuales recogerán la información y la recibirán comandos de los operadores centrales.

Un protocolo de comunicación SCADA significa transferencia de data y comandos emitiendo una arquitectura esclava. Los protocolos más utilizados existen tres, los cuales son: IEC 60870-5, Modbus y DNP3 el cual este de aquí es más utilizado en el sector de energía.

Todos los protocolos mencionados son basados en TCP/IP el cual es el protocolo de transmisión el cual permite establecer una conexión y el intercambio de datos entre dispositivos. (Robledano, 2019).

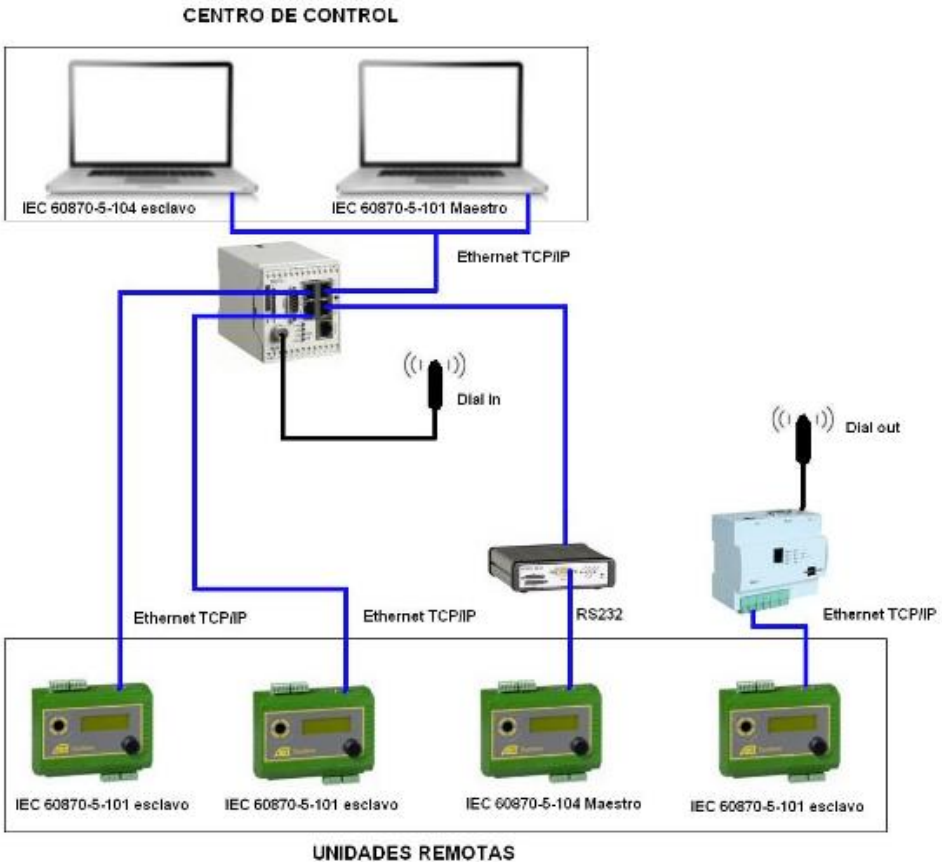


Figura 2. 14: *Protocolo IEC 60870-5*

Fuente: (Sumelco, 2021).

En la Figura 2.14 se puede observar un centro de control con el protocolo IEC el cual es una norma internacional estructurada para controlar sistemas de energía, de control y comunicaciones derivadas.

Según (Siemens, 2019) para poder implementar los protocolos con la norma IEC 60870-5 se ha logrado que los sistemas y las instalaciones que interactúen con técnicas de control remoto o estaciones de fabricantes que se puedan comunicar entre si sin la necesidad de utilizar adaptaciones adicionales. Estos protocolos cuentan con diferentes estándares la cual hace que la norma 60870-5 se divida en diferentes partes:

- IEC 60870-5-101: Normativa que afecta a las aplicaciones para las tareas de supervisión remota (comunicación serie).
- IEC 60870-5-102: Funciones básicas para la transmisión de valores de contaje.
- IEC 60870-5-103: Normativa para la transmisión de avisos de protección (dentro de una instalación de aparellaje).
- IEC 60870-5-104: Normativa que afecta a las tareas de supervisión remota en redes IP. (Siemens, 2019)

En el caso que se necesite implementar estos protocolos con el SIMATIC S7-1500 y las librerías SIPLUS RIC con una SIMATIC S7 tarjeta de memoria adecuada.

Para mantener segura la infraestructura tecnológica, los sistemas, máquinas y redes contra ataques cibernéticos es necesario implementar y mantener el concepto de seguridad IT holístico de última generación. Con esto se quiere decir que la ciberseguridad siempre está avanzando y mejorando de manera rápida, requiere una respuesta consolidada de todos los involucrados.

2.4.3. LabVIEW para la monitorización SCADA

Es una plataforma la cual es amigable y sencilla de utilizar, es utilizada tanto en universidades como en empresas para la monitorización de un sistema. Cuenta con una interfaz gráfica completa la cual sirve para diseñar y programar algoritmos de control en tiempo real, además que dicho programa se lo puede trabajar en cualquier entorno brindando así la posibilidad de acceder al sistema SCADA mediante diferentes navegadores ya sea Google Chrome, Mozilla Fire Fox o Microsoft Edge. (Jorge Juan Rosillo Olmos, 2022).

2.4.4. Interfaz Hombre Maquina

Es una interfaz de usuario asistida por ordenador que forma parte del programa informático que se comunica con el usuario. La HMI es el punto de acción en que un hombre entra en contacto con una máquina y en ella se

presenta el manejo de la máquina, la visualización del proceso, alarmas, historial, informes de producción, entre otros. Además, WinCC se presenta con una mejora en la eficiencia de la ingeniería que puede reducir los tiempos de trabajo.

La ciberseguridad define y explica los diferentes conceptos que rigen la seguridad a través de internet. Esta abarca un abanico extenso de posibilidades de resguardo a nivel de protección de acceso, seguridad IT y seguridad de planta. WinCC incorpora una gestión de usuarios local, mediante la cual existe un registro de todas las acciones del operador. Cuenta con la incorporación de la encriptación SSL para la comunicación entre servidor y cliente. (Berdin, 2017).

2.5. Ciberseguridad en tecnologías de operación.

Actualmente en la industria existen procesos de digitalización en los diferentes sectores que la componen, existen amplios rangos de amenazas en sus sistemas OT (Tecnologías de Operación).

Estas tecnologías se relacionan principalmente en fábricas de automatización y edificios, no es común encontrar un antivirus en estos dispositivos y sobre todo actualizarlos, se entiende que estas implementaran más sistemas de seguridad a futuro debido a la triada CIA que en la comunidad informática estas siglas hacen referencia a Confidencialidad, Integridad y Disponibilidad dichas siglas están en orden de importancia y los expertos en seguridad OT deben hacer todo lo posible para que no exista peligro en las instalaciones de producción.

Según (Siemens, 2019) relata sobre un ataque cibernético realizado por hackers los cuales lograron acceder al sistema de tecnología de operación de un tratamiento de agua en Florida Estados Unidos, en dicho suceso se trató de envenenar el suministro de agua aumentando la cantidad de hidróxido de sodio.

Existen razones por las cuales grandes empresas e industrias no actualizan la seguridad de los dispositivos de automatización y es que, si algo sale mal durante la actualización, la producción se detiene generando

perdidas enormes, los hackers o también conocidos como piratas informáticos tienen como objetivos hospitales, oleoductos, fábricas de automatización y obras hidráulicas como objetivo de extorsión.

2.6. Industria 4.0

También conocida como cuarta revolución industrial, sería la implementación del internet de las cosas con la industria, el internet 4.0 es el cual hace referencia a la manera de producir servicios a gran escala, el uso del internet a gran escala cuenta con requerimientos técnicos diferentes a los demás.

Se tiene el mercado de consumo el cual cuenta con gran demanda en hogares inteligentes, dispositivos integrados como relojes inteligentes monitores y asistentes virtuales en cambio en el mercado industrial se deben tomar en cuenta requerimientos técnicos, audiencias, estrategias. Estas pueden estar ubicadas en pequeñas, medianas y grandes empresas y cuentan con la fabricación y producción de una gran cantidad de equipos.

Como ejemplos de esta cuarta revolución industrial se tienen los siguientes: Realidad virtual, Internet de las cosas, Manufactura aditiva, Big Data.

2.6.1. Tecnología 4.0 en el Ecuador

En el Ecuador la Universidad Técnica Particular de Loja (UTPL) y Epson contribuyeron al estudio y desarrollo hacia la industria 4.0, las carreras de computación y tecnologías de la información de la UTPL junto con Epson inauguraron un laboratorio de robótica en el campus de la universidad con la finalidad de contribuir en el desarrollo de la industria 4.0 en el país.

Juan Pablo Suárez, director del Parque Científico y Tecnológico de la UTPL, señaló que “el laboratorio permitirá que, desde la universidad, se desarrollen soluciones industriales a problemas globales”. Además, resaltó la importancia de comenzar a trabajar en prototipos que contribuyan a la automatización de procesos, manejo de datos e implementación de

inteligencia artificial en beneficio del ecosistema empresarial local. (Universidad Tecnica Particular de Loja, 2022).

Esta universidad tuvo la oportunidad de adquirir robots industriales para beneficiar a los alumnos y así desarrollar y aprender sobre nuevas tecnologías con la modernización y automatización de procesos. El laboratorio de robótica cuenta con cuatro robots industriales que ayudaran con el aprendizaje de los estudiantes y para el desarrollo de investigaciones.

La tecnología 4.0 crece y debido a esto se realizó un lanzamiento de un programa llamado Guayaquil 4.0 el cual busca soluciones innovadoras para impulsar las competencias tecnológicas de Guayaquil, como objetivo de reducir costos, optimizar recursos y contribuir con la generación de empleo al desarrollar actividades de alto impacto.

Según enfatiza (Vinueza, 2021) gerente general de EPICO "Queremos acortar la brecha tecnológica relacionada con la Industria 4.0 y entregarle a la ciudad proyectos con soluciones innovadoras para el sector agroexportador. Para esto, trabajamos desde ya junto a los representantes de toda la cadena de valor para diagnosticar su nivel de madurez, identificar productos, programas o iniciativas de alto impacto y fortalecer las capacidades de pequeñas y medianas empresas, que representan el 85% de la generación de empleo y productividad del país".

2.6.2. Inteligencia artificial como respuesta a la industria 4.0

La inteligencia artificial o como sus siglas lo indican IA hace referencia a máquinas y sistemas las cuales imitan y mejoran la inteligencia humana mediante la información que recopilan.

Se ha convertido en una tecnología utilizada para revolucionar modelos de gestión en la industria, se enfrasca en mejorar la optimización de la eficiencia general de los equipos o como sus siglas en ingles OEE(Overall Equipment Effectiveness), en la calidad 4.0 la cual es la encargada de la mejora de la producción, en diseño generativo que mediante algoritmos de IA y automatización generan diversas soluciones de diseño en un objetivo y en

la robótica la cual mediante las grandes maquinas robóticas apoyan a los usuarios para realizar tareas metódicas o precisas.

La IA es utilizada por diversas empresas, estas utilizan chat automatizados o también conocido como Bot, estos responden con mensajes automáticos para proporcionar respuestas eficientes a los clientes. Así mismo la inteligencia artificial es utilizada actualmente en hogares inteligentes, son más conocidos como asistentes virtuales, los cuales son utilizados para ayudar con la automatización del hogar.

Figura 2. 15: *Aumento en la productividad.*

Fuente: (Redaccion APD, 2021).

La inteligencia artificial en empresas e industrias mejora la productividad realiza las tareas de manera eficiente, en la Figura 2.15 se puede observar una representación gráfica sobre el código de la IA.

2.7. Políticas de ciberseguridad en Ecuador.

En el presente año 2022 el Ecuador se rige con las políticas de ciberseguridad del año 2014, las cuales se presentan a continuación:

- **Articulo 229- Revelación ilegal de base de datos**

La persona que, en provecho propio o de un tercero, revele información registrada, contenida en archivos, bases de datos o medios

semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años. (Codigo Organico Penal, 2014).

- **Articulo 230- Interpretación ilegal de Datos**

La persona será penalizada con privación de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas

informáticos destinados a la comisión del delito descrito en el inciso anterior. (Codigo Organico Penal, 2014).

- **Articulo 231- Transferencia electrónica de activo patrimonial.**

La persona que destruya dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. (Codigo Organico Penal, 2014)

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. (Codigo Organico Penal, 2014)

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (Codigo Organico Penal, 2014)

Capítulo 3: Aportaciones del estudiante e interpretación de resultados

En este capítulo se hablará sobre 2 empresas ubicadas en el Ecuador en la ciudad de Guayaquil que utilizan los programas y software mencionados anteriormente en el capítulo 2, se hará la mención a las empresas contifico impulsada por Siigo y de Procontrolmatsa ya que son lugares que brindan mayor accesibilidad al autor.

Se desarrollan los objetivos específicos los cuales fueron elaborados en el capítulo 1 referente al tema de investigación. Se redactó la formulación del problema, además de esto se abordará con la obtención de objetivos específicos, actividades desarrolladas y elaboradas para esta investigación con la finalidad de brindar un resultado y solución al problema de la investigación.

Se procedió en el capítulo 2 a abordar el primer objetivo específico el cual es fundamentar las teorías de ciberseguridad.

Se abordo el segundo objetivo específico sobre como identificar las vulnerabilidades y las herramientas utilizadas por los ciberdelincuentes las cuales están expuestas desde el numeral 2.2 hasta el 2.2.5.

3.1. Descripción geográfica e infraestructura de los sitios

La ciudad de Guayaquil está compuesta por 347 km^2 de superficie de los cuales 316 km^2, equivalentes al 91.9% del total, pertenecen a la tierra firme suelo, mientras que los restantes 29 km^2, equivalente al 8.1% pertenecen a los cuerpos de agua que comprenden ríos y esteros. En la Figura 3.1 se puede observar de manera geográfica la ciudad de Guayaquil

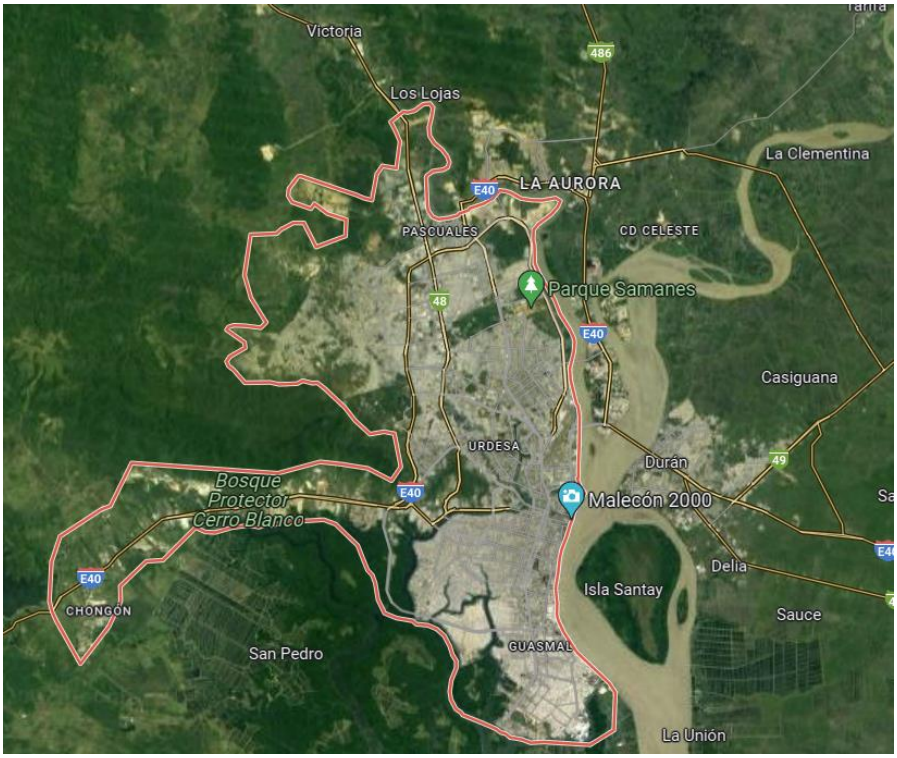


Figura 3. 1: *Vista geográfica de la ciudad de Guayaquil*

Fuente: Autor.

En la Figura 3.2 se puede observar una vista de manera geográfica del edificio de la cámara de comercio en Guayaquil, lugar donde se encuentra ubicada la empresa Contifico impulsada por Siigo en la torre A piso mezanine oficina 3, es una empresa multinacional de facturación electrónica la cual cuenta con un equipo del área del Tecnología en la cual la parte de infraestructura o soporte IT se encarga del mantenimiento de los equipos informáticos de manera presencial para la oficina de Guayaquil y de manera remota para los países como Colombia, Perú Uruguay y México.

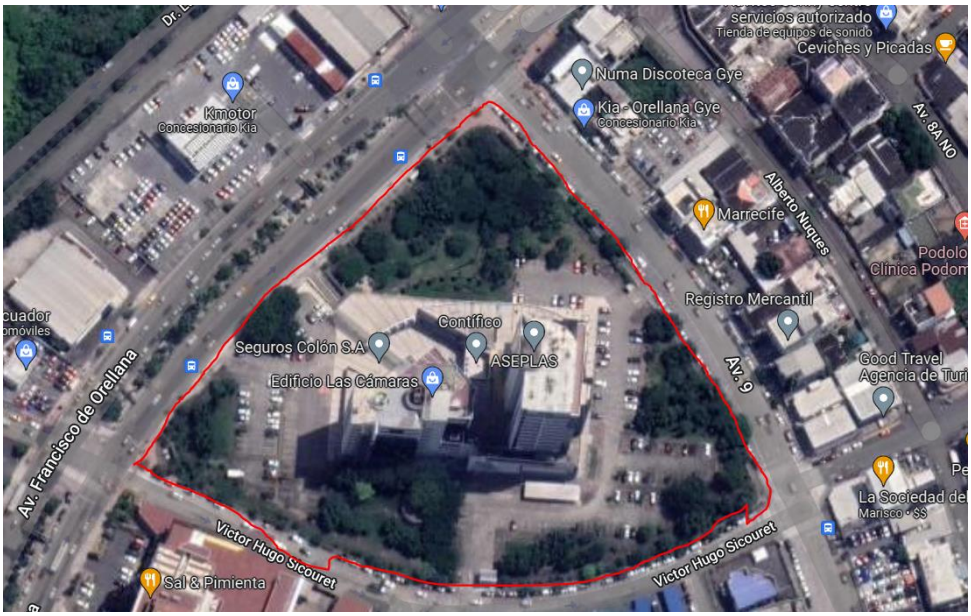


Figura 3. 2: *Vista geográfica de la empresa contifico impulsada por Siigo ubicada en el edificio las cámaras.*

Fuente: Autor.

Se encuentra ubicada en la Avenida Francisco de Orellana y Víctor Hugo Sicouret en la ciudad de Guayaquil, cuenta con dos torres las cuales la torre A cuenta con 7 pisos y la torre B cuenta con 17 pisos.

Figura 3. 3: *Empresa Procontrolmatsa.*

Fuente: Autor.

En la Figura 3.3 se puede observar de manera geográfica proporcionada por Google Maps a la empresa Procontrolmatsa ubicada en la ciudad de Guayaquil-Ecuador en la ciudadela Bellavista Manzana 22 Solar24 al norte de la ciudad

3.2. Vulnerabilidades en los sistemas informáticos.

En este apartado se hará mención sobre las vulnerabilidades de los sistemas informáticos tanto como para la empresa como para los sistemas SCADA. De esta manera se responderá al objetivo específico dos.

3.2.1. Vulnerabilidades de los sistemas SCADA

Estos sistemas por lo general son diseñados como sistemas aislados y autónomos los cuales utilizan enlace de datos utilizando la red netamente para transmitir información y datos. En su mayoría los sistemas SCADA carecen de medidas de seguridad como firewalls, antivirus o mecanismos de cifrado, estas cuentan con vulnerabilidades técnicas, las cuales es común que los SCADA se encuentren vinculadas con las redes de las empresas sin ningún tipo de separación o control de acceso.

En el Ecuador, es frecuente que los equipos personales sean utilizados para la programación y manejo de los sistemas en una empresa. Por lo general, estos equipos portátiles como laptops no suelen contar con software de protección, creando así una puerta de enlace haciendo posible que los hackers logren atacar la red a la cual están conectados estos dispositivos. Es importante resaltar que basta con que una máquina de la red local de una empresa sea atacada para que estos ciberdelincuentes tengan acceso y control total a la red SCADA.

Estos sistemas son sensibles a escaneos de red, suelen contar con IP fáciles de ser vulnerables ante ataques informáticos. Por lo general, los atacantes utilizan de manera autónoma un escaneo de puertos, el cual les permite identificar cuáles de estos se encuentran vulnerables para lograr de esta manera el ataque hacia los sistemas.

Los sistemas SCADA al estar utilizando redes WAN suelen presentar problemas de seguridad, debido que su conexión permite la comunicación de manera remota. Estos sistemas suelen ser compatibles con plataformas como Windows, haciendo que sean vulnerables a los ataques tradicionales como agujeros de gusano, troyanos, spyware y entre otros virus.

3.2.2. Peligros del uso de programas sin licencia

Es común encontrarse con una llave o el cracked, por llave se quiere decir que es un virus como tal el cual su función es burlar la seguridad el programa que se quiere utilizar para poder utilizar funciones premium o funciones de paga, estos programas no solo son utilizados por alumnos de universidad, también son utilizados por empresas. Existen plataformas tales como LabVIEW o PLC studio 5000 las cuales son utilizadas para programar o modificar valores en un PLC.

Estas empresas suelen ser vulnerables ante ataques debido que los empleados utilizan programas piratas debido que las empresas no proporcionan herramientas adecuadas para que el operador pueda trabajar de una manera más segura.

Es de suma importancia tener el equipo protegido al igual que la información digital tanto de la empresa como personal del usuario, al momento de utilizar dichos programas crackeados la empresa y el operador corre el riesgo que la información sea expuesta ante cualquier ciberdelincuente, hay que recordar que la información tiene un gran valor en el internet y al momento de descargar estos programas los cuales proporcionan accesos premium de manera gratuita, es importa recordar que nada es gratis. Al acceder a estas plataformas estamos abriendo una puerta a que la información de dicha maquina sea expuesta. Otro de los riesgos es que el programa no pueda funcionar o que algunas funciones o características no estén disponibles.

Un riesgo muy común es el acabar infectado con malware, al momento de descargar un programa pirata es muy seguro que este se encuentre infectado con virus, troyanos o keylogger. Entonces en una empresa esto puede afectar a otros equipos los cuales se encuentran

conectados a la red, algunos de estos programas suelen instalar softwares adicionales, así como se lo mencionó en la sección 2.2.5, al momento que se instala un software adicional esta puede recopilar información personal o puede contener adware y afectar el sistema de diferentes maneras.

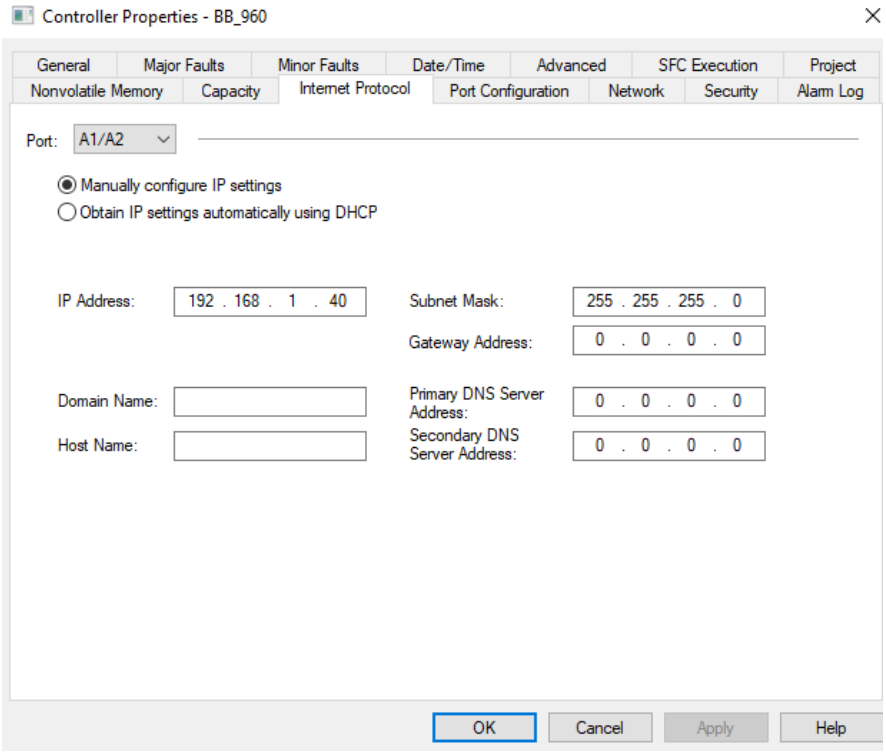


Figura 3. 4: *PLC studio 5000 se muestra las propiedades de control en la empresa PROCONTROLMATSA*

Fuente: El Autor.

En la Figura 3.4 se puede observar la ejecución del programa PLC studio 5000 en la cual está mostrando la dirección IP. Se puede observar que el sistema operativo de la maquina no se encuentra activado, por lo cual no cuenta con actualizaciones de seguridad y puede ser un riesgo para la empresa.

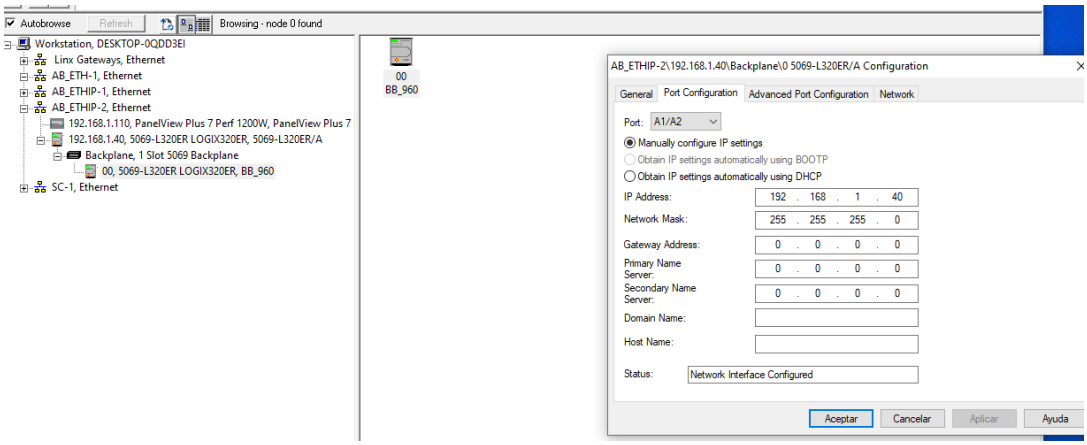


Figura 3. 5: *Configuracion de los puertos del PLC utilizando PLC studio 5000 en la empresa PROCONTROLMATSA*

Fuente: El Autor.

Como se aprecia en la Figura 3.5 se ingresó a la configuración del PLC studio 5000 para poder configurar el PLC, aquí se modifica la dirección IP para poder configurar los puertos

Las llaves o activadores existen para diversos programas y para diferentes sistemas operativos. Dentro del software LabVIEW podemos encontrar el activador de licencias de National Instruments, el cual sirve para liberar funciones premium de sus diferentes paquetes de software. Al momento de instalar este activador es necesario desactivar el antivirus debido que luego este lo bloquea. Las llaves de activación en si son virus informáticos controlados con la finalidad de solo activar el programa, pero el asunto está en que se comparte información personal del pc hacia quien creo esta llave desactivación, debido que en el internet lo más valioso es la información.

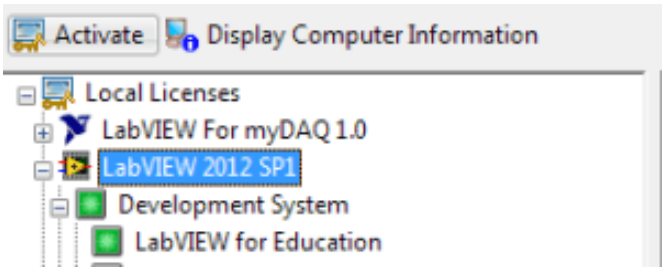


Figura 3. 6: *Activador de National Instruments.*

Elaborado por: Autor.

Como se puede ver en la figura 3.6 se tiene el activador de LabVIEW en el cual se puede seleccionar que funciones desbloquear del programa para poder acceder a contenido premium de manera gratuita.

3.3. Métodos de protección en los sistemas informáticos en Ecuador – Guayaquil en la empresa contifico impulsada por Siigo y Procontrolmatsa.

Antes de mencionar los métodos de protección en los sistemas informáticos, es importante conocer sobre como el Ecuador aumentó sus casos de ataques cibernéticos.

Según (Agencia EFE, 2021) durante la pandemia se registrador un mayor porcentaje de ataque en el país llegando así a tener un 75% de ataques diarios según datos de Kaspersky, esto se debió a que el país entro a la modalidad de teletrabajo.

Los ataques cibernéticos aumentaron debido a la virtualidad, esto se debe a que empleados suelen utilizar programas piratas, licencias falsas y algunos no cuentan con algún antivirus. Actualmente según la agencia citada en el párrafo anterior, el Ecuador se encuentra en la posición número 40 de los países con más ataques cibernéticos en el mundo según estadísticas en tiempo real de Kaspersky.

Para tener un sistema seguro es recomendable:

- Contar con actualizaciones.
- Licencias originales de programas.
- Tener contraseñas alfanuméricas.
- Contar con un gestor de contraseñas.
- Tener un antivirus actualizado y con una suscripción.
- Utilizar paginas confiables.
- No descargar archivos o programas de dudosa procedencia.

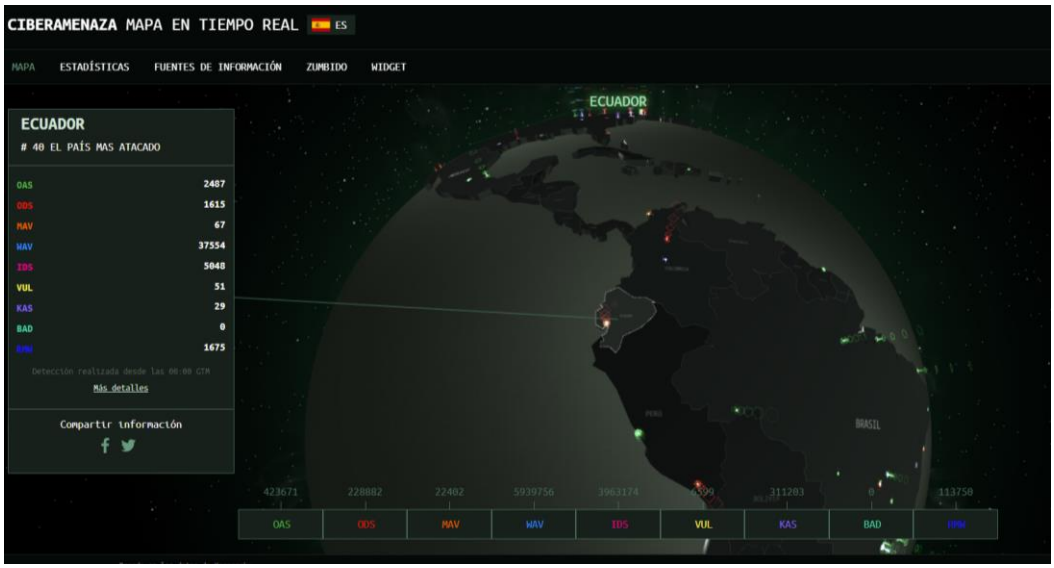


Figura 3. 7: *Análisis actual del mes de agosto de 2022.*

Fuente: Autor (Cybermap Kaspersky).

Figura 3. 8: *Análisis del mes de agosto*.

Fuente: El Autor.

En la Figura 3.7 como se puede observar se muestra el análisis en tiempo real del mes del día 7 de agosto del presente año. Se utilizo el ciber-mapa proporcionado por Kaspersky para visualizar el análisis.

Con la finalidad de comprender mejor la Figura 3.8 se realizó una tabla en la cual se explicará las siglas y los valores leídos.

Tabla 3. 1: Explicación de las siglas de la Figura 3.8

QAS	Escaneos realizados por el usuario	2487
ODS	Escaneos en demanda	1615
MAV	Mail Antivirus	67
WAV	Web Antivirus	37554
IDS	Sistema de detección de intrusos	5048
VUL	Vulnerabilidades	51
KAS	Kaspersky Anti-Spam	29
BAD	Botnet detectados	0
RMW	Ransomware	1675

Fuente: Autor.

3.3.1 Programas utilizados

Respondiendo al objetivo específico numero 3 como método de protección en un sistema informático se utilizó el antivirus checkpoint, el cual es utilizado en una pequeña y mediana empresa o mejor conocido como Pyme del Ecuador llamada Siigo.

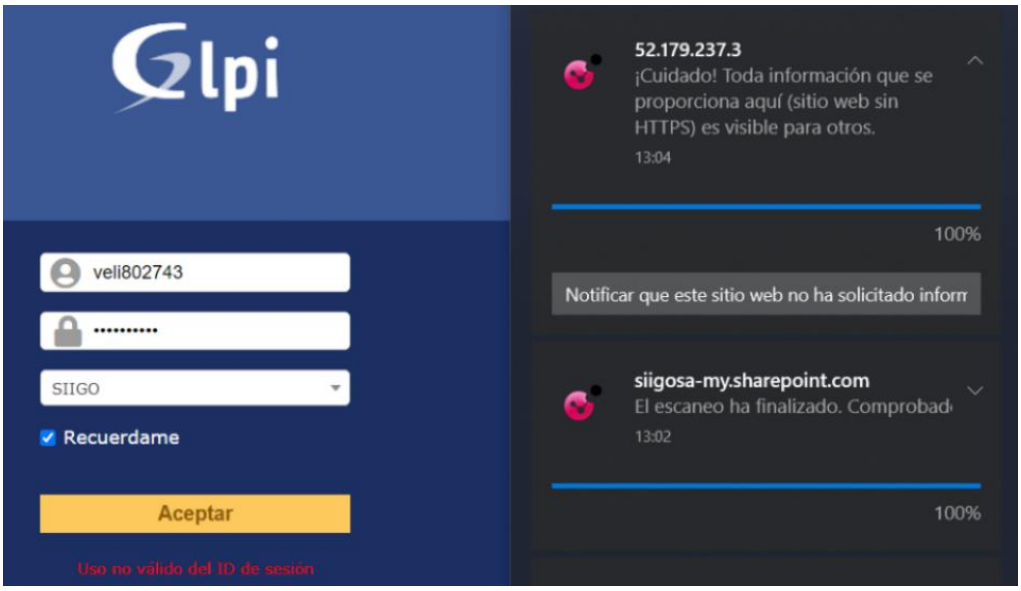


Figura 3. 9:*Checkpoint realizando el escaneo de sitio web*.

Fuente: El Autor.

Como se puede observar en la figura 3.9 el antivirus se encuentra analizando una página web antes de acceder. Checkpoint detecta si la página es segura o no, esta comprobación se realizó en una máquina de la empresa Siigo, además también muestra si es phishing y sobre todo en caso de que se trate de utilizar la misma contraseña para diferentes sitios, el antivirus advertirá que eso es inseguro por lo cual recomendara que no se use la misma contraseña mostrando los sitios en los cuales uno cuenta con la misma clave.

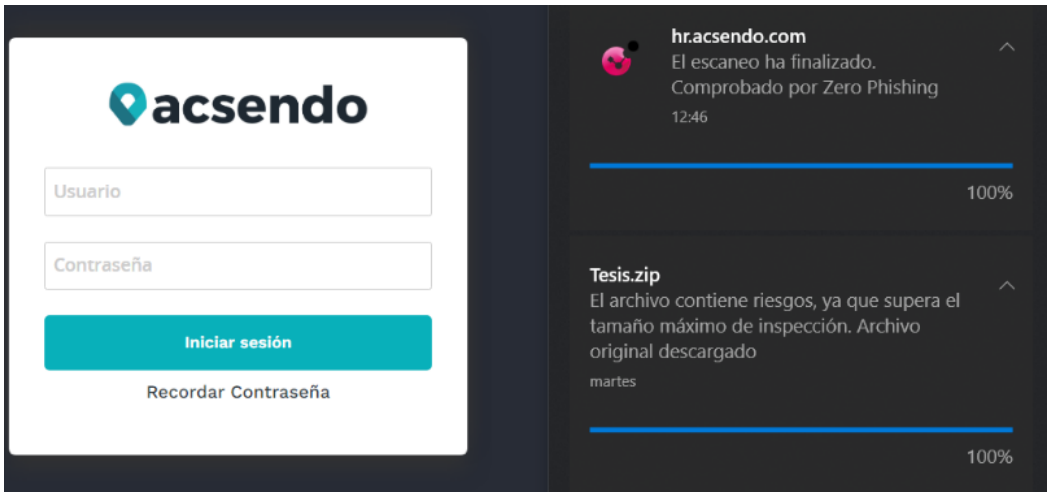


Figura 3. 10:*Checkpoint detectando que la pagina no contiene phishing.*

Fuente: El Autor.

Como se observa en la Figura 3.10 el antivirus escanea paginas nuevas en las cuales piden acceso de usuario, esta prueba fue realizada en una computadora de la empresa Siigo en la cual se abrió un enlace que redirigió a un sitio web llamado acsendo el cual sirve para el crecimiento profesional, la función del antivirus en este caso es verificar que la pagina sea confiable, no cuente con phishing y sobre todo que no se utilicen nombres de usuario o contraseñas utilizadas en otros sitios web.

Un método para la protección de datos en un sistema SCADA es SCADA Wall el cual es un firewall industrial utilizado para supervisar y regular el tráfico hacia y desde una red, con el fin de asegurar los dispositivos en una red. Además, analiza los datos que pasen por el dispositivo mediante un protocolo de vigilancia el cual se encuentra definido descartando datos que no cumplen con los requisitos del protocolo. (Mungekar Abhishek, 2020).

3.4. Medidas para la protección y prevención de los ciberataques en la industria 4.0.

En el proceso de implementación de soluciones en un Data Center se necesita una protección perimetral, para amortiguar el riesgo de las amenazas modernas los firewalls de siguiente generación más conocido por sus siglas en ingles NGFW (Next-Generation Firewall) gestionan el flujo tradicional de protocolos y puertos, como el análisis profundo de aplicaciones, usuarios y tráfico, estos pueden detener más amenazas con la finalidad de permitir que la organización optimice recursos.

Para tomar medidas de protección y prevención es necesario:

- identificar, contener y bloquear las amenazas desde el día cero y las amenazas insistentes.
- Identificar y controlar el acceso de los usuarios sobre las aplicaciones comerciales mediante políticas móviles, sociales y que cuente con un uso aceptable.
- Mediante una interfaz centralizada y proporcionar funciones de seguridad de la red para diferentes NGFW además de incluir la información obtenida a través de otros dispositivos de la red.

- Contar con un filtrado de URL en el cual los usuarios no puedan acceder a sitios web sospechosos como juegos y sitios web con contenido para adultos, con la finalidad de mitigar ataques de adware, phishing y spyware.

Shodan el cual es el motor de búsqueda utilizado en la seguridad de la información en la industria, esta es una herramienta para encontrar vulnerabilidades o encontrar sistemas mal configurados por ejemplo; si este realiza una búsqueda y revela que uno de los sistemas HMI o uno de los autómatas de la empresa es visible en internet, se puede detectar que el sistema se encuentra mal configurada , estas debilidades son causadas por sistemas no parcheados o por puntos abiertos que por stock no se modificaron. (Rentero, 2022).

Este motor de búsqueda puede ser también pirateado lo que lo hace vulnerable, por lo cual es recomendable utilizar una versión de paga. Los ciberataques contra entornos industriales es algo más común el cual sigue los esquemas dirigidos a empresas del sector de servicios.

Conpot y Shodan son buenas propuestas para que una empresa ponga en práctica su uso, para mejorar sus prácticas de ciberseguridad y resguardar las partes de las redes las cuales son de acceso público, así mismo se tiene Blue Coat en el cual este propone una estación de protección y análisis el cual protege sistemas industriales frente a malwares que pueden infectar mediante los periféricos USB del mismo modo se tiene Security Analytics Platform el cual propone un módulo SCADA en el cual identifica en tiempo real actividades potencialmente peligrosas.

3.4.1 Software para la monitorización de los equipos

Con la finalidad de identificar, contener y bloquear las amenazas es necesario contar con firewalls y antivirus con licencias originales, la ayuda de estas herramientas informaticas brindara al usuario proteccion ante sus datos e informacion.

En informatica existe un termino llamado “dia cero” el cual en pocas palabras quiere decir el primer dia en que existe un inconveniente. Entonces

tener un virus de dia cero se describe como un virus el cual es descubierto y no puede ser detectado o eliminado por el antivirus, el usuario al momento en que ve comportamientos extraños en su despositivo como el borrado de carpetas, archivos dañados, pantallazos azules o la maquina muy lenta, estos pueden ser indicios que el dispositivo esta infectado.

No existen maneras de prevenir estos ataques de dia cero, pero hay metodos para evitar ser victima de estos por lo que es necesario tener actualizados todos los programas del dispositivos, contar con las ultimas actualizaciones del sistema operativos, eliminar porgramas que ya no son utilizados, contar con antivirus actualizado y con licencia original

Como medida tomada para la proteccion y prevencion de ataques ciberneticos se utilizo el software de gestion de servicios de la tecnologia de la informacion mas conocido como GLPI, es de codigo abierto esto queire decir que se puede modificar, ejecutar o desarrollar ya que es libre y los modulos pueden ser modificados.

Se utiliza este software para llevar una gestion del sistema de informacion de una empresa, es capaz de crear un inventario en el cual se puede registrar las maquinas de una empresa y poder monitorear que programas o aplicativos tienen instalados, la ultima vez que encendio el computador, detectar el antivirus que tiene instalado, a que punto de red se ha conectado el dispositivo, entre otros apartados.

A continuacion se mostraran capturas de pantalla de la interfaz del GLPI y como es su uso en una empresa, por temas de ciberseguridad los datos como nombres,apellidos,direcciones, correos o cualquier otro dato que pueda poner en peligro a la empresa o al usuario seran censurados.

Para poder filtrar paginas no deseadas y la proteccion de datos es necesario contar con antivirus que permitan realizar estos controles como antivirus recomendados ya que fueron utilizados son sophos y checkpoint.

Nombre	Sistema operativo - Nombre	Complementos - FusInv - Last inventory	Usuario	Datos financieros - Número de activo	Datos financieros - Número de pedido	ID	Localización
MU[redacted] 13	Windows	2021-12-23 14:50	[redacted] Muñoz Antepara	P-2[redacted]		3 [redacted]	Ecuador
AA[redacted]	Windows	2022-08-26 08:32	[redacted]			3 [redacted]	Mexico
AB[redacted] 11	Windows	2022-08-26 08:02	[redacted]	ML-15[redacted]	37.3[redacted]	79[redacted]	Bogota
AB[redacted]	Windows	2022-08-26 15:58	[redacted] Arevalo	5[redacted]		3[redacted]	Bogota
AB[redacted] 11	Windows	2022-08-26 13:16	[redacted]	ML-[redacted]	27.9[redacted]	2[redacted]7	Bogota
AC[redacted] 11	Windows	2022-08-26 09:56	[redacted]	FP[redacted]2	35.[redacted]	3[redacted]7	Guayaquil
AC[redacted] 11	Windows	2022-08-26 08:05	[redacted]	0[redacted]6	37.1[redacted]	3[redacted]6	Bogota
AC[redacted] 12	Windows	2022-08-26 08:49	[redacted]	M[redacted]0	31[redacted]	3[redacted]4	Barranquilla
AC[redacted] 11	Windows	2022-08-25 17:11	[redacted]	M[redacted]9	22[redacted]	7[redacted]	Medellin
AC[redacted] 11	Windows	2022-08-26 14:19	[redacted]	3[redacted]	38.[redacted]	3 [redacted]	Barranquilla

Figura 3. 11: *Software GLPI mostrando usuarios en el sistema*

Fuente: El Autor.

En la figura 3.11 se puede apreciar la interfaz del GLPI en la cual muestra una base de datos en tiempo real de los usuarios que se encuentran en una empresa, como se indicó anteriormente este software permite monitorear al usuario, se puede observar el ultimo ingreso y ubicación de la persona.

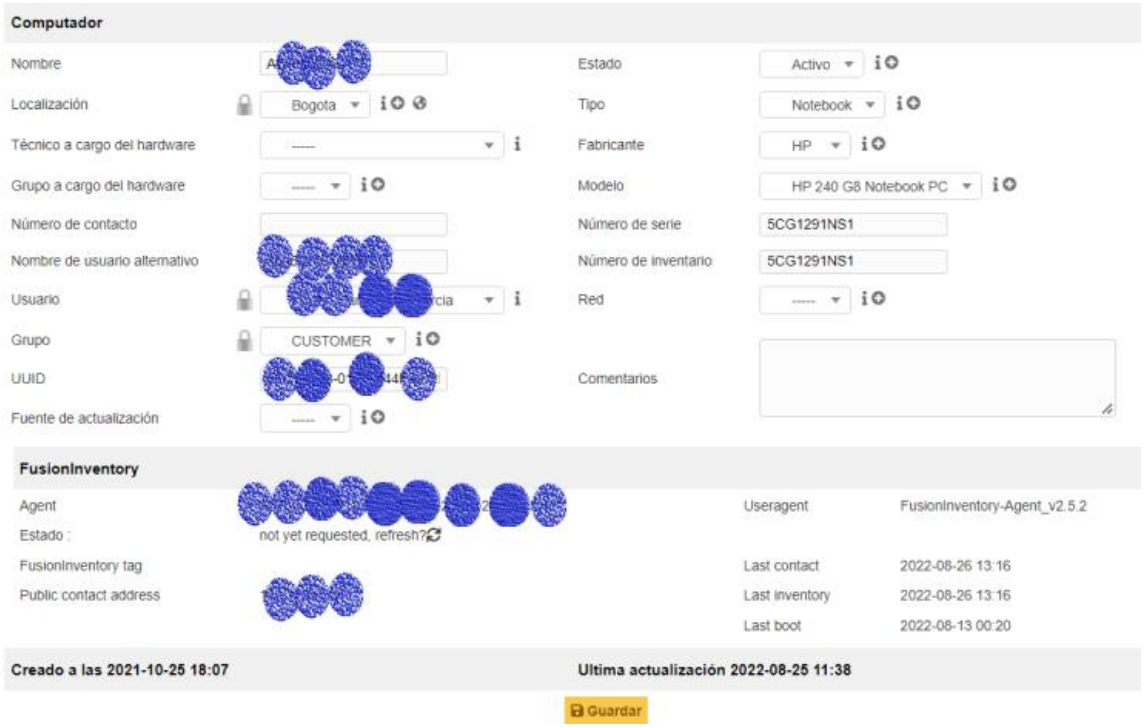


Figura 3. 12: *Visualización de las características del dispositivo*

Fuente: El Autor.

En la figura 3.12 se puede observar las características del dispositivo como el nombre y modelo del equipo, a que área pertenece y la ubicación.

Figura 3. 13: *Información de internet del dispositivo.*

Fuente: El Autor.

En la Figura 3.13 se puede observar las redes IP y que tipo de wifi tiene el dispositivo y también la dirección IP, por temas de ciberseguridad esto se encuentra censurado. De esta manera se puede monitorear el dispositivo para saber a qué redes se encuentra conectado o a cuáles se ha conectado.

Análisis del Glpi: Según lo investigado esta plataforma al ser libre no obstante es pagada, debido que protege los datos de las empresas que la utilizan, este software es moldeable puesto que se puede modificar el código a conveniencia. Es eficaz para crear una base de datos, como ejemplo se puede obtener una base de datos de las computadoras que cuenta una empresa o en el caso de una fábrica se puede obtener información sobre los dispositivos que se encuentren operando, basta con agregar al dominio e incluir el programa en el dispositivo. Permite estandarizar procesos, reducir costes y optimizar la productividad del personal.

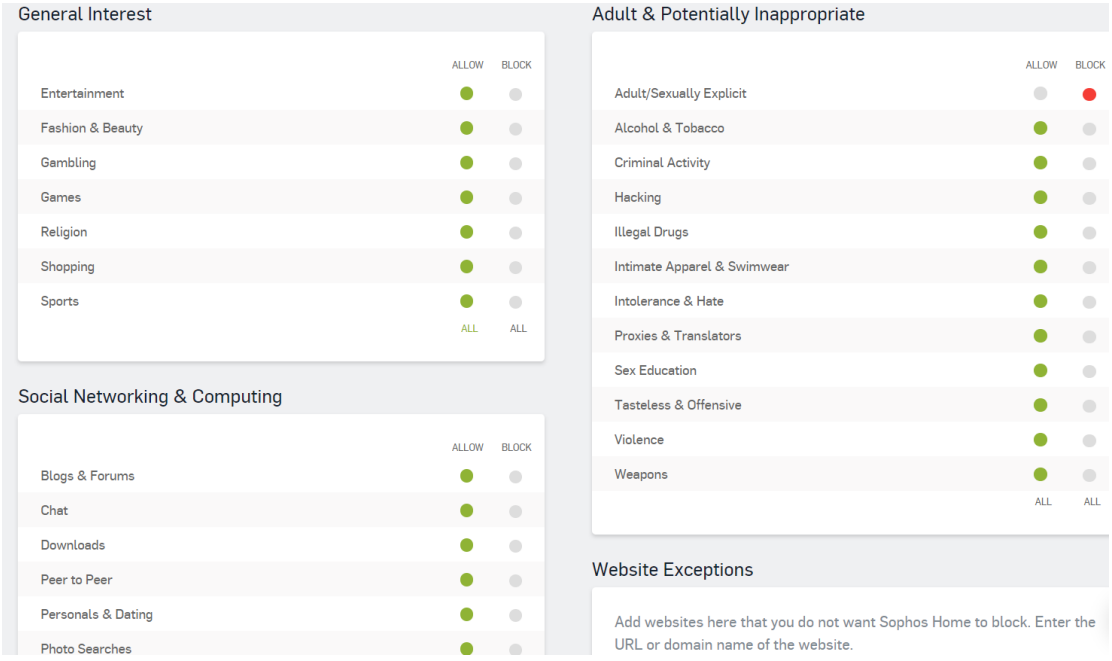


Figura 3. 14: *Monitorización y control de sitios*

Fuente: El Autor.

En la Figura 3.14 se puede observar como por medio del antivirus se puede restringir contenido en la web, para de esta manera prevenir ransomware, spyware, adware u otra clase de virus informáticos no deseados.

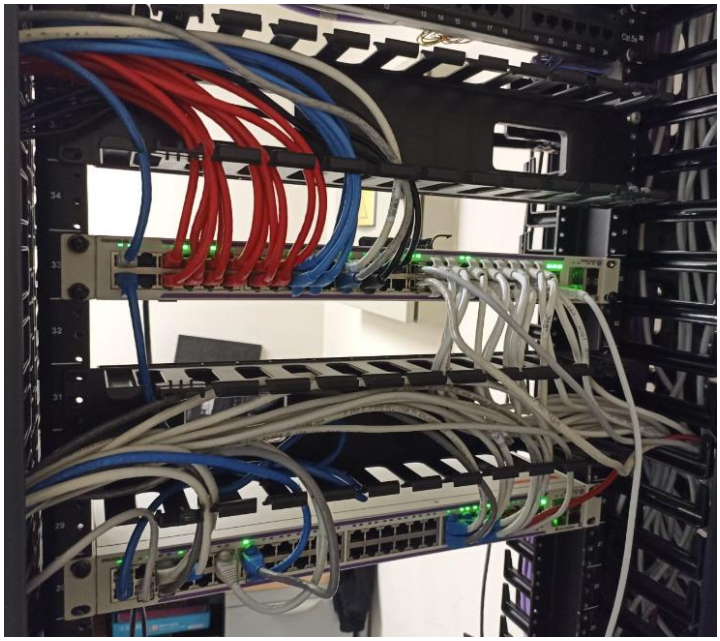


Figura 3. 15: *Data center de siguiente generación.*

Fuente: El Autor

En la Figura 3.15 se puede observar un data center de siguiente generación el cual cuenta con 48 puertos este permite mantener una red estable en una empresa al igual que su información, conexiones y datos. Por seguridad de la empresa no es permitido agregar el modelo de este data center.

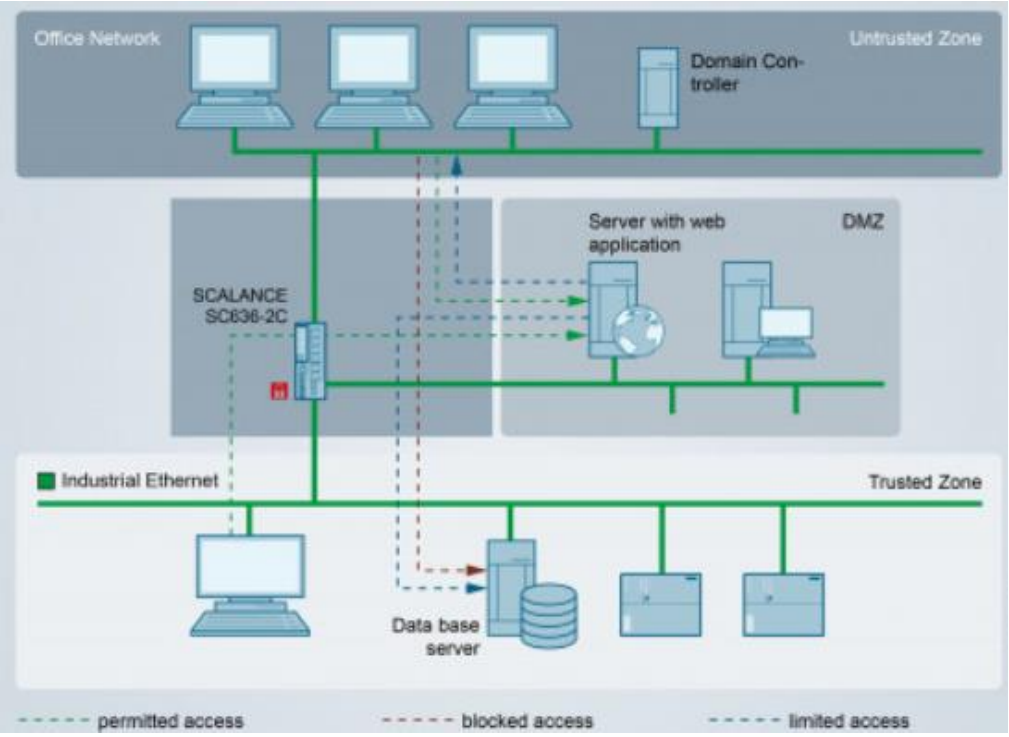


Figura 3. 16: *Componentes de red de ciberseguridad*

Fuente: (Lopez, 2020)

La Figura 3.16 muestra un diagrama sobre los componentes de red de ciberseguridad, se puede observar lo que se conoce como segmentación de redes el cual permite impedir que inconvenientes o ataques sufridos por otras se propaguen por la planta, así de esta forma habilita el paso de las comunicaciones imprescindibles entre las áreas. Los dispositivos que se encuentran dentro del dominio de la empresa se encuentran protegidos en tiempo real, los firewalls centrales pueden controlar solicitudes de acceso de diferentes lugares.

A su vez es posible controlar y reducir la carga de una red, la transmisión de datos hacia las diferentes áreas o también conocidas como células, pueden ser filtradas utilizando una Virtual Protect Network (VPN) para así proteger a los dispositivos ante espionajes u ataques cibernéticos. (Lopez, 2020)

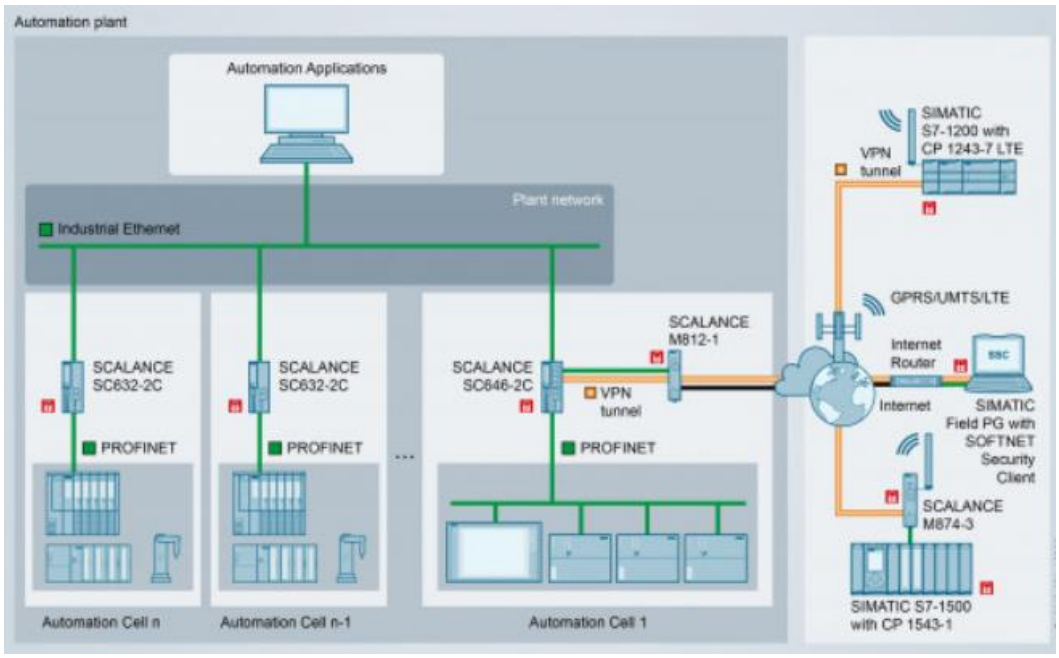


Figura 3. 17: *Procesadores de comunicaciones de seguridad para el sistema de automatización Simatic S7*

Fuente: (Lopez, 2020)

En la figura 3.17 se puede observar una comunicación remota segura, esto quiere decir que la instalación se encuentra conectada a internet para así poder realizar mantenimiento o controlarla desde cualquier parte del mundo, mientras se cuente con acceso a internet, es necesario asegurarse que los nodos de comunicación se encuentren autenticados, los datos se encuentren encriptados y protegidos.

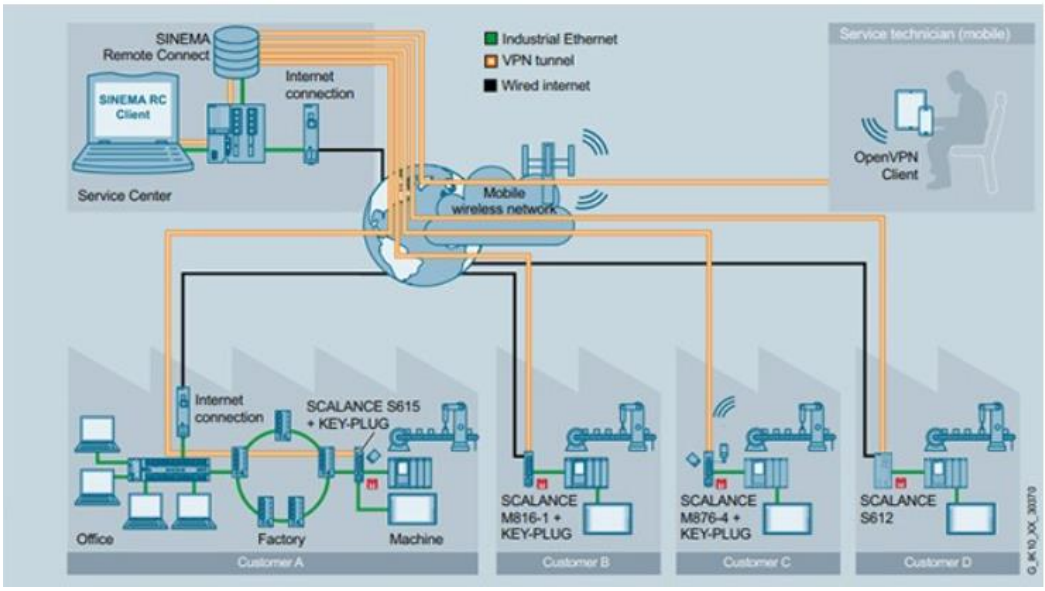


Figura 3. 18: *Integridad del sistema*

Fuente: (Lopez, 2020).

En la Figura 3.18 se puede observar un diagrama sobre un sistema SCADA y una Interfaz Hombre Maquina (HMI). En este ejemplo de configuración de un SCADA se puede observar que se tiene una central de servicio la cual esta conectada a internet y esta a su vez se conecta a los dispositivos como computadoras, maquinas y fabrica, utilizando una VPN para poder cifrar los datos.

La protección del nivel de control hace referencia a los sistemas de protección actuales, los cuales tienen mejor funcionalidad debido que brindan tareas como mantenimiento, leer y escribir variables.

3.4.2 Descripción de los instrumentos, herramientas y procedimientos de la investigación

En este apartado del trabajo de titulación se basa el cumplimiento del cuarto objetivo específico elaborando encuestas que posteriormente serán presentadas. Los datos extraídos serán exclusivamente para el desarrollo del trabajo de titulación y se manejarán con absoluta confidencialidad, por esta razón no se emplearán nombres, apellidos ni números de cedula, haciendo referencia al artículo 6 de la ley orgánica de transparencia y acceso a la información pública.

La finalidad de esta encuesta es conocer el nivel de conocimiento sobre ciberseguridad en los sistemas informáticos debido que la tecnología se encuentra evolucionando en la industria, volviéndola vulnerable a piratas informáticos, puede correr peligro de ser atacada cibernéticamente como ya se han hecho públicos los casos de fábricas o empresas atacadas cibernéticamente las cuales se podrán observar en la sección de anexos.

Por esta razón se realizará el análisis de cada pregunta y la medición por medio de gráficos para así de esta manera conocer el nivel de conocimiento e importancia de la ciberseguridad y si el país se encuentra preparado para prevenir ataques informáticos.

3.4.3 Tamaño de la muestra.

La muestra que se consideró en el trabajo de titulación fue a 10 personas entre las cuales hay ingenieros electrónicos, ingenieros en software e ingenieros en telecomunicaciones.

3.4.4 Técnica

La técnica utilizada con la finalidad de recolectar datos para el trabajo de titulación es por medio de una encuesta, esta cuenta con un total de 10 preguntas, por temas de trabajo y tiempo de las personas encuestadas, esta se realizó de manera virtual, se utilizó la herramienta Google Forms ya que permite crear herramientas en línea y puede ser compartida mediante un Link a través de medios electrónicos como el celular hacia la población encuestada.

3.4.5 Estructura de la encuesta

La estructura de la encuesta cuenta con un total de 10 preguntas entre las cuales son de opción múltiple como se puede apreciar en la tabla 3.2 con el fin de obtener los datos recopilados para el análisis y la elaboración de los objetivos.

Tabla 3. 2: Estructura de la encuesta

Preguntas	Reactivos
1.- ¿Qué nivel de conocimiento considera usted sobre las medidas de ciberseguridad en los sistemas informáticos en su lugar de trabajo?	Alto
	Medio
	Bajo
2.- ¿En su empresa existen normas o practicas enfocadas a la ciberseguridad?	Sí
	No
	Sí

3.- ¿Su empresa realiza capacitación sobre temas ciberseguridad y prevención ante amenazas cibernéticas?	No
4.- ¿Sabe usted qué medidas tomar ante un ciberataque?	Sí
	No
5.- ¿En su empresa existen herramientas que aseguren su información digital?	Sí
	No
6.- ¿Existe un área en su lugar de trabajo para buscar soluciones ante ataques informáticos	Si
	No
7.- ¿Conoce usted que los sistemas SCADA son vulnerables ante ataques informáticos?	Sí
	No
8.- ¿En su empresa el sistema de red industrial o algún sistema albergado a ella cuenta con conexión a internet?	Si, permanentemente conectado a la red.
	Si, solo conexión temporal a la red.
	No
	No lo se
9.- ¿Se dispone de acceso remoto a la red industrial que permita la supervisión y/o control de sus sistemas	Sí
	No
10.- ¿En su opinión, cuál cree usted que será la evolución de cara al futuro en inversión de ciberseguridad industrial incluyendo su aplicación a la industria 4.0?	Opinión del encuestado

Elaborado: Autor.

3.4.6 Análisis de los resultados de la encuesta.

La presente encuesta fue realizada hacia Ingenieros electrónicos en control y automatización, software y telecomunicaciones sus datos personales como sus nombres y correos no serán mostrados por lo mencionado anteriormente en el capítulo 3.4.1, esta encuesta tiene como finalidad analizar e interpretar las respuestas de los encuestados.

Pregunta1: ¿Qué nivel de conocimiento considera usted sobre las medidas de ciberseguridad en los sistemas informáticos en su lugar de trabajo?

Tabla 3. 3: Resultados de la pregunta 1

Respuesta	Resultado	Porcentaje
Alto	1	10%
Medio	4	40%
Bajo	5	50%
Total	10	100%

Elaborado: Autor.

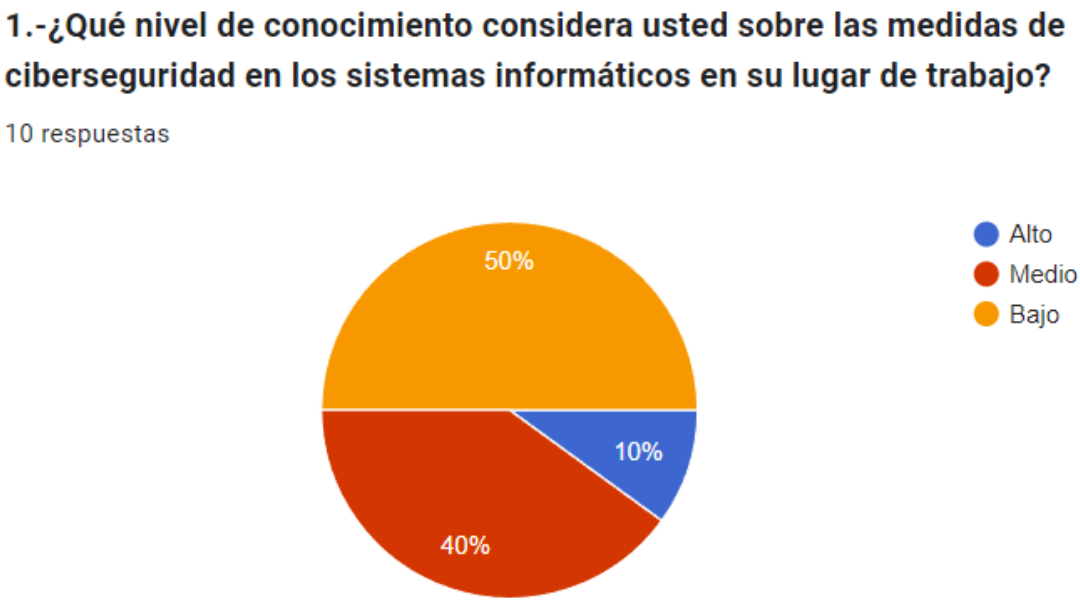


Figura 3. 19: *Grafico estadístico de la pregunta 1*

Fuente: El Autor.

Análisis: De acorde a lo recopilado en la pregunta número 1 se observa mediante la Figura 3.19 que el 10% de las personas encuestadas

tiene un nivel bajo de conocimiento sobre las medidas de ciberseguridad en los sistemas informáticos en su lugar de trabajo, Luego se obtiene que el 40% de las personas indico tener un nivel medio de conocimiento el cual es considerado aceptable para así poder prevenir ciertos ataques cibernéticos y solo el 10% afirma tener un nivel de conocimiento alto en estos sistemas de ciberseguridad.

Pregunta 2. ¿En su empresa existen normas o practicas enfocadas a la ciberseguridad?

Tabla 3. 4: Resultados de la pregunta 2

Respuesta	Resultado	Porcentaje
Sí	4	40%
No	6	60%
Total	10	100%

Fuente: El Autor.

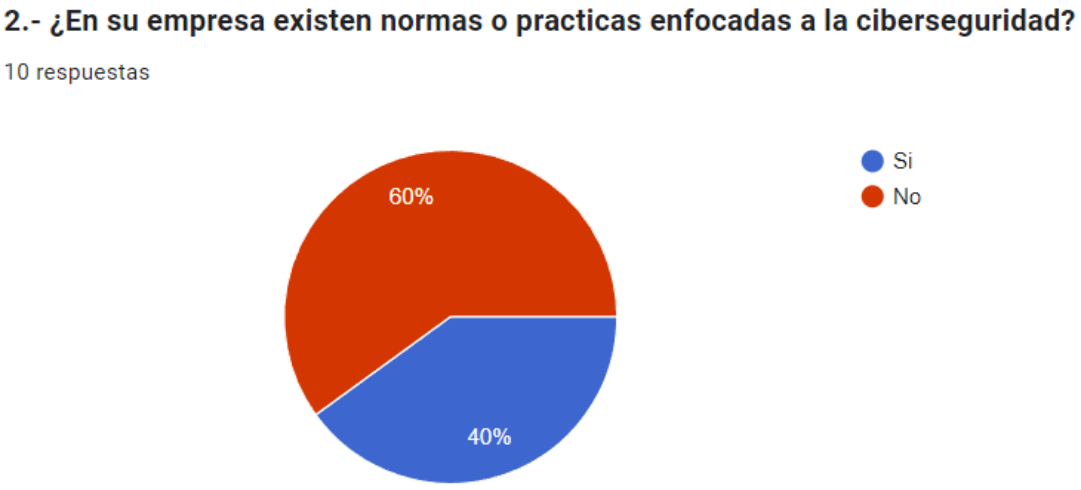


Figura 3. 20: *Grafico estadístico de la pregunta 2*

Fuente: El Autor.

Análisis: En base a los resultados que se pueden apreciar en la Figura 3.20, se puede observar que el 60% de las personas encuestadas afirman que en la empresa donde laboran no existen practicas o normas enfocadas en la ciberseguridad. A su vez se puede observar que el 40% de

las personas afirman que en su lugar de trabajo existen normas o practicas enfocadas a la ciberseguridad. Esto presenta un inconveniente para la empresa y para el usuario debido que la información puede correr peligro ante ataques cibernéticos.

Pregunta 3: ¿Su empresa realizan capacitaciones sobre temas de ciberseguridad y prevención ante amenazas cibernéticas?

Tabla 3. 5: Resultados de la pregunta 3

Respuesta	Resultado	Porcentaje
Sí	2	20%
No	8	80%
Total	10	100%

Fuente: El Autor.

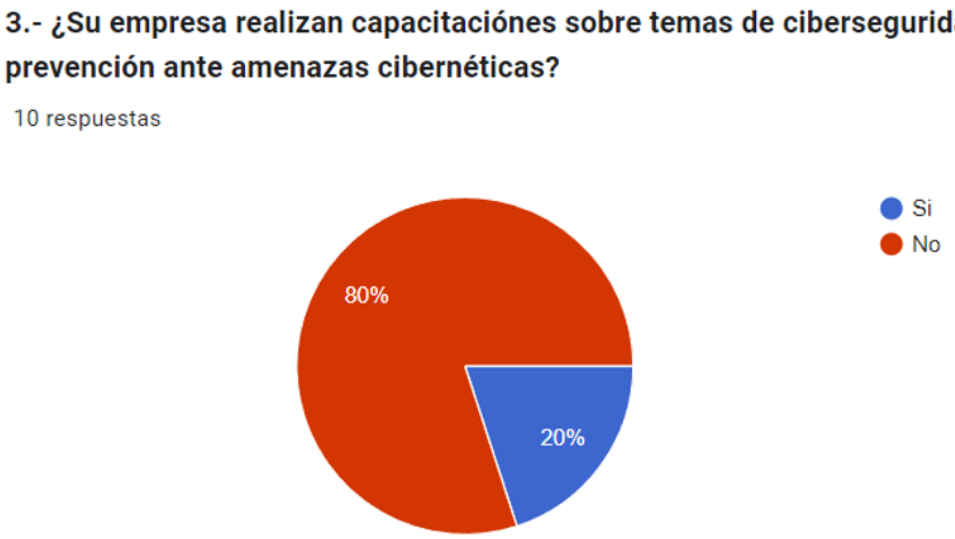


Figura 3. 21: *Grafico estadístico de la pregunta 3*

Fuente: El Autor.

Análisis: Según los porcentajes obtenidos en la pregunta 3 acerca de capacitaciones sobre temas de ciberseguridad y prevención ante amenazas cibernéticas, observamos en la Figura 3.21 que 8 de las 10 personas afirman

que su empresa no realiza estas capacitaciones, las cuales son importantes ya que los atacantes suelen buscar a empleados con menor noción en temas de tecnología ya que basta con afectar una máquina para obtener datos de una empresa, así como se menciona en el capítulo 3.2.1 párrafo 2, en la cual se habla sobre las vulnerabilidades de los SCADA. Y de los encuestados el 2% afirma que su empresa si realiza estas capacitaciones.

Pregunta 4: ¿Sabe usted qué medidas tomar ante un ciberataque

Tabla 3. 6: Resultados de la pregunta 4

Respuesta	Resultado	Porcentaje
Sí	3	30%
No	7	70%
Total	10	100%

Fuente: El Autor.

Figura 3. 22: *Grafico estadístico de la pregunta 4*

Fuente: El Autor.

Análisis: Como se puede observar en la Figura 3.22 y en la tabla 3.6 los porcentajes sobre la pregunta que trata sobre si los encuestados saben qué medidas tomar ante un ciberataque fue que el 70% no sabe qué medidas

tomar, mientras que solo el 30% afirma saber qué medidas tomar. Es preocupante que la mayoría de las personas no sepa qué hacer ante un ataque.

Pregunta 5: ¿En su empresa existen herramientas que aseguren su información personal?

Tabla 3. 7: Resultados de la pregunta 5

Respuesta	Resultado	Porcentaje
Sí	5	50%
No	5	50%
Total	10	100%

Fuente: El Autor.

Figura 3. 23: *Grafico estadístico de la pregunta 5*

Fuente: El Autor.

Análisis: Un tema de importancia es tener la información digital protegida tal y como se lo menciono en el capítulo 3.2.2 en el segundo párrafo**,** entonces en base a los resultados obtenidos se puede apreciar en la Figura 3.23 que el 50% de los encuestados cuentan en su empresa con herramientas que aseguren su información digital y el otro 50% no cuenta con estas herramientas.

Pregunta 6: ¿Existe un área en su lugar de trabajo para buscar soluciones ante ataques informáticos?

Tabla 3. 8: Resultados de la pregunta 6

Respuesta	Resultado	Porcentaje
Sí	6	60%
No	4	40%
Total	10	100%

Fuente: El Autor.

Figura 3. 24: *Grafico estadístico de la pregunta 6*

Fuente: El Autor.

Análisis: Como se puede observar en la Figura 3.24 se puede decir que el 60% de las personas encuestadas afirma que la empresa donde laboran cuenta con un área en la cual buscan soluciones ante ataques informáticos, mientras que el 40% de los encuestados no cuentan en su empresa un área especializada en esto.

Pregunta 7: ¿Conoce usted que los sistemas SCADA son vulnerables ante ataques informáticos?

Tabla 3. 9: Resultados de la pregunta 7

Respuesta	Resultado	Porcentaje
Sí	7	77.8%
No	2	22.2%
Total	9	100%

Fuente: El Autor.

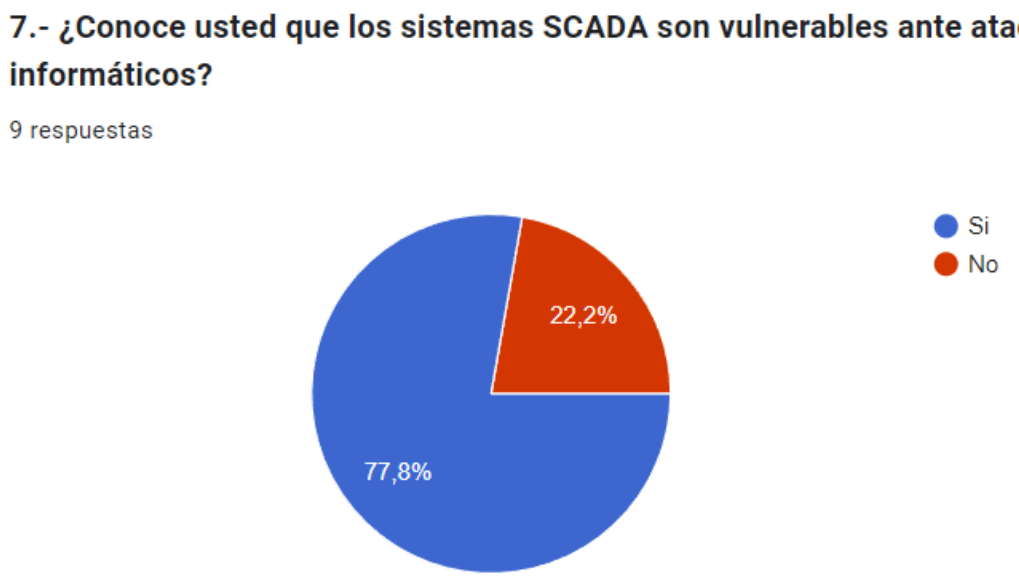


Figura 3. 25: *Grafico estadístico de la pregunta 7*

Fuente: El Autor.

Análisis: Según los datos obtenidos como se puede observar en la Figura 3.25 se puede decir que el 77.8% de las personas encuestadas conocen que un sistema SCADA puede ser vulnerable ante un ciberataque, mientras que el 22.2% de los encuestados afirman no conocer que estos sistemas pueden ser vulnerables. Esto es algo importante ya que es necesario informar a los usuarios acerca de este tema.

Pregunta 8: ¿En su empresa el sistema de red industrial o algún sistema albergado a ella cuenta con conexión a internet?

Tabla 3. 10: Resultados de la pregunta 8

Respuesta	Resultado	Porcentaje
Sí, permanentemente conectado a la red	6	60%
Sí, solo conexión temporal a la red	1	10%
No	1	10%
No lo sé	2	20%
Total	10	100%

Fuente: El Autor.

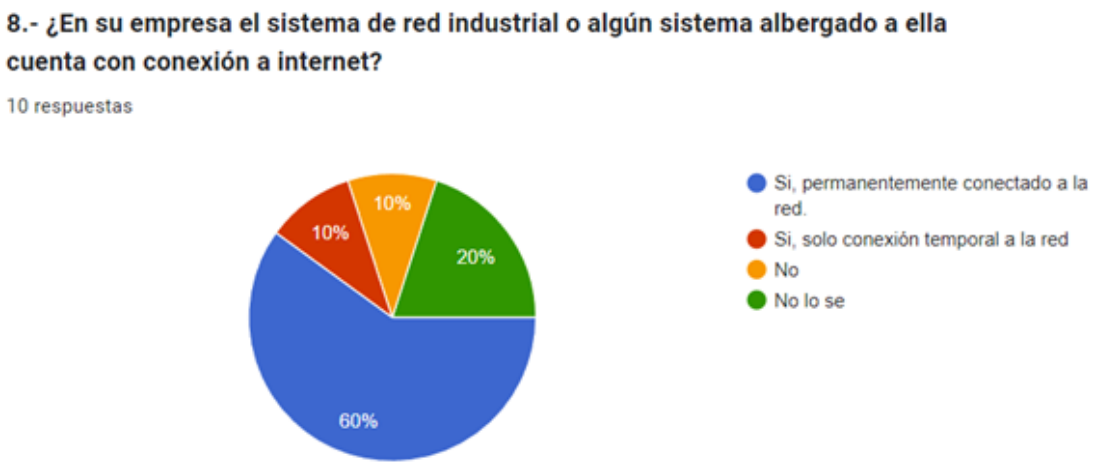


Figura 3. 26: *Grafico estadístico de la pregunta 8*

Fuente: El Autor.

Análisis: En base a lo recopilado en la pregunta número 8 como se observa en el gráfico de la Figura 3.26 , se desea conocer si el sistema de red industrial o algún sistema albergado a ella cuenta con conexión a internet de manera permanente o temporal, según las opciones de respuesta a los

entrevistados, se observa que el 60% afirma que el sistema se encuentra conectado de manera permanente, mientras que el 10% dice que el sistema se encuentra conectado de manera temporal, el otro 10% también afirma que el sistema no se encuentra con conexión a internet y por ultimo un 20% no conoce si este sistema cuenta con conexión a internet.

Pregunta 9: ¿Se dispone de acceso remoto a la red industrial que permita la supervisión y/o control de sus sistemas?

Tabla 3. 11: Resultados de la pregunta 9

Respuesta	Resultado	Porcentaje
Sí	4	40%
No	6	60%
Total	10	100%

Fuente: El Autor.

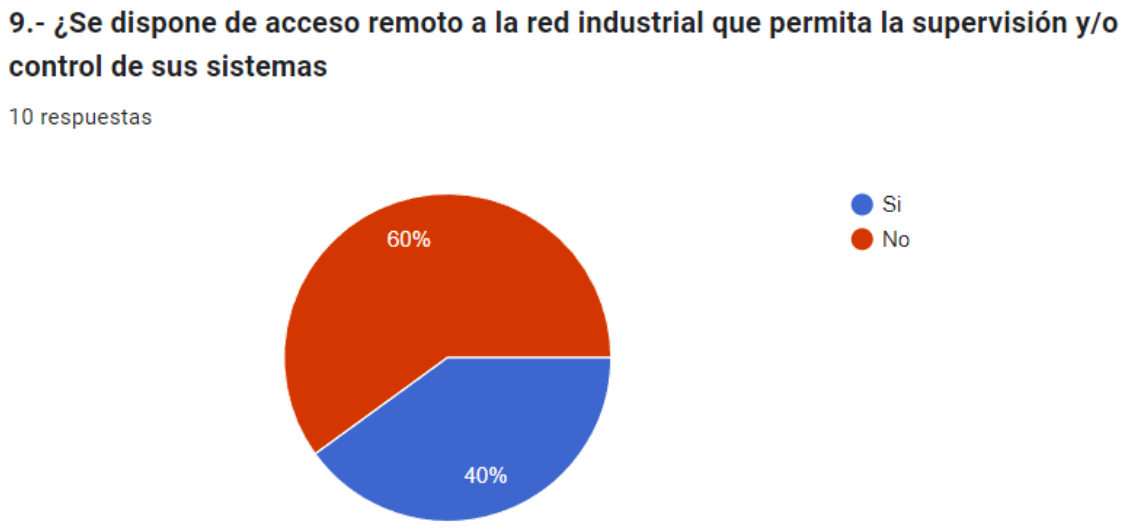


Figura 3. 27: *Grafico estadístico de la pregunta 9*

Fuente: El Autor.

Análisis: De acuerdo con los resultados como se puede observar en la Figura 3.27 el 60% de las personas encuestadas respondieron que en su empresa no disponen de acceso remoto a la red industrial que permita la

supervisión y/o control de sus sistemas, mientras que el 40% de estos si cuentan con el acceso remoto.

Pregunta 10: En su opinión, cual ¿cree usted que será la evolución de cara al futuro en inversión de ciberseguridad industrial incluyendo su aplicación a la industria 4.0?

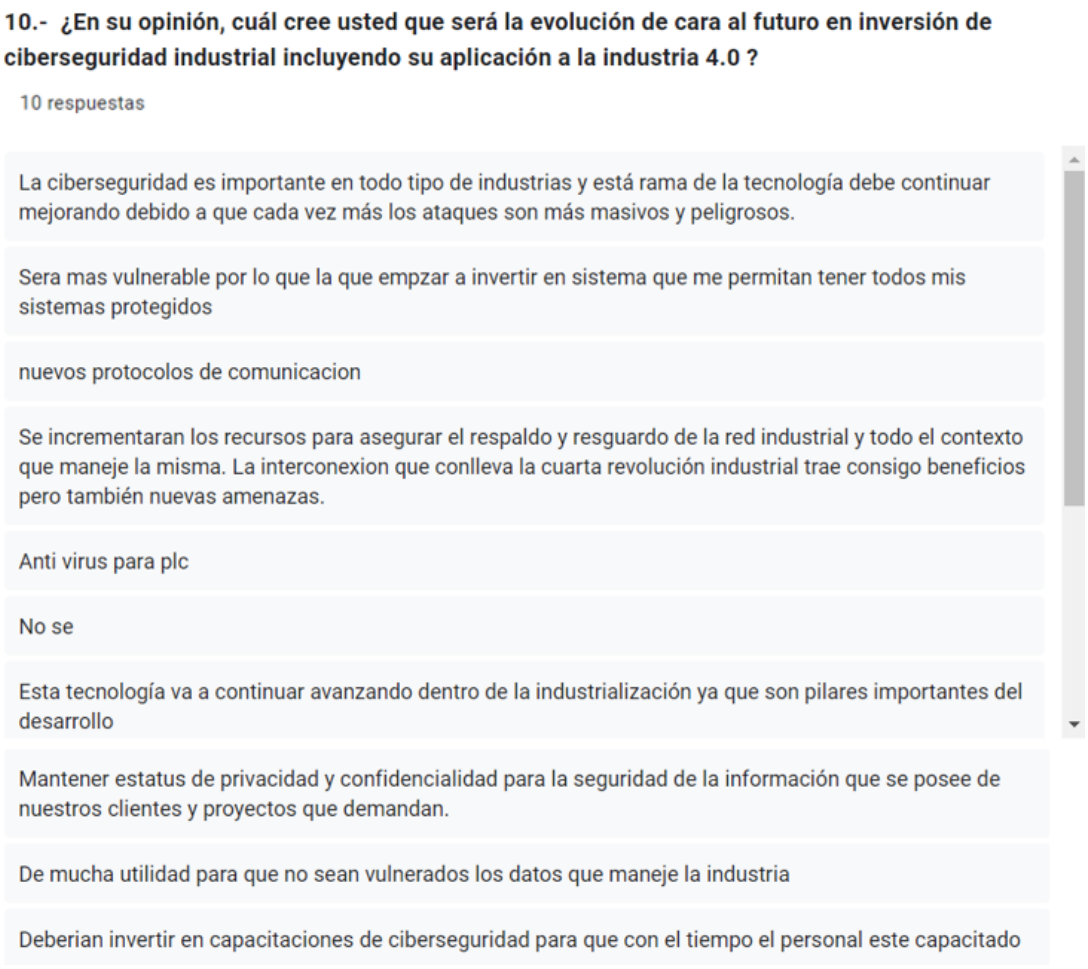


Figura 3. 28: *Opiniones de los encuestados*

Fuente: El Autor.

Análisis: En base a las respuestas de los encuestados como se observa en la Figura 3.28 se determinó que, el 3% opina que sería conveniente invertir en algún sistema que permita tener los sistemas protegidos, invertir en capacitaciones y en nuevos protocolos de comunicación. Con la finalidad que los sistemas se encuentren protegidos.

Existe un 4% hace referencia que se necesitaran medidas de protección de datos, según lo analizado en las siguientes opiniones; se necesita antivirus para el PLC. La interconexión que conlleva la cuarta revolución industrial trae consigo beneficios, pero también amenazas. Y esta rama de la tecnología debe continuar mejorando debido que cada vez más los ataques son más masivos y peligrosos. Se debe mantener un estatus de privacidad y confidencialidad para la seguridad de la información que se poseen de los clientes y proyectos.

El 2% opina que esta tecnología continuara evolucionando y avanzando dentro de la industrialización debido que son pilares importantes para el desarrollo.

El 1% menciono que no sabe cómo sería esta evolución de ciberseguridad.

Todos estos porcentajes se resumen en la tabla 3.12 que se muestra a continuación:

Tabla 3. 12: Interpretación de resultados de las opiniones de los encuestados

Palabras clave	Resultado	Porcentaje
Inversión y Capacitación	3	30%
Protección ante amenazas	4	40%
Evolución	2	20%
No opina	1	10%
Total	10	100%

Fuente: El Autor.

Los resultados de las opiniones de los encuestados fueron interpretados por medio de porcentajes, tomando en cuenta las palabras clave las cuales los encuestados mencionaban palabras en común. De tal manera que se obtuvo un resultado.

Análisis general de las encuestas:

Como análisis general de las encuestas, se puede determinar en base a las preguntas contestadas que existe poco conocimiento sobre las medidas de ciberseguridad, esto es algo preocupante debido que es un tema importante en la actualidad puesto que la tecnología avanza y actualmente las

personas dependen de la tecnología para poder realizar tareas del día a día al igual que las empresas para poder llevar a cabo sus funciones hacen uso de la tecnología. A su vez es posible recomendar en base a las encuestas lo importante que es la capacitación del personal, ya que la tecnología está en constante desarrollo es necesario que las personas aprendan a utilizarla

Este estudio de ciberseguridad se realizó debido que en la pandemia aumentaron casos de ciberataques tanto en el Ecuador como en otras partes del mundo y la finalidad que esto no ocurra en el país se recomienda que se capaciten los empleados para así tener un conocimiento básico sobre la ciberseguridad, en la sección de anexos se podrán observar ejemplos de estos ataques cibernéticos.

Citando a Albert Einstein “Temo el día en que la tecnología sobrepase nuestra humanidad; el mundo solo tendrá una generación de idiotas”.

Capítulo 4: Conclusiones y Recomendaciones

Conclusiones.

- En base a lo investigado se puede concluir se fundamentaron las teorías de ciberseguridad y además se describieron los sitios donde se realizó el estudio.
- Se puede concluir que, mediante lo investigado en el marco teórico, se identificó en el capítulo 2.2 hasta el 2.2.5 las vulnerabilidades y las herramientas utilizadas por los ciberdelincuentes.
- Se cumplió con lo deseado estableciendo métodos de protección en los sistemas informáticos de una pyme del Ecuador como se puede observar en los capítulos 3.3.1 y 3.4.1
- Por medio de las encuestas se logró determinar el conocimiento de los encuestados y además analizar la importancia que le brindan a este tema, con la finalidad de planificar y tomar medidas para la protección y prevención de los ciberataques.

Recomendaciones.

- Mediante el estudio se determinó la importancia del uso de programas legales, por lo que es importante fomentar el uso de programas y aplicaciones de procedencia conocida y de manera legal.
- Es importante la Implementación talleres sobre ciberseguridad básica hacia tanto para los empleados sin importar el área como para estudiantes sin importar la carrera.
- Que se fomente el uso de antivirus de paga y buscadores seguros para así de esta manera obtener medidas de prevención contra ataques informáticos.
- Es indispensable los sistemas se encuentren actualizados, esto aplica más a los sistemas informáticos como los computadores.
- Por temas de seguridad es necesario escanear semanalmente los equipos de manera automática para así llevar un control de protección semanal, de esta manera se podrán eliminar cookies de rastreo
- Es importante contar con el uso de Firewalls y Sistemas detectores de intrusos.
- Es recomendable utilizar una mínima cantidad de conexiones desde servidores o laptops.

Bibliografía

Abril, L. (3 de septiembre de 2021). Los ataques informaticos pymes crecen en el Ecuador. *Tecnologia*.

Agencia EFE. (31 de agosto de 2021). *Elcomercio*. Obtenido de https://www.elcomercio.com/actualidad/seguridad/ecuador-latinoamerica-aumento-ciberataques-kaspersky.html

Amir Vera, J. L. (8 de febrero de 2021). *CNN en español*. Obtenido de https://cnnespanol.cnn.com/2021/02/08/florida-envenenar-lejia-oldsmar/

Berdin. (25 de octubre de 2017). *Berdin Grupo*. Obtenido de http://www.berdin.com/noticias/el-sistema-scada-en-la-industria-4-0/#:~:text=Un-sistema-SCADA(Supervision-Control,por-completo-los-procesos-automaticos.

Boyer, S. A. (15 de febrero de 2016). Obtenido de https://www.goodreads.com/book/show/30196968-scada

Burdova, C. (21 de Marzo de 2022). *Avast*. Obtenido de https://www.avast.com/es-es/c-rootkit

Buxton, D. (20 de abril de 2020). *kaspersky daily*. Obtenido de https://latam.kaspersky.com/blog/news-windows-bsod/7008/

Carlos, S. (21 de enero de 2022). *Chekpoint*. Obtenido de https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/

Codigo Organico Penal. (10 de febrero de 2014). *Sherloc.* Obtenido de https://sherloc.unodc.org/cld/legislation/ecu/codigo_organico_penal/libro_primero/articulo_229/articulo_229.html?lng=en

Granados, H. D. (8 de junio de 2021). *Kaspersky.* Obtenido de https://latam.kaspersky.com/blog/kaspersky-industrial-cybersecurity-for-networks-se-actualiza-con-nuevas-funcionalidades/22085/

Haran, J. M. (20 de diciembre de 2021). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2021/12/20/ransomware-2021-datos-ataques-grupos-mas-activos/

ITtrends. (21 de marzo de 2022). *IT Digital Media Group*. Obtenido de https://www.ittrends.es/gestion-del-dato/2022/03/la-proteccion-de-datos-deberia-ir-mas-alla-de-las-regulaciones-actuales

Jimenez, J. (30 de marzo de 2022). *redeszone*. Obtenido de https://www.redeszone.net/tutoriales/seguridad/rubber-ducky-ataque-dispositivo/

Jorge Juan Rosillo Olmos, M. J. (2022). *ni.com*. Obtenido de https://www.ni.com/es-cr/innovations/case-studies/19/scada-system-to-monitor-and-control-an-agroclimatic-station-and-network-of-real-time-lysimetric-stations.html

Kaspersky. (1 de junio de 2020). Obtenido de https://latam.kaspersky.com/about/press-releases/2020_kaspersky-reveals-new-details-into-series-of-targeted-attacks-on-industrial-companies

Kaspersky. (24 de septiembre de 2020). *Kaspersky.antivirus*. Obtenido de https://kaspersky.antivirus.lv/rus/about/news/events/agc-rupnica-vacija-turpina-pastiprinat-kiberdrosibu-sadarbiba-ar-kaspersky/

Kaspersky. (2022 de agosto de 2022). *Cybermap.kaspersky*. Obtenido de https://cybermap.kaspersky.com/es/stats#country=35&type=OAS&period=w

Kiguolis, L. (2 de abril de 2019). *LosVirus*. Obtenido de https://losvirus.es/la-estafa-congratulations-you-have-won/

Kuskov, V. (23 de octubre de 2020). *Securelist by Kaspersky*. Obtenido de https://securelist.lat/maze-ransomware/91660/

Ley organica de transparencia y acceso a la informacion publica. (18 de mayo de 2004). *portoaguas.gob.ec.* Obtenido de https://portoaguas.gob.ec/wp-content/uploads/2021/12/LOTAIP.pdf

Lopez, D. M. (2020). Automatica e instrumentacion. *Automatica e instrumentacion no 56*, 24-28. Obtenido de https://www.automaticaeinstrumentacion.com/texto-diario/mostrar/2734896/aei-516-ciberseguridad-sector-agua

Medina, E. (10 de diciembre de 2019). Obtenido de https://www.muycomputer.com/2019/12/10/avast-recolecta-datos-usuarios-venderlos-publicistas/#:~:text=3'-,Avast-recolecta-los-datos-de-sus-400,usuarios-para-venderlos-a-publicistas&text=Los-datos-de-las-400,empresas-dedicadas.

Mendez, T. (29 de diciembre de 2021). *Primicias*. Obtenido de https://www.primicias.ec/noticias/sociedad/ecuador-registra-bajo-indice-ciberseguridad/

Mungekar Abhishek, S. Y. (2020). Augmentation of a SCADA based firewall againsy foreign hacking devices. *International Journal of Electrical and Computer Engineering*, 1366.

Nicholas R. Rodofile, K. R. (junio de 2019). Extending the cyber-attack landscape for SCADA- based critical infrastructure. *International Journal of Critical Infrastructure Protection, volume 25, Issue C*, 35. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S1874548217300276?via-Dihub

Onofa, M. (30 de junio de 2022). *Dialogo Americas.* Obtenido de https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-Ecuador/#.Ys5B4nbMK5c

Profiworks. (2022). *Profiworks.com*. Obtenido de https://www.profiworks.com/que-es-profibus/

Redaccion APD. (29 de julio de 2021). *APD.es*. Obtenido de https://www.apd.es/el-gran-impacto-de-la-inteligencia-artificial-en-las-empresas/

Rentero, A. (18 de agosto de 2022). *Silicon*. Obtenido de https://www.uv.mx/infosegura/general/noti_seguridad-40/

Robledano, A. (18 de junio de 2019). *Open Webinars*. Obtenido de https://openwebinars.net/blog/que-es-tcpip/

Seguin, P. (9 de mayo de 2022). *Avast*. Obtenido de https://www.avast.com/es-es/c-spyware

Siemens. (14 de junio de 2018). *Info PLC*. Obtenido de https://www.infoplc.net/noticias/item/105533-siemens-router-industrial-acceso-remoto-seguro-maquinas-profibus

Siemens. (9 de septiembre de 2019). *Siemens Industry*. Obtenido de https://support.industry.siemens.com/cs/document/109422039/-como-puede-implementar-los-protocolos-iec-60870-5-con-el-simatic-s7-1500-?dti=0&lc=es-ES

Strelkov, A. (8 de junio de 2021). *Kaspersky.* Obtenido de https://latam.kaspersky.com/blog/kaspersky-industrial-cybersecurity-for-networks-se-actualiza-con-nuevas-funcionalidades/22085/

Sumelco. (25 de julio de 2021). Obtenido de https://www.sumelco.com/blog/transmision-de-datos-a-traves-del-protocolo-iec-60870-5-101-iec-60870-5-104-y-dnp3/

Terry Lanfear, B. T. (2 de junio de 2022). *Microsoft*. Obtenido de https://docs.microsoft.com/es-es/azure/security/fundamentals/overview

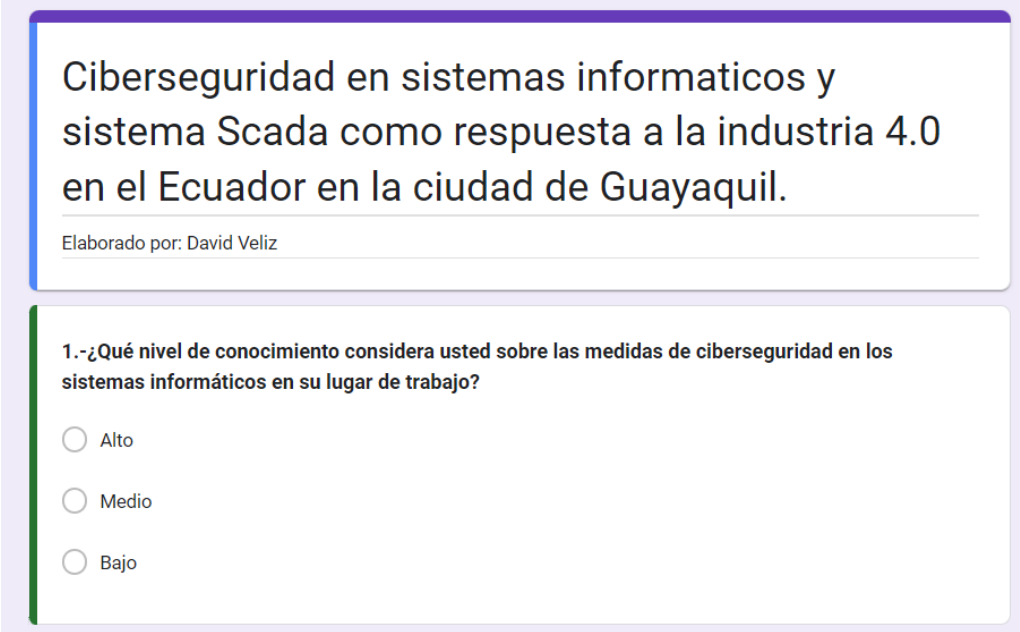
Universidad Tecnica Particular de Loja. (18 de mayo de 2022). Obtenido de Juan Pablo Suárez, director del Parque Científico y Tecnológico de la UTPL, señaló que “el laboratorio permitirá que desde la universidad, se desarrollen soluciones industriales a problemas globales”. Además, resaltó la importancia de comenzar a trabajar

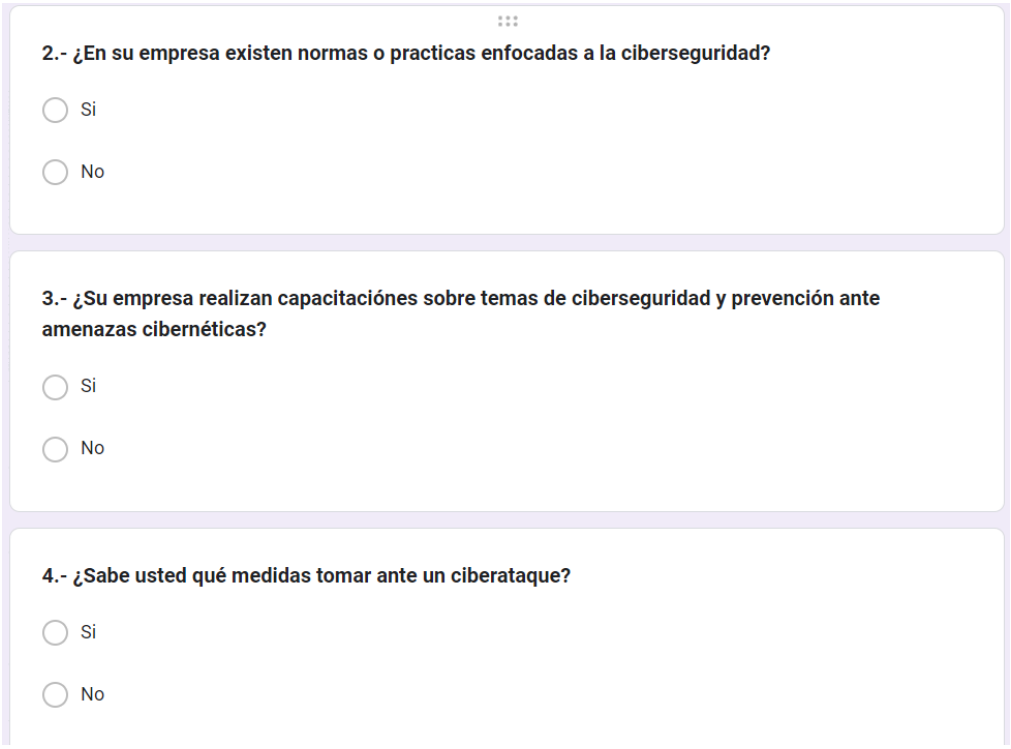
Vinueza, C. (6 de octubre de 2021). *Epico*. Obtenido de https://epico.gob.ec/epico-realizo-el-lanzamiento-del-programa-guayaquil-4-0-que-busca-soluciones-innovadoras-para-impulsar-la-competitividad-de-la-agroindustria-del-gran-Guayaquil/

Anexos

Anexo 1

Encuesta en Google Forms sobre la ciberseguridad en sistemas informáticos y sistemas SCADA como respuesta a la industria 4.0 en el Ecuador en la ciudad de Guayaquil.





5.- ¿En su empresa existen herramientas que aseguren su información digital?

- ◯ Si
- ◯ No

6.- ¿Existe un área en su lugar de trabajo para buscar soluciones ante ataques informáticos

- ◯ Si
- ◯ No

7.- ¿Conoce usted que los sistemas SCADA son vulnerables ante ataques informáticos?

- ◯ Si
- ◯ No

8.- ¿En su empresa el sistema de red industrial o algún sistema albergado a ella cuenta con conexión a internet?

- ◯ Si, permanentemente conectado a la red.
- ◯ Si, solo conexión temporal a la red
- ◯ No
- ◯ No lo se

9.- ¿Se dispone de acceso remoto a la red industrial que permita la supervisión y/o control de sus sistemas

- ◯ Si
- ◯ No

10.- ¿En su opinión, cuál cree usted que será la evolución de cara al futuro en inversión de ciberseguridad industrial incluyendo su aplicación a la industria 4.0 ?

Texto de respuesta corta

Anexo 2

Este articulo a pesar de ser del 2004, se encuentra vigente.

Articulo 6.- Información Confidencial. Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas.

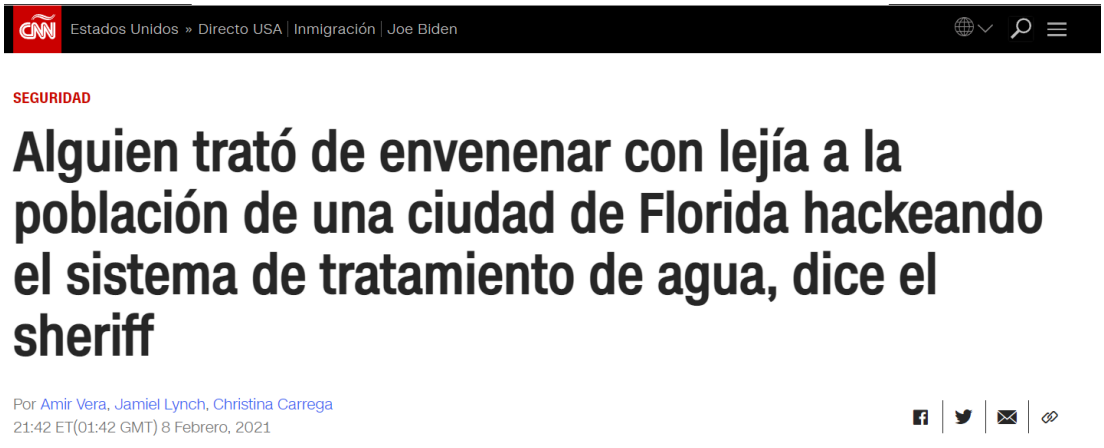
(Ley organica de transparencia y acceso a la informacion publica, 2004)

Anexo 3

Un pirata informático obtuvo acceso al sistema de tratamiento de agua de Oldsmar, Florida, el viernes e intentó aumentar los niveles de hidróxido de sodio, comúnmente conocido como lejía, en el agua de la ciudad, dijeron las autoridades, poniendo a miles de personas en riesgo de envenenamiento.

El incidente tuvo lugar el viernes cuando un operador notó la intrusión y observó al pirata informático acceder al sistema de forma remota. El hacker ajustó el nivel de hidróxido de sodio a más de 100 veces sus niveles normales, según el alguacil del condado de Pinellas, Bob Gualtieri.

El operador del sistema redujo inmediatamente el nivel. En ningún momento hubo un efecto adverso significativo en el suministro de agua de la ciudad y el público nunca estuvo en peligro, dijo Gualtieri. Se desconoce si la infracción ocurrió por parte de alguien a nivel local, nacional o incluso fuera de Estados Unidos. (Amir Vera, 2021)



En tiempos en que la tecnología es una herramienta cotidiana, pues la mayoría de las personas accede a servicios en línea, como compras, transferencias, entre otros, la ciberseguridad en Ecuador es clave.

A lo largo de 2021, entidades públicas como la Corporación Nacional de Telecomunicaciones (CNT), Agencia Nacional de Tránsito (ANT) e Instituto Ecuatoriano de Seguridad Social (IESS) han sufrido ataques informáticos. (Mendez, 2021)

PRIMICIAS

SUSCRÍBASE

Home Política Economía Sociedad Tecnociencia En Exclusiva Sucesos Firmas y Análisis

#ciberseguridad #ciberseguridad en Ecuador #Ecuador #hackeos #Ministerio de Telecomunicaciones #Naomi A

Ecuador registra un bajo índice de ciberseguridad

La ministra de Telecomunicaciones, Vianna Maino, se refirió al hackeo al sistema informático de la Policía, a propósito del caso de Naomi Arcentales. Ecuador trabaja en fortalecer su ciberseguridad.

El índice de ciberseguridad en Ecuador bordea los 25 puntos sobre 100. Así lo reveló **la ministra de Telecomunicaciones, Vianna Maino,** al ser consultada sobre los constantes hackeos a sistemas informáticos del país.

El **más reciente fue el reportado por la Policía Nacional, que dio paso a la detención del fiscal Juan Carlos Izquierdo**, dentro del caso de Naomi Arcentales.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Véliz García David Daniel** con C.C: # 095549060-2 autor del Trabajo de Titulación: **Estudio de ciberseguridad en sistemas SCADA y sistemas informáticos como respuesta a la industria 4.0 en el Ecuador** previo a la obtención del título de **INGENIERO ELÉCTRONICO EN CONTROL Y AUTOMATISMO** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 14 de septiembre del 2022

f. _____

Nombre: Véliz García, David Daniel

C.C: 095549060-2

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Estudio de ciberseguridad en sistemas SCADA y sistemas informáticos como respuesta a la industria 4.0 en el Ecuador.		
AUTOR(ES)	Véliz García, David Daniel		
REVISOR(ES)/TUTOR(ES)	Romero Rosero, Carlos Bolívar		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería Electrónica en Control y Automatismo		
TITULO OBTENIDO:	Ingeniero Electrónico en control y automatismo		
FECHA DE PUBLICACIÓN:	14 de septiembre del 2022	**No. DE PÁGINAS:**	80
ÁREAS TEMÁTICAS:	Redes de Datos, Sistemas Informáticos, Empresas		
PALABRAS CLAVES:	SCADA, Ciberdelincuente, Hacker, Malware, Troyano, Adware, Software		

RESUMEN:

El presente trabajo de titulación consiste en un estudio de ciberseguridad en sistemas informáticos y sistemas SCADA como respuesta a la industria 4.0 en el Ecuador con el fin de dar una respuesta y dar a conocer la calidad de conocimiento que cumplen los Ingenieros que trabajan en estas áreas se realizó una encuesta en la cual se efectuó el análisis de cada pregunta y respuesta para así evaluar a los encuestados sobre que tanto conocen sobre ciberseguridad.

En el capítulo 1 se abordó sobre ¿Cómo incide la ciberseguridad en los sistemas informáticos y sistemas SCADA actualmente en el Ecuador? Siendo ésta el problema a investigar, además se plantearon los objetivos para así de esta manera llevar a cabo la investigación.

En el capítulo 2 se abordó el marco teórico en el cual se hizo referencia hacia las herramientas que utilizan los ciberdelincuentes, maneras de evitar ataques cibernéticos mediante antivirus, buscadores seguros y sobre todo conocer las leyes que existen en caso de sufrir un ataque cibernético. Las personas suelen mal utilizar términos como hacker y cracker puesto que, en este trabajo, se explicará la manera correcta en la cual se conoce a estos ciberdelincuentes.

Se abordarán temas de cómo lidiar con malwares, troyanos y adware, los cuales pueden abrir una brecha e irrumpir en los softwares de programación

Además de esto en el trabajo se muestra ataques cibernéticos en empresas e industrias fuera del país. Las cuales hicieron que corra peligro la vida del ser humano.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593981447512	E-mail: david_v_20@hotmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Vélez Tacuri, Efraín Olivero	
	Teléfono: +593 -9-94084215	
	E-mail: efrain.velez@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	