

U N I V E R S I D A D V E R A C R U Z A N A

TC

**EXPERIENCIA EDUCATIVA**

SEGURIDAD

**PROYECTO FINAL**

Seguridad para la empresa

“SOFTWARE -TC”

 ALVAN ARGUELLES ANA PAULA

 MEJIA PERALTA EDUARDO

 MARTINEZ GUTIERRES JOSUE DAVID

 VAZQUEZ VIDAL MARICARMEN

**INTEGRANTES**

**DOCENTE**

Mtra. Alicia Yazmin Rojas Luna

Xalapa, Ver., a 03 enero del 2024

# **INDICE**

[**INDICE** 2](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924579)

[**INTRODUCCIÓN** 3](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924580)

[**DESCRIPCIÓN** 4](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924581)

[**ANALISIS DE LA SITUACIÓN ACTUAL** 6](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924582)

[**PROBLEMÁTICA Y SOLUCIONES** 8](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924583)

[**DISEÑO DE SEGURIDAD PROPUESTO** 10](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924584)

[**1.** **Medidas Físicas de seguridad** 10](#_Toc154924585)

[**2.** **Seguridad de Red y Sistemas** 12](#_Toc154924586)

[**VPN** 12](#_Toc154924587)

[**Firewall** 13](#_Toc154924588)

[**3.** **Acceso a internet** 13](#_Toc154924589)

[**Proxy** 13](#_Toc154924590)

[**4.** **Reporte de cultura en seguridad** 13](#_Toc154924591)

[**5.** **Estrategias de cifrado de archivos y acceso a los mismos** 13](#_Toc154924592)

[**Cifrado simétrico** 13](#_Toc154924593)

[**Cifrado Asimétrico** 13](#_Toc154924594)

[**6.** **Sistema de Registro de Empleados** 13](#_Toc154924595)

[**Sitio Web con PHP y MySQL** 13](#_Toc154924596)

[**7.** **Vulnerabilidades** 13](#_Toc154924597)

[**Inyección SQL** 13](#_Toc154924598)

[**XSS** 14](#_Toc154924599)

[**CSRF** 14](#_Toc154924600)

[**8.** **Reporte de ingeniería social** 14](#_Toc154924601)

[**Clonación de red social** 14](#_Toc154924602)

[**9.** **Bloquear Acceso** 14](#_Toc154924603)

[**Proxy** 14](#_Toc154924604)

[**10.** **Monitoreo de red y escaneo de puertos** 14](#_Toc154924605)

[**CONCLUSIÓN** 15](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924606)

[**ANEXOS** 16](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924607)

[**REFERENCIAS** 17](file:///C:\Users\Win10\Documents\SEGURIDAD%20PROYECTO%20EQ.%204.docx#_Toc154924608)

# **INTRODUCCIÓN**

La empresa "SOFTWARE -TC" busca mejorar la seguridad en sus instalaciones, las cuales actualmente carecen de mecanismos de seguridad física. Además, la empresa cuenta con una red de área local que alberga sistemas críticos, como Recursos Humanos, Finanzas y Soporte e Informática, así como acceso a Internet mediante redes cableada e inalámbrica. También se enfrenta a desafíos relacionados con la pandemia COVID-19, como el trabajo remoto y la necesidad de acceso remoto a sistemas internos.

Para esto, se incluye la implementación de soluciones para cifrar archivos importantes de acuerdo con diferentes tipos de usuarios, la construcción de un sistema de registro de empleados para el departamento de Soporte e Informática, la detección y solución de vulnerabilidades en sitios web y la protección de accesos a sitios no deseados, entre otros aspectos de seguridad.

Además, se implementa un sistema de monitoreo de red y escaneo de puertos para verificar las configuraciones existentes, así como la preparación para una auditoría por parte de un equipo externo de auditores. Se incluye la descripción detallada de las configuraciones con código fuente, en caso de ser implementadas, y la explicación de cómo se instalan, configuran y funcionan.

Se espera incluir la configuración de un Firewall, un proxy, listas de acceso y scripts o configuraciones de programas para cumplir con cada uno de los puntos descritos en el proyecto.

Este proyecto representa un desafío integral en el ámbito de la seguridad informática, con el objetivo de fortalecer la protección de la empresa "SOFTWARE -TC" en todos los aspectos relacionados con la seguridad y la ciberseguridad.

#### 

# **DESCRIPCIÓN**

Físicamente, la empresa no tiene implementados mecanismos de seguridad, esta se encuentra ubicada en un espacio abierto construida por un edificio, dentro de este se comparten accesos para comunicarse entre sí, cuenta con una entrada y salida de vehículos, así como dos áreas de estacionamiento. Para las personas hay una entrada, aunque muchas veces se utiliza también la entrada o salida de los automóviles para ingresar o salir de las instalaciones, por lo que se te solicita que generes un **reporte** para dar solución al problema.

La empresa cuenta con una red de área local y dentro de ésta se encuentran los siguientes sistemas:

* Sistema de Recursos humanos (Acceso solo dentro de la empresa y parte de integrantes del departamento)
* Sistema de Finanzas (Acceso solo dentro de la empresa y parte de integrantes del departamento)
* Sistema Soporte e Informática (Acceso solo dentro de la empresa y parte de integrantes del departamento)
* Acceso a Internet mediante la red cableada (Se restringen sitios de pornografía, juegos y sitios con contenidos de software ilegal)
* Acceso a Internet mediante red inalámbrica (Se restringen sitios de pornografía, juegos y sitios con descargas).

Debido a la pandemia COVID-19, se implementaron diversas medidas que aún siguen activas, como lo es el trabajo remoto y las autoridades necesitan ingresar desde su casa para tener acceso a los sistemas internos de la misma. Por lo que no se cuenta con un plan de fomento a cultura en seguridad dentro de la empresa. Deberás implementar una solución para este aspecto.

Los archivos importantes que se comparten entre diversos usuarios de la empresa se deben cifrar simétrica y asimétricamente para asegurar su

contenido de acuerdo con los diferentes tipos de usuarios, existen 4 tipos de usuarios para cifrar el contenido:

* Usuario de Recursos humanos: UserRH (simétrica)
* Usuario de Finanzas: UserFinza (simétrica)
* Usuario Soporte e Informática: UserSeInfo (asimétrica)
* Usuario Director: UserDir (asimétrica)

Como parte del proceso la empresa solicita una capacitación de seguridad para los programadores del departamento de Soporte e Informática, por lo que, se deberá realizar la construcción de un sistema de registro de empleados (CRUD) que será utilizado por 2 usuarios:

* Usuario de Recursos humanos: UserRH
* Usuario de Finanzas: UserFinza.

Se les pide que tenga las siguientes características:

* Una página que lleve a una red social (Facebook, Twitter, Youtube, tiktok)
* Una página que permita iniciar sesión

Como se les ha contratado deberán comprobar por lo menos 3 de las vulnerabilidades más comunes en estos sitios, recomendaciones y pasos que llevaste a cabo para detectar la vulnerabilidad. Así mismo, se realizará la capacitación y difusión de aspectos relacionados con ingeniería social, una demostración sobre la clonación para robar las credenciales de un usuario (Facebook, Twitter, Youtube).

Además, para brindar aspectos de seguridad, es necesario proteger los accesos a sitios pornográficos, redes sociales para las siguientes redes sociales: Instagram, tiktok, snapchat y palabras relacionadas con violencia, así como bloquear peticiones a puertos que no pertenezcan a: SMTP, HTTP, HTTPS, Bases de datos y POP. Cualquier otra petición que no coincida con ese tipo de puertos deberá bloqueada y detectada.

En auditorías pasadas se detectaron puertos abiertos en el equipo, además de tráfico inusual, por lo que se te pide que implementes un sistema de monitoreo a la red y scan de puertos para corroborar que las actuales configuraciones funcionan en óptimas condiciones.

# **ANALISIS DE LA SITUACIÓN ACTUAL**

**Seguridad Física**

**Situación Actual:** La empresa carece de mecanismos de seguridad física adecuados. Existe una entrada principal para vehículos y personas, con accesos compartidos, lo cual representa un riesgo de seguridad.

**Solución Propuesta**: Implementación de sistemas de control de acceso físico, como tarjetas de acceso o sistemas biométricos, para regular y monitorear la entrada y salida de personal y visitantes. Además, se podría considerar la instalación de cámaras de vigilancia y alarmas.

**Seguridad de Red y Sistemas**

**Situación Actual:** La empresa tiene sistemas críticos como Recursos Humanos, Finanzas y Soporte e Informática, con acceso restringido.

**Solución Propuesta:** Establecer VPN, incluyendo firewalls, sistemas de prevención de intrusiones (IPS) y segmentación de red para limitar el acceso a estos sistemas solo a usuarios autorizados.

**Acceso a Internet**

**Situación Actual:** Existe control sobre el acceso a ciertos sitios web a través de la red cableada e inalámbrica.

**Solución Propuesta:** Implementación de un sistema de filtrado de contenido más robusto para bloquear sitios no seguros o inapropiados, y uso de un proxy para monitorear y controlar el tráfico de Internet.

**Trabajo Remoto y Cultura de Seguridad**

**Situación Actual:** La necesidad de acceso remoto a los sistemas internos debido al trabajo remoto, sin un plan de fomento a la cultura de seguridad.

**Solución Propuesta:** Desarrollar y aplicar políticas de seguridad para el trabajo remoto, incluyendo el uso de VPNs seguras y autenticación de dos factores. Además, proponer programas de capacitación y concienciación en seguridad para todos los empleados.

**Cifrado de Archivos**

**Situación Actual:** Cifrar archivos importantes usando métodos simétricos y asimétricos según el tipo de usuario.

**Solución Propuesta**: Implementar soluciones de cifrado de datos en reposo y en tránsito, seleccionando algoritmos adecuados para cada tipo de usuario y asegurando la gestión segura de claves.

**Sistema de Registro de Empleados (CRUD)**

**Situación Actual:** Creación de un sistema CRUD accesible por usuarios de RH y Finanzas, con enlaces a redes sociales y funcionalidades de inicio de sesión.

**Solución Propuesta:** Desarrollar una sitio web, utilizando prácticas de desarrollo seguro.

**Vulnerabilidades**

**Situación Actual:** Comprobar vulnerabilidades en estos sitios.

**Solución Propuesta:** Implementación 3 de las vulnerabilidades (Inyección SQL, XSS y CSRF) proponer recomendaciones y mencionar el procedimiento para detectar la vulnerabilidad.

**Protección contra Ingeniería Social**

**Situación Actual:** Capacitar a empleados en el reconocimiento y prevención de ataques de ingeniería social.

**Solución Propuesta:** Proponer talleres y simulaciones para enseñar a los empleados a identificar intentos de phishing y otras tácticas de ingeniería social como la clonación de sitios web para robar credenciales.

**Bloquear Accesos**

**Situación Actual:** Proteger los accesos a sitios pornográficos, redes sociales y palabras relacionadas con violencia, así como bloquear peticiones a puertos que no pertenezcan a: SMTP, HTTP, HTTPS, Bases de datos y POP.

**Solución Propuesta:** Implementación de un sistema de filtrado de contenido para bloquear sitios no seguros o inapropiados, por medio de un proxy para detectar y bloquear.

**Monitoreo de Red y Escaneo de Puertos**

**Situación Actual**: Detectar puertos abiertos y tráfico inusual en la red.

**Solución Propuesta:** Implementar herramientas de monitoreo de red y escaneo de puertos para identificar y mitigar posibles vulnerabilidades y actividades sospechosas.

# **PROBLEMÁTICA Y SOLUCIONES**

|  |  |  |
| --- | --- | --- |
| **No.** | **Problemática**  **(situación actual)** | **Solución Propuesta** |
| **1** | Físicamente, la empresa no tiene implementados mecanismos de seguridad, esta se encuentra ubicada en un espacio abierto construida por un edificio, dentro de este se comparten accesos para comunicarse entre sí, cuenta con una entrada y salida de vehículos, así como dos áreas de estacionamiento. Para las personas hay una entrada, aunque muchas veces se utiliza también la entrada o salida de los automóviles para ingresar o salir de las instalaciones | **Reporte de seguridad física**  (Medidas de seguridad física) |
| **2** | La empresa cuenta con una red de área local y dentro de ésta se encuentran los siguientes sistemas:   * Sistema de Recursos humanos (Acceso solo dentro de la empresa y parte de integrantes del departamento) * Sistema de Finanzas (Acceso solo dentro de la empresa y parte de integrantes del departamento) * Sistema Soporte e Informática (Acceso solo dentro de la empresa y parte de integrantes del departamento) | **VPN y Firewall**  (Seguridad de Red y Sistemas) |
| **3** | * Acceso a Internet mediante la red cableada (Se restringen sitios de pornografía, juegos y sitios con contenidos de software ilegal) * Acceso a Internet mediante red inalámbrica (Se restringen sitios de pornografía, juegos y sitios con descargas). | **Proxy**  (Acceso a internet) |
| **4** | Debido a la pandemia COVID-19, se implementaron diversas medidas que aún siguen activas, como lo es el trabajo remoto y las autoridades necesitan ingresar desde su casa para tener acceso a los sistemas internos de la misma. Por lo que no se cuenta con un plan de fomento a cultura en seguridad dentro de la empresa. | **Reporte de cultura en seguridad** |
| **5** | Los archivos importantes que se comparten entre diversos usuarios de la empresa se deben cifrar simétrica y asimétricamente para asegurar su  contenido de acuerdo con los diferentes tipos de usuarios, existen 4 tipos de usuarios para cifrar el contenido:   * Usuario de Recursos humanos: UserRH (simétrica) * Usuario de Finanzas: UserFinza (simétrica) * Usuario Soporte e Informática: UserSeInfo (asimétrica) * Usuario Director: UserDir (asimétrica) | **Cifrado simétrico y Cifrado Asimétrico**  (Estrategias de cifrado de archivos y acceso a los mismos) |
| **6** | Como parte del proceso la empresa solicita una capacitación de seguridad para los programadores del departamento de Soporte e Informática, por lo que, se deberá realizar la construcción de un sistema de registro de empleados (CRUD) que será utilizado por 2 usuarios:   * Usuario de Recursos humanos: UserRH * Usuario de Finanzas: UserFinza.   Se les pide que tenga las siguientes características:   * Una página que lleve a una red social (Facebook, Twitter, Youtube, tiktok) * Una página que permita iniciar sesión | **Sitio Web con PHP y MySQL**  (Sistema de Registro de Empleados) |
| **7** | Como se les ha contratado deberán comprobar por lo menos 3 de las vulnerabilidades más comunes en estos sitios, recomendaciones y pasos que llevaste a cabo para detectar la vulnerabilidad. | **Inyección SQL, XSS y CSRF**  (escaneo de vulnerabilidades) |
| **8** | Se realizará la capacitación y difusión de aspectos relacionados con ingeniería social, una demostración sobre la clonación para robar las credenciales de un usuario (Facebook, Twitter, Youtube). | **Reporte de ingeniería social y**  **Clonación de red social** |
| **9** | Además, para brindar aspectos de seguridad, es necesario proteger los accesos a sitios pornográficos, redes sociales para las siguientes redes sociales: Instagram, tiktok, snapchat y palabras relacionadas con violencia, así como bloquear peticiones a puertos que no pertenezcan a: SMTP, HTTP, HTTPS, Bases de datos y POP. Cualquier otra petición que no coincida con ese tipo de puertos deberá bloqueada y detectada. | **Proxy**  (Bloquear Acceso) |
| **10** | En auditorías pasadas se detectaron puertos abiertos en el equipo, además de tráfico inusual, por lo que se te pide que implementes un sistema de monitoreo a la red y scan de puertos para corroborar que las actuales configuraciones funcionan en óptimas condiciones. | (Monitoreo de red y escaneo de puertos) |

# **DISEÑO DE SEGURIDAD PROPUESTO**

## **Medidas Físicas de seguridad**

Las instalaciones de la empresa **Software-TC**, no cuentan con medidas de seguridad física, por lo cual, se encuentra vulnerable a cualquier amenaza que pueda producirse dentro de las instalaciones. Ya sea por personal no autorizado o algún empleado descontento con la empresa, que quiera tomar justicia por mano propia. Por lo cual, se sugieren las siguientes medidas de seguridad que pueden implementarse en las instalaciones de la empresa, tanto en exterior como en interior.

En las imágenes ilustrativas de la empresa, se marcaron puntos con números, cada marca está colocada en la posición aproximada donde irá una media de seguridad. Como están diferenciados por números, cada número especifica qué medida se colocará. Es decir, si en una esquina de una habitación hay una marca con el número 2 y el número 2 está nombrado como “cámara de vigilancia”, quiere decir que en esa esquina se colocará una cámara de video vigilancia.

A continuación se muestran las imágenes, tanto del interior como del exterior con las marcas tomadas para establecer medidas de seguridad física en las instalaciones de la empresa.

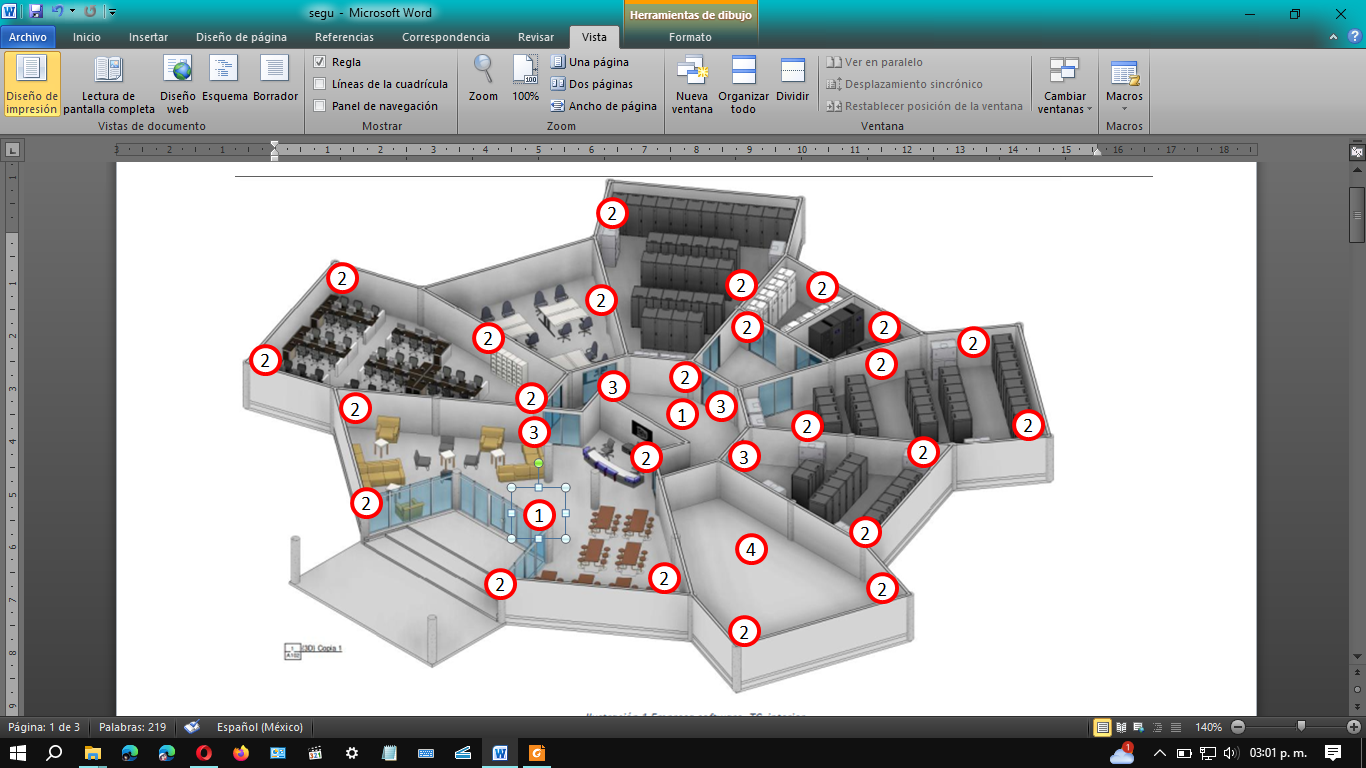


Fig1: Empresa Software-TC, Interior.

**1.- Guardia de seguridad:** Implementación de personal de seguridad para protección del personal del lugar y apoyo en posible detención de personas sospechosas.

**2.-Camaras de vigilancia:** Instalación de cámaras de vigilancia para monitorear el área en busca de cualquier actividad sospechosa.

**3.- Lector de tarjetas de identificación:** Permite que solo personal autorizado pueda entrar en las instalaciones. (Se aplica en todas las puertas para mantener un registro de quién entra y sale)

**4.- Área de destrucción de discos duros:** Para proteger los datos sensibles, cumplir con regulaciones y normativas, prevenir el robo de información y gestionar adecuadamente los residuos electrónicos.

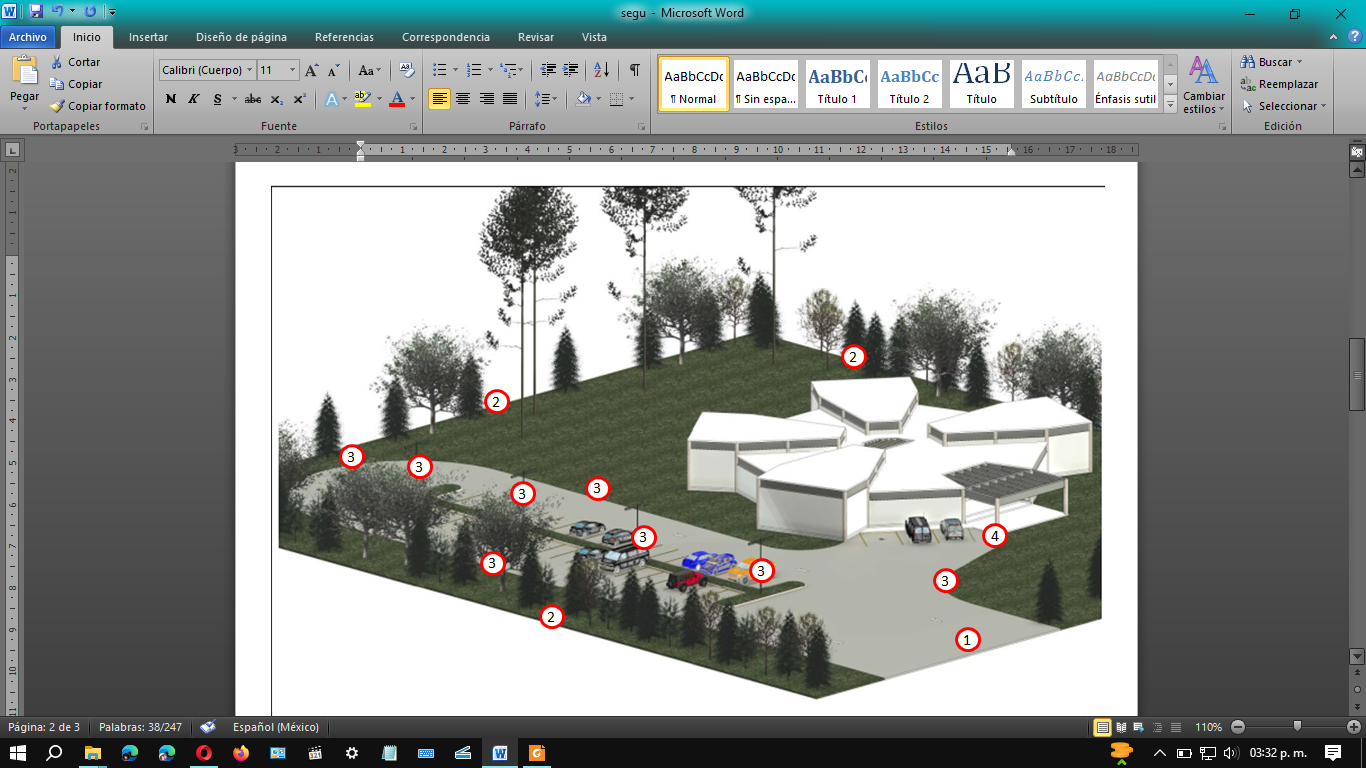


Fig2: Empresa Software-TC, Exterior.

**1.- Instalación de una caseta de vigilancia y Parada de barreras:** Personal de seguridad dedicado a registrar el ingreso de toda persona en la instalación.

**2.- Construcción de una valla de seguridad:** Para evitar la entrada de personal no autorizado entre a las instalaciones por la entrada principal, se construirá una valla de un aproximado de 5 metros de altura que rodee el área.

**3.- Instalación de cámaras de vigilancia:** Se instalarán postes con cámaras de vigilancia para monitorear las áreas alrededor de las instalaciones.

**4.- Personal de seguridad:** Para permitir el acceso al personal autorizado y garantizar la seguridad del personal.

## **Seguridad de Red y Sistemas**

### **VPN**

### **Firewall**

## **Acceso a internet**

### **Proxy**

## **Reporte de cultura en seguridad**

## **Estrategias de cifrado de archivos y acceso a los mismos**

### **Cifrado simétrico**

### **Cifrado Asimétrico**

## **Sistema de Registro de Empleados**

### **Sitio Web con PHP y MySQL**

## **Vulnerabilidades**

### **Inyección SQL**

### **XSS**

### **CSRF**

## **Reporte de ingeniería social**

### **Clonación de red social**

## **Bloquear Acceso**

### **Proxy**

## **Monitoreo de red y escaneo de puertos**

# **CONCLUSIÓN**

# **ANEXOS**

# **REFERENCIAS**