



**Galileo**  
UNIVERSIDAD

La Revolución en la Educación



**UNIVERSIDAD GALILEO**

**FACULTAD DE INGENIERÍA DE SISTEMAS, INFORMÁTICA**

**Y CIENCIAS DE LA COMPUTACIÓN**

**INSTITUTO DE EDUCACIÓN ABIERTA**

**FISICC-IDEA**

**SEMINARIO DE TELECOMUNICACIONES**

**“Proyecto para la Implementación de Control y Monitoreo de Accesos a las Instalaciones de la Empresa Elite”**

PRESENTADO POR:

**Marcelino Antonio Fajardo Sosa**

**Carné IDE0812344**

Previo a optar el grado académico de:

**LICENCIATURA EN TECNOLOGÍA Y ADMINISTRACIÓN DE LAS  
TELECOMUNICACIONES**

Guatemala, 9 de enero del 2023

## Contenido

A. Descripción de la empresa o mercado .....	1
Antecedentes .....	1
Actividades principales.....	1
Misión .....	2
Visión.....	2
Organigrama .....	2
Productos.....	3
Servicios.....	4
Segmento de mercado .....	4
Principales competidores .....	4
B. Evaluación de la empresa.....	5
Comportamiento de las ventas .....	7
Participación de mercado .....	8
Tecnología de la empresa y tecnología del mercado .....	9
Procesos fundamentales de la empresa .....	10
Estados financieros de la empresa .....	11
C. Hallazgos y evidencias.....	12
Análisis y tabulación de la encuesta .....	12
Encuesta de investigación .....	13
Hallazgos.....	18
D. Identificación del problema .....	19
Incidencia del problema .....	19
Descripción del problema u oportunidad.....	20
Diagrama de flujo del proceso actual.....	21
Desventajas de no resolverse el problema identificado .....	22
Matriz de decisiones .....	23

Matriz de proveedores.....	24
Solución TO-BE.....	25
E. Factibilidad técnica.....	26
E.1. Hardware .....	26
E.2. Software.....	28
E.3. Protocolo de red.....	29
E.4. Seguridad.....	30
E.5. Prototipo .....	31
E.6. Diagrama de red actual .....	32
E.7. Diagrama de red con solución propuesta.....	33
F. Factibilidad administrativa .....	34
F.1. Organigrama propuesto .....	34
F.2. Manual de funciones.....	35
F.3. Factibilidad operativa .....	36
F.3.1 Diagrama de Gantt. Implementación.....	36
F.3.2 Diagrama de Gantt. Capacitación .....	36
F.4. Planes de contingencia.....	37
F.4.1 Análisis de riesgos y establecimiento de controles.....	37
F.5. Análisis de factibilidad legal .....	39
F.6. Análisis de factibilidad ambiental .....	40
F.7. Factibilidad financiera .....	41
Costos.....	41
Beneficio .....	42
Matriz costo – beneficio.....	42
Punto de equilibrio.....	43
Movimiento de fondos .....	44
Conclusiones .....	45

Recomendaciones .....	46
Anexo .....	47
Manual de uso .....	47
Cotización .....	52
Movimiento de fondos optimista .....	53
Movimiento de fondos pesimista .....	54
Glosario.....	55
G. E-grafía.....	56
H. Bibliografía .....	59

## **A. Descripción de la empresa o mercado**

Elite Solutions

### **Antecedentes**

La empresa “Elite Solutions”, fue fundada el 01 de agosto del 2016, en Guatemala, Guatemala. Nace como una empresa líder a la vanguardia en soluciones informáticas y asesorías de seguridad proveer soporte y asesoría en seguridad informática en Guatemala, expandiendo su mercado en Centro América en El Salvador y Honduras.

Elite Solutions, por siete 7 años continuos ha contribuido a que muchas empresas a nivel centro americano a conseguir:

- Ahorro de tiempo
- Reducción de costos
- Aprovechamiento de las tecnologías con un carácter diferenciador para cada cliente.

Mediante los productos y servicios que ofrecemos en el mercado, brindando esto un mejor aprovechamiento de los recursos, de las empresas privadas y sector de gobierno. Ayudando tanto a la administración de forma eficiente y segura de su data y protección de datos.

### **Actividades principales.**

- Brindar soluciones informáticas sencillas, efectivas y orientadas a la necesidad de cada cliente.
- Consultorías informáticas.
- Mantenimientos de sistema y dispositivos informáticos.

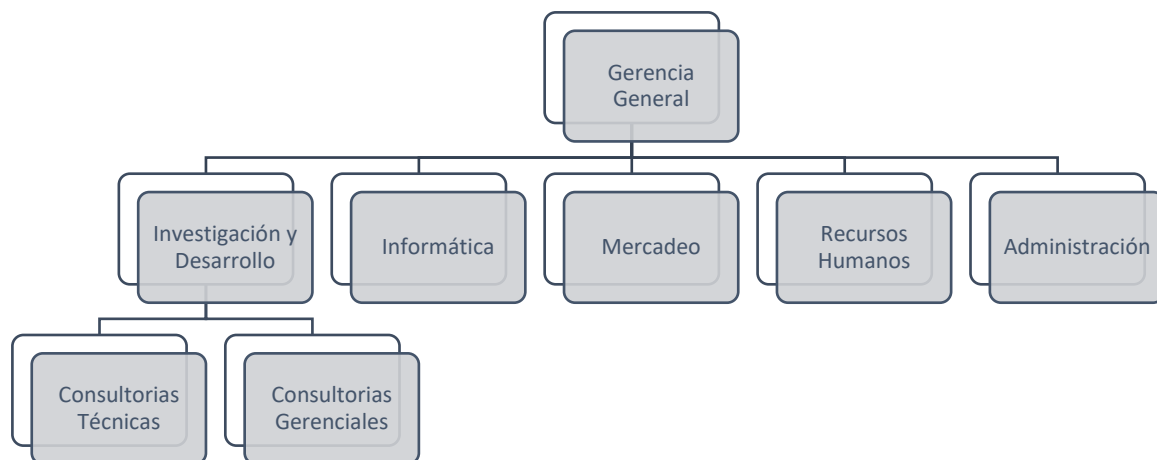
## Misión

Ser una empresa líder dedicada a la implementación de productos y servicios de seguridad informática cumpliendo con los estándares en seguridad de la información, siendo innovadores en la calidad de servicios, productos y tecnologías en evolución.

## Visión

Ser empresa líder, con ventajas competitivas en el área de telecomunicaciones y seguridad informática a nivel nacional y regional, contribuyendo a su desarrollo a través de la prestación de productos y servicios innovadores especializados de software especializados en seguridad informática.

## Organigrama<sup>1</sup>



<sup>1</sup> Fuente: Recursos humanos, Elite solutions

## **Productos**

### **Software de antivirus**

Todos los ordenadores corporativos conectados a la red de trabajo deben contar con un antivirus de calidad y fiable. Los antivirus aportan medidas de protección efectivas ante la detección de un malware o de otros elementos maliciosos, cierran posibles amenazas y son capaces de poner el dispositivo en cuarentena para evitar males mayores.

### **Firewalls perimetrales<sup>2</sup>**

Una de las principales herramientas de seguridad informática es el firewall. Se dedica a escanear los paquetes de red y los bloquea o no según las reglas que previamente ha definido el administrador.

### **Servidores proxy<sup>3</sup>**

Se trata de un dispositivo que actúa como intermediario entre Internet y las conexiones del navegador, y filtra los paquetes que circulan entre ambos puntos. Gracias al proxy se bloquean sitios web que se estima que pueden ser peligrosos o de los que esté prohibida su visita dentro del ambiente laboral. Gracias al proxy también se define un sistema de autenticación que limita el acceso a la red externa.

### **End Point Disk Encryption<sup>4</sup>**

También llamado cifrado de punto final, se trata de un proceso de codificación de datos para que nadie que no guarde la clave de descifrado pueda leerlo. Protege los sistemas operativos de la instalación de archivos corruptos, al bloquear los archivos almacenados en ordenadores, servidores y otros puntos finales.

---

<sup>2</sup> Programa o dispositivo informático que controla el acceso de una computadora a la red.

<sup>3</sup> Software que proporciona una puerta de enlace entre los usuarios e Internet

<sup>4</sup> Software de encriptación de datos utilizado para la seguridad informática

## **Servicios**

### **Escáner de vulnerabilidades**

El escáner es un software que detecta, analiza y gestiona los puntos débiles que tenga el sistema. Y muy importante, mandar alertas en tiempo real al detectar problemas, lo que acorta mucho el tiempo de resolución de los conflictos.

### **Gestión de eventos e información de seguridad (SIEM)**

Visibilidad centralizada para detectar, investigar y responder a las amenazas de ciberseguridad más críticas de toda su empresa.

### **El centro de operaciones de seguridad (SOC)**

Se refiere al equipo responsable de garantizar la seguridad de la información. El SOC es una plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota.

### **Segmento de mercado**

La empresa está orientada tanto para el sector privado y el sector público, enfocada a la mediana y grande empresa que cuenten con infraestructura informática que pueda estar en riesgos la información de no contar con las medidas de seguridad tecnológica necesarias para mitigar las amenazas actuales.

### **Principales competidores**

1. Segga Guatemala  
<https://gruposiega.net/>
2. Tigo Business  
<https://www.tbo.com.gt/>
3. Smart Solutions  
<https://smart-latam.com/>



## B. Evaluación de la empresa

Herramienta de diagnóstico: FODA

Tabla 1 Herramienta de diagnóstico: FODA

	Fortalezas	Debilidades
	<ul style="list-style-type: none"> <li>-Personal certificado y en constante capacitación.</li> <li>-Uso de hardware y tecnología de nube de última generación.</li> <li>-Convenios con empresas extranjeras para apoyo en tecnología.</li> <li>-Disponibilidad de soporte 24/7</li> <li>-Creación de soluciones y/o consultoría a medida.</li> </ul>	<ul style="list-style-type: none"> <li>-Falta de personal con certificaciones específicas solicitadas por el cliente.</li> <li>-Dificultad para mantenerse a la vanguardia en tecnología por la rápida evolución de esta.</li> <li>-Falta de innovación en servicios comparado con la competencia.</li> <li>-Limitante de existencia de productos que la competencia pueda tener para entrega inmediata.</li> </ul>
Interior		
	Oportunidades	Amenazas
	<ul style="list-style-type: none"> <li>-Crecimiento de necesidades tecnológicas para medianas empresas.</li> <li>-Demanda de servicios informáticos con tiempos de respuesta más eficientes.</li> <li>-Proyectos finalizados que pueden ser replicables para otros clientes potenciales al tener un modelo funcional implementado.</li> <li>-Escalabilidad de proyectos existentes.</li> <li>-Importación de nuevas tecnologías para ser pioneros en la región.</li> </ul>	<ul style="list-style-type: none"> <li>-Crecimiento de cobertura de servicios de los competidores.</li> <li>-Moderación de inversión en tecnología de clientes debido a inestabilidad por pandemia.</li> <li>-Surgimiento de nuevas tecnologías amigables que el cliente pueda adquirir directamente del fabricante.</li> </ul>
Exterior		

Tabla 2 Matriz FODA: Maxi-Mini

FO (Maxi-Maxi)	DO (Mini-Maxi)
<p>-Mantener un contacto adecuado con los clientes sobre mejoras de servicios y/o escalabilidad que puedan ayudarlos a la mejora de eficiencia de sus procesos actuales.</p> <p>-Creación de pruebas de concepto de nuevas tecnologías para ofrecer a nuevos clientes potenciales.</p>	<p>-Generar un plan de capacitación de personal sobre certificaciones en nuevas tecnologías.</p> <p>-Análisis de ventas y tendencia de mercado para proyectar un inventario suficiente que abastezca la demanda.</p> <p>-Creación de planes a mediano y largo plazo para mantener el desarrollo tecnológico interno de la empresa.</p>
FA (Maxi-Mini)	DA (Mini-Mini)
<p>-Generar estrategias de marketing que puedan posicionar la empresa como referente en el mercado.</p> <p>-Crear nuevas alianzas estratégicas para la representación de nuevos productos.</p>	<p>-Aumento de seguridades internas y compartimentación de áreas de trabajo.</p> <p>-Adquisición de nuevas tecnologías en auge.</p>

## Comportamiento de las ventas

Empresa: Elite Solutions

Periodo fiscal: 2022

Tabla 3 Comportamiento de ventas de Elite Solutions<sup>5</sup>

	<b>Enero a Marzo</b>	<b>Abril a Junio</b>	<b>Julio a Septiembre</b>	<b>Octubre a Noviembre</b>
<b>Productos</b>	9	7	11	4
<b>Servicios</b>	13	22	18	7
<b>Total vendido</b>	22	29	29	11
<b>Incremento/Decremento</b>	22	7	0	-18

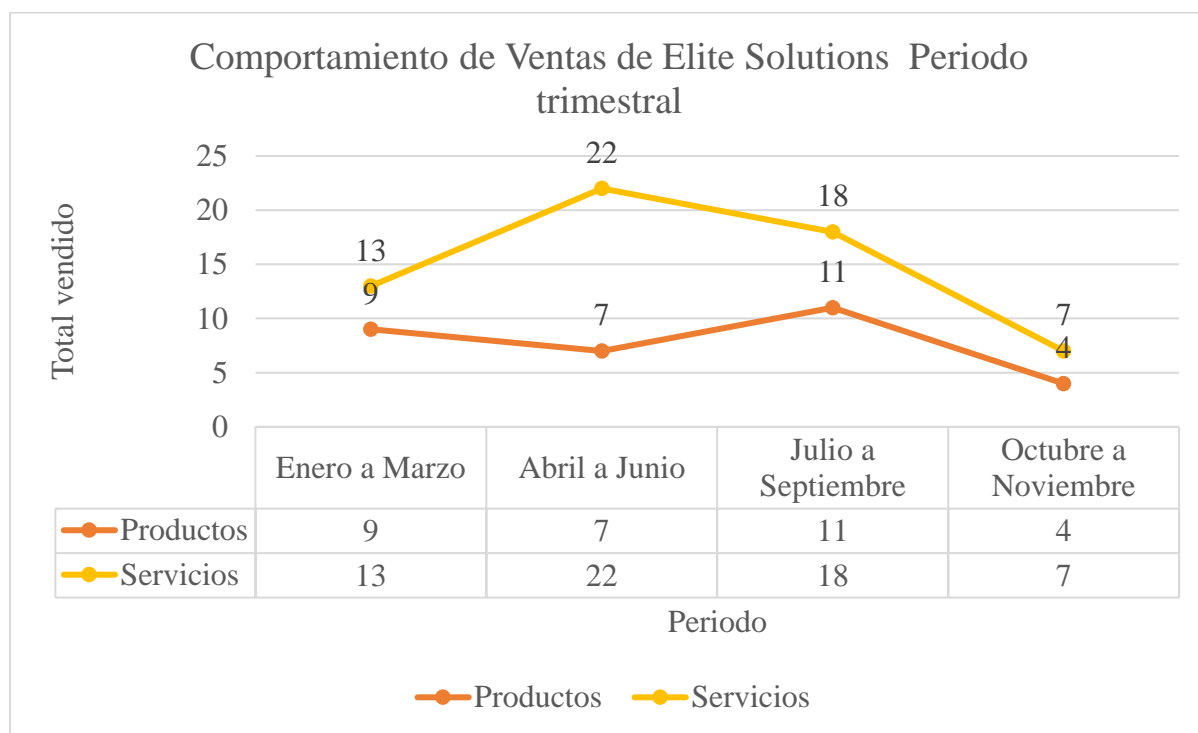


Ilustración 1 Comportamiento de ventas de Elite Solutions

<sup>5</sup> Fuente: Departamento de finanzas Elite

## Participación de mercado

Según el informe “Producto interno bruto Trimestral, segundo trimestre 2022<sup>6</sup>”, en su Cuadro 2: Producto Interno Bruto Trimestral medido por el origen de la producción.

Tomando de referencia la actividad económica en la que se encuentra Elite Solutions la cual sería: “Información y comunicaciones”, este representa un 3.7% del producto interno bruto del país. (Guatemala, 2022) En el año 2021 la cifra del PIB de Guatemala fue de 72,642 millones de euros. (Macro, s.f.)

### Cálculo:

Ingresos totales de la industria = (Cifra PIB Guatemala 2021) \* (% de actividad económica)

Ingresos totales de la industria = (72,642,000,000euros) \* (3.7%)

***Ingresos totales de la industria = 2,687,754,000 Euros***

Ingresos comerciales = 2,687,754,000 euros \* 7.73 Quetzales<sup>7</sup>

***Ingresos comerciales = 20,776,338,420 Quetzales***

Participación de mercado = (Ingresos comerciales / Ingresos totales de la industria) x 100

Participación de mercado = (3,5000,000 Quetzales<sup>8</sup> / 20,776,338,420 Quetzales) x 100

Participación de mercado = (3,5000,000 Quetzales / 20,776,338,420 Quetzales) x 100

**Participación de mercado = 0.017%**

---

<sup>6</sup> Informe Producto Interno Bruto Trimestral:

[https://www.banguat.gob.gt/sites/default/files/banguat/cuentasnac/PIB2013/2T\\_2022\\_JM\\_AR2013.pdf](https://www.banguat.gob.gt/sites/default/files/banguat/cuentasnac/PIB2013/2T_2022_JM_AR2013.pdf)

<sup>7</sup> Tipo de cambio entre el euro y el quetzal al 21 de octubre de 2022 [https://www.banguat.gob.gt/tipo\\_cambio/](https://www.banguat.gob.gt/tipo_cambio/)

<sup>8</sup> Datos estimados de ingresos proveído por Departamento de finanzas Elite

## Tecnología de la empresa y tecnología del mercado

Tipo de equipo	Tecnología de Elite Solutions	Tecnologías del mercado
	Lector de huellas dactilares y RFID T5S <sup>9</sup> 32-Bit CPU	Terminal de Reconocimiento Facial Inteligente Todo en Uno <sup>10</sup> Dual Core 1.0GHz Velocidad de reconocimiento <0.3s Cámara 1080HD

<sup>9</sup> Lector de huellas dactilares: <https://www.anviz.com/es/product/t5s-access-control.html>

<sup>10</sup> Terminal de reconocimiento facial inteligente: <https://www.anviz.com/es/facepass7pro-smart-face-recognition-terminal.html>

## **Procesos fundamentales de la empresa**

### Dirección

1. Toma de decisiones
2. Organización y control

### Comercialización

1. Promocionar productos y servicios
2. Definir precios
3. Establecer presupuestos

### Gestión de proveedores

1. Establecer comunicación directa con proveedores

### Gestión de personal

1. Proceso de contrataciones
2. Control de inducción y capacitaciones
3. Control de ausencias y retrasos
4. Registro y archivos de datos.

### Gestión de atención a clientes

1. Proporcionar atención especializada al cliente
2. Brindar consultorías informáticas
3. Realizar mantenimiento de equipos informáticos.

### Procesos contables

1. Registrar las actividades económicas de la empresa
2. Elaboración de presupuestos
3. Actualización de libros contables
4. Pagos de planilla de empleados
5. Proveer de recursos económicos de las diversas áreas.

## **Estados financieros de la empresa**

Debido a la sensibilidad de la información de Elite Solutions, no se puede compartir ningún tipo de información financiera.

## C. Hallazgos y evidencias

### Análisis y tabulación de la encuesta

De instrumento se utilizó la aplicación de una encuesta con el objetivo de obtener un análisis del proyecto “*Implementación de control y monitoreo de accesos a las instalaciones de la empresa Elite*”, se tomó una muestra de 16 encuestados con un universo de 25 empleados existentes en la empresa. Mediante los cuales se identifica los principales puntos que requieren atención, con lo cual se hace evidente la imperante necesidad de un control y monitoreo de las instalaciones.



## Encuesta de investigación

Proyecto “Implementación de control y monitoreo de accesos a las instalaciones de la empresa Elite”

### 1. ¿Se monitorea las oficinas de la empresa fuera del horario laboral?

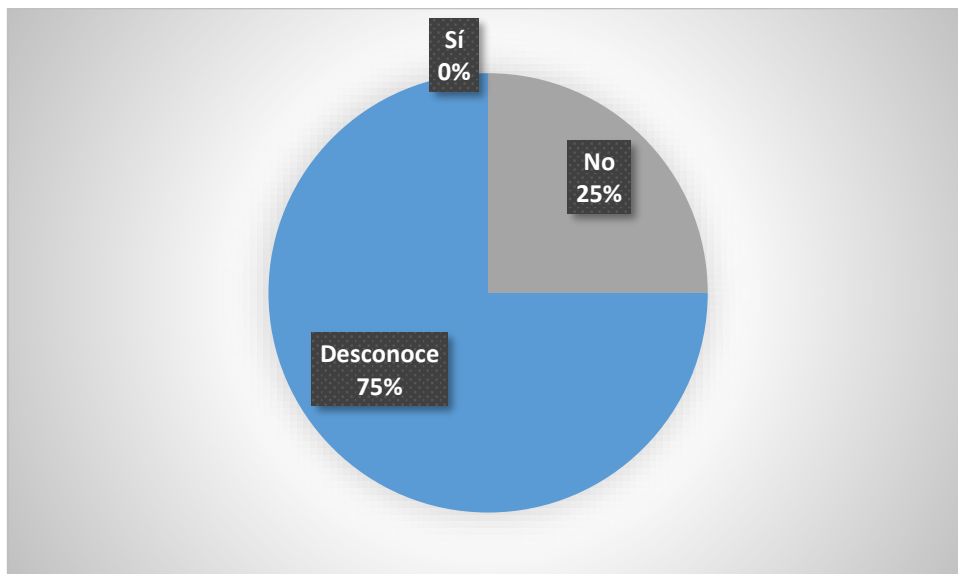
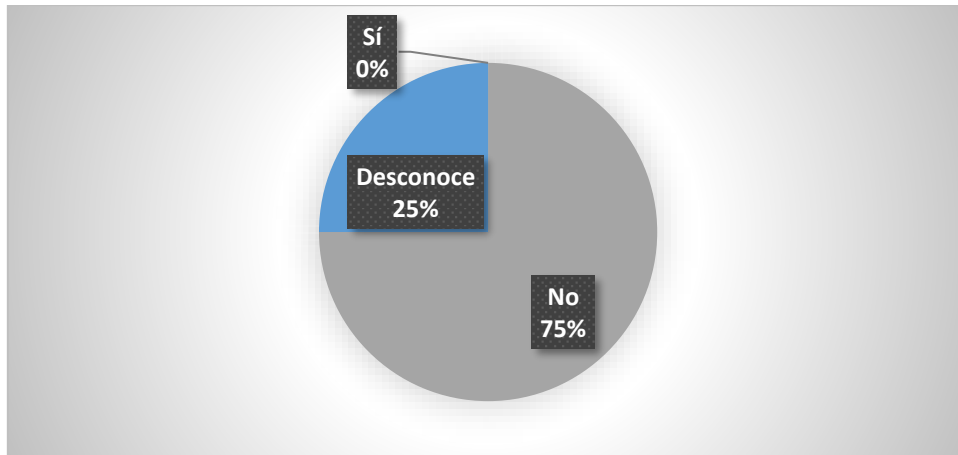


Ilustración 2 Gráfico de consulta de monitoreo de oficinas

El resultado obtenido nos indica que 75% de la muestra del personal encuestado, desconoce si se monitorean las oficinas en horarios no laborables, el 25% restante, indican que no se realiza monitoreo en los horarios especificados.

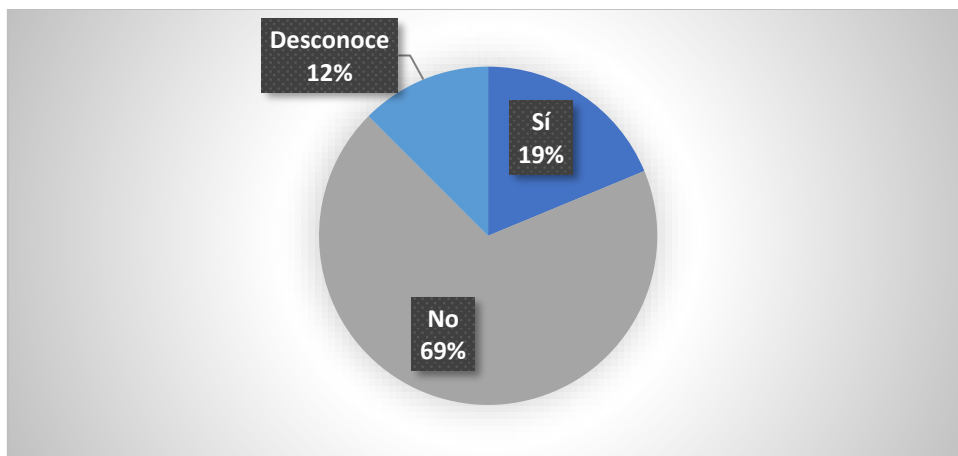
**2. ¿Se registran los ingresos y salidas del personal a las diferentes áreas de oficinas?**



*Ilustración 3 Gráfico de consulta registro de ingresos y salidas del personal*

El resultado de la muestra del personal encuestados manifiesta con un 75% la no existencia de registros de ingresos y salidas del personal por ende y el otro 25% desconoce si este control existe.

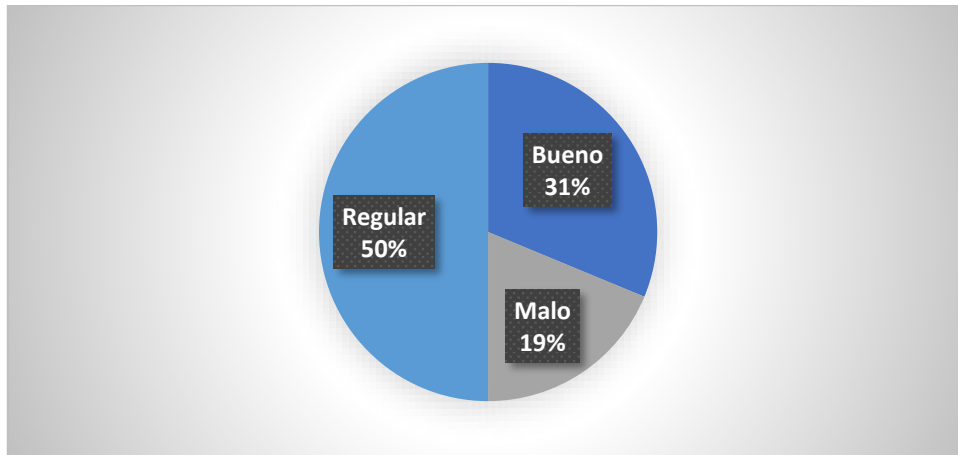
**3. ¿Se tiene un protocolo para autorizar el ingreso de visitas a las oficinas?**



*Ilustración 4 Gráfico de consulta de protocolo de autorización de ingreso*

En su mayoría, los encuestados indican que no se tiene un protocolo de autorización de ingreso de visitas a las oficinas. Superando el 65% de la muestra del universo.

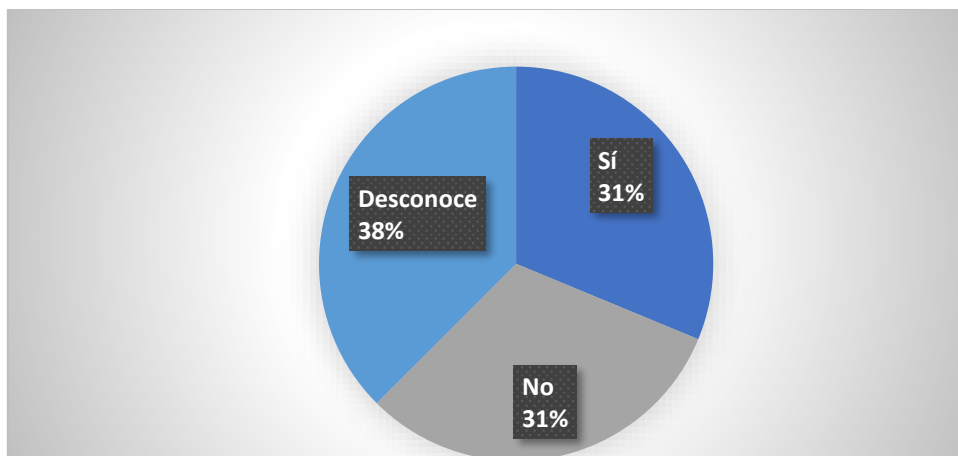
**4. ¿Cómo calificaría el control de acceso para el público en general?**



*Ilustración 5 Gráfico de calificación de control de acceso*

El 50% de la muestra del personal encuestado califica el proceso de control de acceso de la empresa como Regular, un 31% lo considera Bueno y el 19% considera que los procesos de control no están malos.

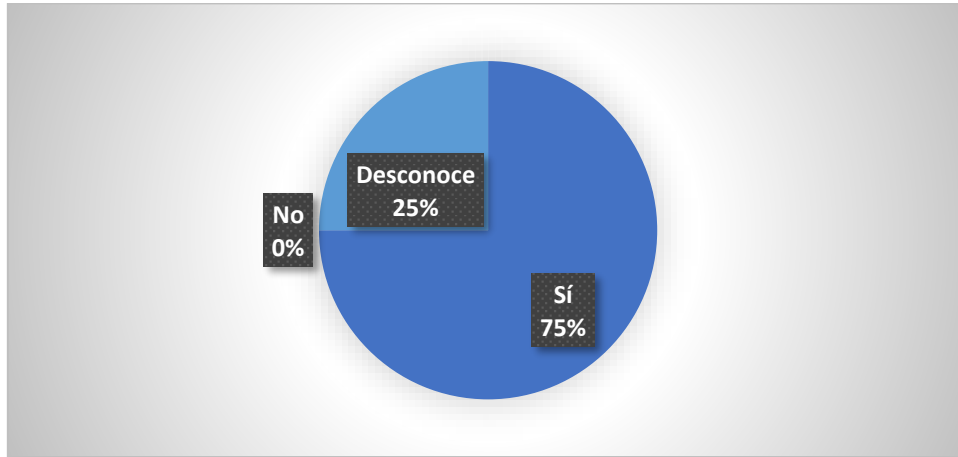
**5. ¿Se tiene un protocolo para autorizar el ingreso de personal a áreas restringidas?**



*Ilustración 6 Gráfico de consulta de protocolo de autorización de ingreso*

En cuanto a las áreas restringidas de la empresa, la muestra de personal encuestado indica en un 38% que desconoce su existencia, por otra parte, para los que indican que sí o no existe un protocolo de autorización, en ambos casos el porcentaje de respuestas es de un 31%.

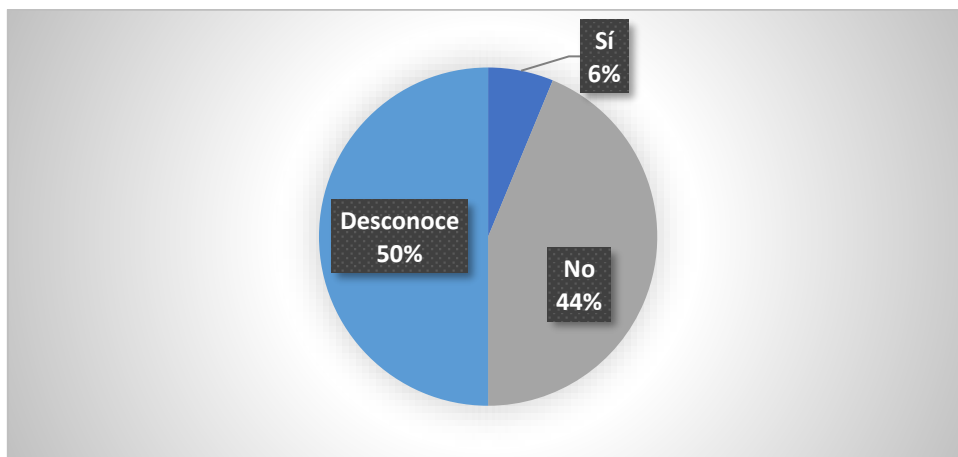
**6. ¿Se permite el uso de dispositivos electrónicos y/o de almacenamiento en todas las áreas?**



*Ilustración 7 Gráfico permiso de uso de dispositivos*

Se identifica que no hay restricciones en el uso de dispositivos electrónicos y/o de almacenamiento en todas las áreas, siendo un 75% de la muestra del personal encuestado los que indican que está permitido su uso.

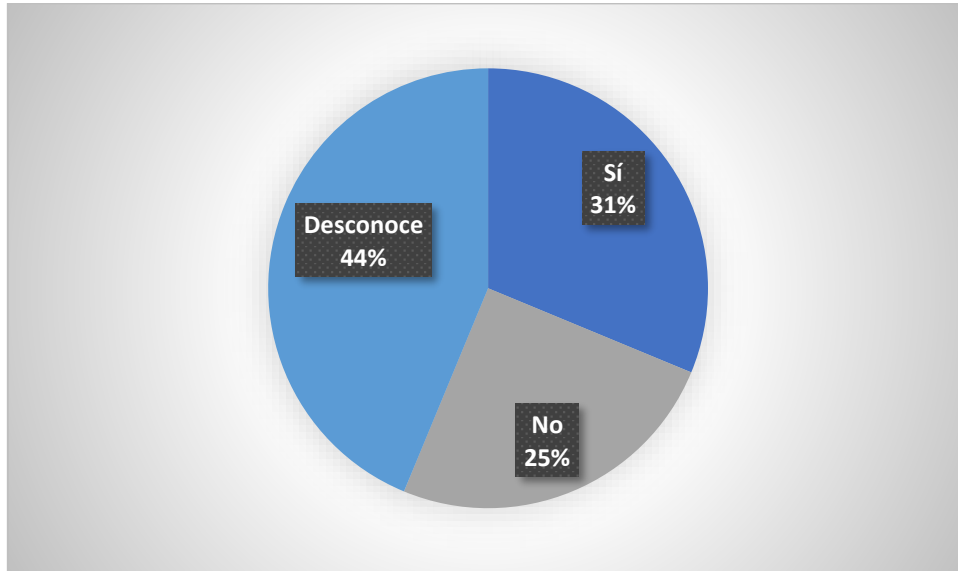
**7. ¿Se cuenta con alarma contra intrusos para accesos no autorizados en horas fuera de horario laboral?**



*Ilustración 8 Gráfico de consulta de existencia de alarma contra intrusos*

La mitad de la muestra del personal encuestado, indica que desconoce si existen alarmas contra intrusos y un 44% adicional considera que no existen estos controles para accesos no autorizados en horas fuera del horario laboral.

**8. ¿Tiene conocimiento de cuáles son las áreas de oficina a las cuales tiene permitido el ingreso?**



*Ilustración 9 Gráfica de consulta de áreas permitidas*

El 44% de la muestra del personal encuestado indica que desconoce cuáles son las áreas de oficina a las cuales tiene permitido el ingreso y otro 25% indica que no conoce estas. Siendo solo un 31% del personal que indican que sí están al tanto de ellas.

## Hallazgos

1. Ninguno de la muestra del personal encuestados indica que conoce si se realiza monitoreo en las oficinas de la empresa fuera del horario laboral.
2. Se identifica en base a la muestra del personal encuestada que no se realizan registros o no se tienen métodos que permitan el registro de los ingresos y egresos del personal en las diversas áreas. Siendo un total de 0% los que indiquen lo contrario.
3. Menos del 20% de la muestra del personal encuestado, indica que sí existen protocolos para autorizar el ingreso de visitas a la oficina, dejando en claro que en su mayoría este proceso se realiza sin medidas de control.
4. Se logra identificar que existe cierta aceptación del proceso de control de acceso para el público en general. Siendo solamente un 19% de la muestra de personal encuestado quienes lo califican como malo.
5. Se desconocen o se niega la existencia de protocolos de autorización de ingreso de personal a áreas restringidas.
6. No se establece un control en cuanto al uso dispositivos electrónicos y/o de almacenamiento en todas las áreas, siendo una nulidad los que indiquen lo contrario.
7. Es un pequeño sector de la muestra del personal encuestado que indican que sí existen con alarma contra intrusos para accesos no autorizados en horas fuera de horario laboral, alcanzando un 6% de total
8. En su mayoría el personal encuestado indica desconocer cuales son las áreas de oficina a las cuales tiene permitido el ingreso.

## **D. Identificación del problema**

La falta de protocolos y controles de acceso da como resultado que las áreas de oficinas sean de libre acceso para los empleados sin importar si estos están o no autorizados para ingresar a las diferentes oficinas de la empresa, provocando falta de supervisión y auditoría ante eventos que se puedan generar.

### **Incidencia del problema**

- Riesgo de acceso de los empleados y/o personal de visita a áreas no autorizadas.
- Deficiencia a respuestas de emergencia ante ingreso de intrusos durante horas no laborales para la protección de los bienes físicos e información.
- Falta de bitácora de registros de control para monitoreo y auditoría ante incidentes.
- Carencia de información para el registro de empleados y control de labores.
- Inexactitud para la trazabilidad de eficiencia de personal.

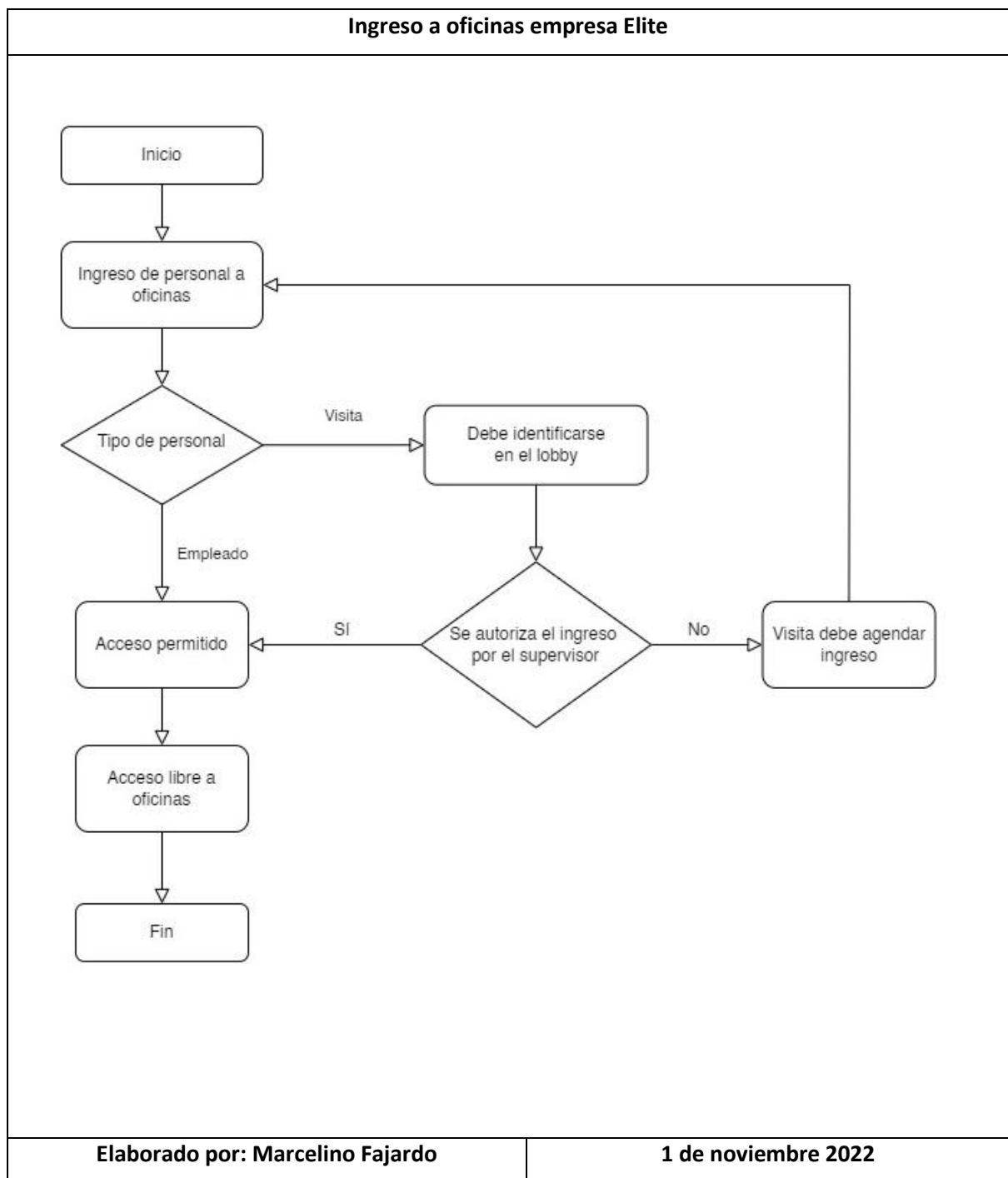
## **Descripción del problema u oportunidad**

La deficiencia en los controles de acceso dentro de las oficinas de la empresa Elite genera una falta de control de los empleados, así como también personal externo de visitas, el riesgo más importante es la seguridad donde las instalaciones no limitan el ingreso a áreas no autorizadas, esto genera la vulnerabilidad ante un robo de equipos y/o información., no solo es una vulnerabilidad en horas laborales ya que también se puede dar la situación en horas no laborales donde el impacto puede ser mayor al no tener un sistema que pueda detectar la presencia de intrusos y tener una respuesta de acción inmediata.

La carencia de las bitácoras de control a su vez deriva al retraso y falta de información para supervisores encargados de velar por el cumplimiento eficiente del personal en oficina y poder tener una herramienta que les ayude ante incidentes de cualquier índole que se necesite individualizar responsabilidades en áreas específicas.



## Diagrama de flujo del proceso actual



Fuente: elaboración propia utilizando la herramienta web <https://app.diagrams.net/>

## **Desventajas de no resolverse el problema identificado**

### Desventajas a corto plazo

- Se proyecta una imagen poco profesional en las instalaciones ante la visita de los clientes.
- Incidentes en áreas sin poder determinar responsables.
- Acceso de personal no capacitado y/o autorizado a áreas sensibles.
- Deficiencia para llevar un control interno y generación de reportes del personal y visitas

### Desventajas a largo plazo

- Robo de equipo en áreas de poco monitoreo o presencia de personal.
- Fuga de información por falta de segmentación y compartimentación entre las áreas de oficinas.

## Matriz de decisiones

### Matriz tecnológica de hardware de sistemas de control de acceso

MDT	Suprema <sup>11</sup>	ZKteco <sup>12</sup>	Hikvision <sup>13</sup>
Registro de ingresos y salidas	1	1	1
Generación de informes detallados	1	1	1
Crear zonas de acceso restringido	1	1	1
Manejo de base datos con opción de importar y exportar	1	1	0
Acceso sin contacto	1	1	1
Acceso biométrico	1	1	1
Acceso por tarjeta	1	1	1
Acceso por código	1	1	1
Plataforma de administración unificada	1	1	1
Integración de aplicación móvil	1	0	0
Puntaje / Total	10/10	9/10	8/10

<sup>11</sup> <https://www.supremainc.com/es/hardware/biometric-products.asp>

<sup>12</sup> <https://www.zktecolatinoamerica.com/>

<sup>13</sup> <https://www.hikvision.com/es-la/products/Access-Control-Products/>

## Matriz de proveedores

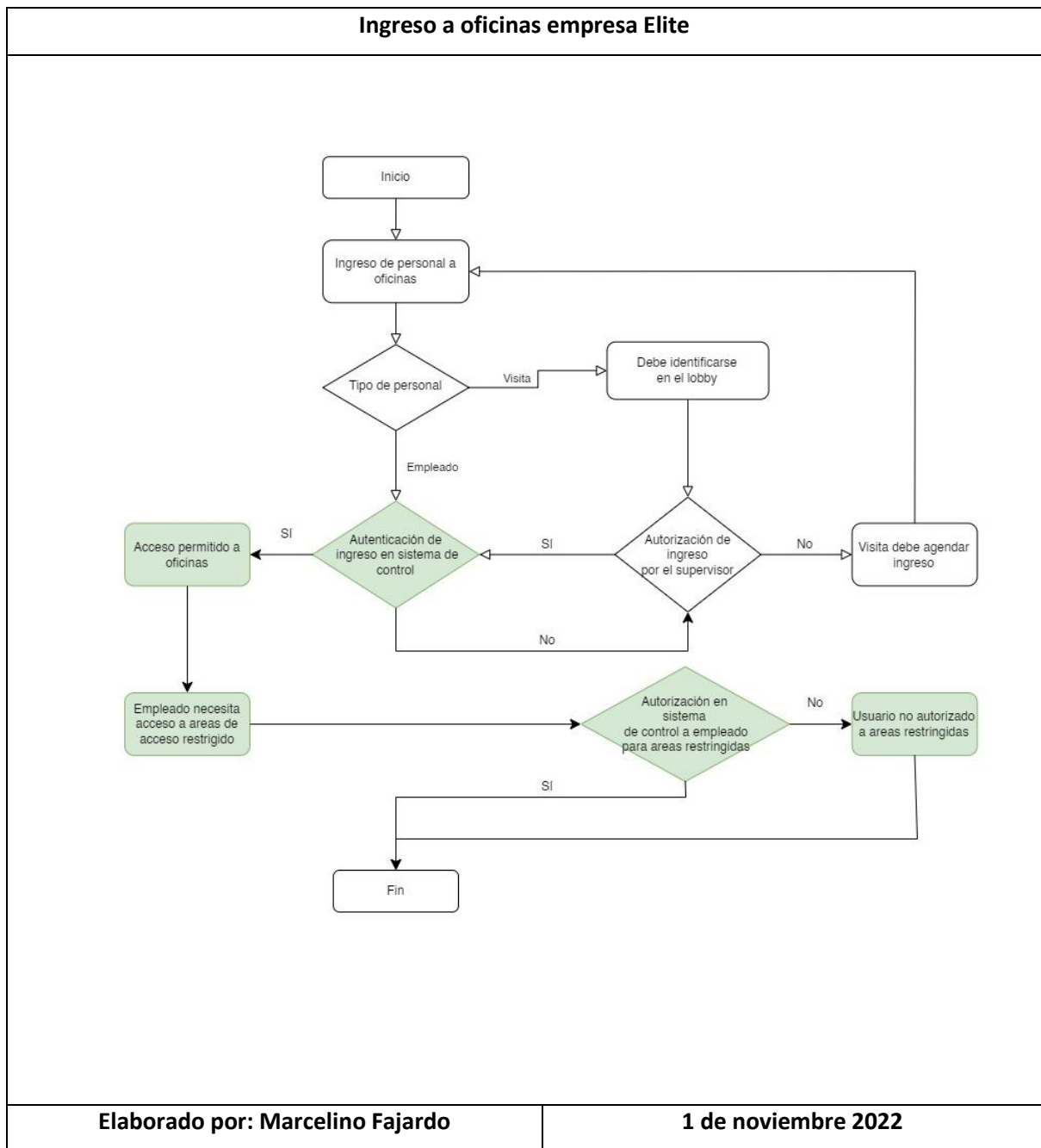
MDP	INALARM <sup>14</sup>	CHIPCOM <sup>15</sup>	Cámaras de seguridad Guatemala <sup>16</sup>
Garantía de equipo por 1 o más años	1	1	1
Disponibilidad en almacén de los dispositivos	1	0	1
Soporte 24/7	1	0	0
Servicio de soporte en sitio	1	1	1
Tiempo de entrega de equipo en 1 semana o menor	1	1	1
Instalación de equipo	1	1	0
Servicio de mantenimiento	1	1	0
Puntaje / Total	7/7	5/7	4/7

<sup>14</sup> <https://inalarm.gt/>

<sup>15</sup> <https://chipcom.com.gt/>

<sup>16</sup> <https://camarasdeseguridad.com.gt/>

## Solución TO-BE



Fuente: elaboración propia utilizando la herramienta web <https://app.diagrams.net/>

## E. Factibilidad técnica

### E.1. Hardware <sup>17</sup>

Descripción	Características	Uso
FaceStation F2 <sup>18</sup>	<p><b>Biometría</b></p> <ol style="list-style-type: none"> <li>1. FSF2-DB, AB: Facial / FSF2-ODB: Facial, Huella dactilar</li> <li>2. detección de Huellas reales: FSF2-DB, AB: - / FSF2-ODB: Soportado (basado en SW)</li> <li>3. Protección IP65</li> </ol> <p><b>RF</b></p> <ol style="list-style-type: none"> <li>4. FSF2-DB: 125 kHz EM &amp; 13.56 MHz MIFARE, MIFARE Plus, DESFire EV1/EV2(2), FeliCa</li> <li>5. SF2-AB: 125 kHz EM, HID Prox &amp; 13.56 MHz MIFARE, MIFARE Plus, DESFire EV1/EV2(2), FeliCa, iCLASS SE/SR/Seos</li> <li>6. FSF2-ODB: 125 kHz EM &amp; 13.56 MHz MIFARE, MIFARE Plus, DESFire EV1/EV2(2), FeliCa</li> <li>7. BSA2-OMPW: NFC / BSA2-OIPW: NFC</li> </ol> <p><b>Móvil</b></p> <ol style="list-style-type: none"> <li>8. NFC, BLE</li> </ol> <p><b>Capacidad</b></p> <ol style="list-style-type: none"> <li>9. 100,000 usuarios</li> <li>10. Máximo credenciales (1:N) para rostros: 50,000 y huella dactilar: 100,000</li> <li>11. Máximo credenciales (1:1) para rostros: 100,000 Huella dactilar: 100,000 PIN: 100,000 Tarjeta: 100,000</li> <li>12. Máximo registro de texto: 5,000,000</li> <li>13. Máximo registro de imágenes: 50,000</li> </ol> <p><b>Interfaces</b></p> <ol style="list-style-type: none"> <li>14. TCP/IP</li> <li>15. RS-485: 1 canal Host o Esclavo</li> <li>16. Wiegand: un canal de entrada o salida</li> <li>17. E/S dos entradas</li> <li>18. 1 Relé</li> <li>19. USB 2.0 (host)</li> </ol> <p><b>Hardware</b></p> <ol style="list-style-type: none"> <li>20. CPU: Cuádruple Núcleo de 1.8 GHz + CPU de Cuádruple Núcleo de 1.4 GHz</li> <li>21. Memoria: 16 GB de Flash + 2 GB de RAM</li> <li>22. Soporta Crypto Chip</li> <li>23. Audio de 16 bits</li> <li>24. Temperatura operativa: - 20 °C ~ 50 °C</li> </ol>	<p>Establecer reglas de tiempo y asistencia, ajuste de turnos, visitas calendarizadas, servidor de autenticación, registro y gestión de visitas, autenticación de rostros.</p>

<sup>17</sup> [https://spm.biostar2.com/help/en/index.html?install\\_systemrequirement.htm](https://spm.biostar2.com/help/en/index.html?install_systemrequirement.htm)

<sup>18</sup> BioStation A2: [https://www.supremainc.com/images/upload/brochure/Product\\_Line\\_up\\_Brochure\\_ES.pdf?v2](https://www.supremainc.com/images/upload/brochure/Product_Line_up_Brochure_ES.pdf?v2)

	<ul style="list-style-type: none"> <li>25. Seguro contra alteraciones: Tamper</li> <li>26. Alimentación: 12 VDC</li> <li>27. Dimensiones: FSF2-DB, AB: 119.8 x 223 x 23.5 FSF2-ODB: 119.8 x 268.4 x 49.7</li> <li>28. Certificaciones: CE, FCC, KC, RoHS, REACH, WEEE</li> </ul>	
DE-620 <sup>19</sup>	<ul style="list-style-type: none"> <li>1. USB 2.0 integrado</li> <li>2. CPU: ARM 32 bit Cortex M3(72MHz)</li> <li>3. Potencia de entrada: DC5V, 200mA (USB)</li> </ul> <p>Tarjetas admitidas</p> <ul style="list-style-type: none"> <li>1. CSN: MIFARE Classic, MIFARE Plus, Felica, DESFire</li> <li>2. Método de acceso a la tarjeta: MIFARE Classic</li> </ul>	Lector/grabador de tarjetas inteligentes
BioMini plus 2 <sup>20</sup>	<ul style="list-style-type: none"> <li>1. USB 2.0 integrado</li> <li>2. Lector de huellas dactilares</li> </ul>	Dispositivo de registro de huellas dactilares
Servidor virtual	<ul style="list-style-type: none"> <li>1. CPU: 4GHz 16 Core</li> <li>2. RAM: 32 GB</li> <li>3. SSD: 1 TB</li> </ul>	Servidor BioStar 2

Fuente: Elaboración propia

		
FaceStation F2 de Suprema Inc <sup>21</sup>	DE-620: Lector/grabador de tarjetas inteligentes <sup>22</sup>	BioMini: Dispositivo de registro de huellas dactilares <sup>23</sup>

<sup>19</sup> <http://www.duali.com/en/product/reader/desktop-reader/de-620--de-620r/>

<sup>20</sup> DE-620: <https://support.supremainc.com/en/support/solutions/articles/24000068279--faqs-using-de-620-with-suprema-integration-options>

<sup>21</sup> <https://www.supremainc.com/es/hardware/fusion-multimodal-terminal-facestation-f2.asp>

<sup>22</sup> <http://www.duali.com/en/product/reader/desktop-reader/de-620--de-620r/>

<sup>23</sup> <https://www.suprema-id.com/es/contents/detail.php?code=010104>

## E.2. Software<sup>24</sup>

Descripción	Características
Sistema operativo del servidor	Windows Server 2016
Sistema operativo del cliente	Windows 10, 64 bit
Base de datos	SQL Server 2016 SP1
Navegador web	Google Chrome versión 107.0.5304
BioStar 2 aplicación móvil para Android	Versión 2.6.3.0

Fuente: Elaboración propia

---

<sup>24</sup> [https://spm.biostar2.com/help/en/index.html?install\\_systemrequirement.htm](https://spm.biostar2.com/help/en/index.html?install_systemrequirement.htm)



### E.3. Protocolo de red<sup>25</sup>

Protocolo/Puerto	Descripción
DHCP (67)	Utilizada para permitir que el dispositivo utilice una dirección IP dinámica.
DNS (23)	Servidor de nombres de dominio
Web Socket (9002)	Socket web del servidor BioStar
Base de datos (3312)	Conexión con la base de datos configurada.
TCP (1433, 4022, 135, 1434,) UDP (1434) <sup>26</sup>	Servicios de motor de la base de datos SQL Server
T&A HTTPS (3002, 3000) <sup>27</sup>	Transmisión de video
AC Cloud (52000, 8781. 8786)	Servicios en la nube
NGrok (4443)	Permite exponer a internet una URL generada dinámicamente, la cual apunta a un servicio web que se está ejecutando en nuestra máquina local.  Dirección URL: cloud.biostar2.com, api.biostar2.com
HTTPS (443)	Proporcionará una conexión segura entre el cliente y el servidor.
WebDAV (445)	Uso compartido de archivos
API (27017, 9010)	Servidor API local
Web Server (9002)	Actualizaciones de versiones
BioStar (51211)	BioStar, conexión del dispositivo al servidor
BioStar (51212)	BioStar, conexión de servidor a dispositivo
FastCGI (9000)	Servidor Web NGinx
HTTPS (8081, 8082) <sup>28</sup>	Agente USB

Fuente: Elaboración propia

<sup>25</sup> [https://spm.biostar2.com/help/en/device\\_edit\\_network.htm](https://spm.biostar2.com/help/en/device_edit_network.htm)

<sup>26</sup> <https://learn.microsoft.com/es-es/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver16>

<sup>27</sup> [https://spm.biostar2.com/help/en/index.html?install\\_server.htm](https://spm.biostar2.com/help/en/index.html?install_server.htm)

<sup>28</sup> <https://support.supremainc.com/en/support/solutions/articles/24000005909--biostar-2-server-and-device-port-usage>

#### E.4. Seguridad<sup>29</sup>

Descripción	Características
Cifrar datos personales en la base de datos	Todos los datos confidenciales, incluidos los datos de credenciales y la información personal, se almacenarán en la base de datos cifrados.
Cifrado de datos personales	Clave de cifrado de datos personales de 32 caracteres usando letras, números y símbolos
Certificados de comunicación	<p>BioStar 2 crea y envía un certificado al dispositivo. El dispositivo puede usar un canal seguro para intercambiar datos con BioStar 2 usando este certificado.</p> <p>Para utilizar un certificado externo, se deben cargar los archivos de certificado raíz, certificado de clave pública y clave privada.</p> <p>Estos certificados son configurados para ser usados una o más veces, una vez que el estado cambia el certificado será eliminado y no podrá volver a usarse</p>
VPN	El servidor estará en la LAN del cuarto de servidores, contará con una VPN (Red Privada Virtual) configurada para acceder a la red.
Firewall	Cortafuegos CheckPoint configurado para controlar los accesos a la red de la empresa.

Fuente: Elaboración propia

<sup>29</sup> [https://spm.biostar2.com/help/en/index.html?settings\\_security.htm](https://spm.biostar2.com/help/en/index.html?settings_security.htm)

## E.5. Prototipo

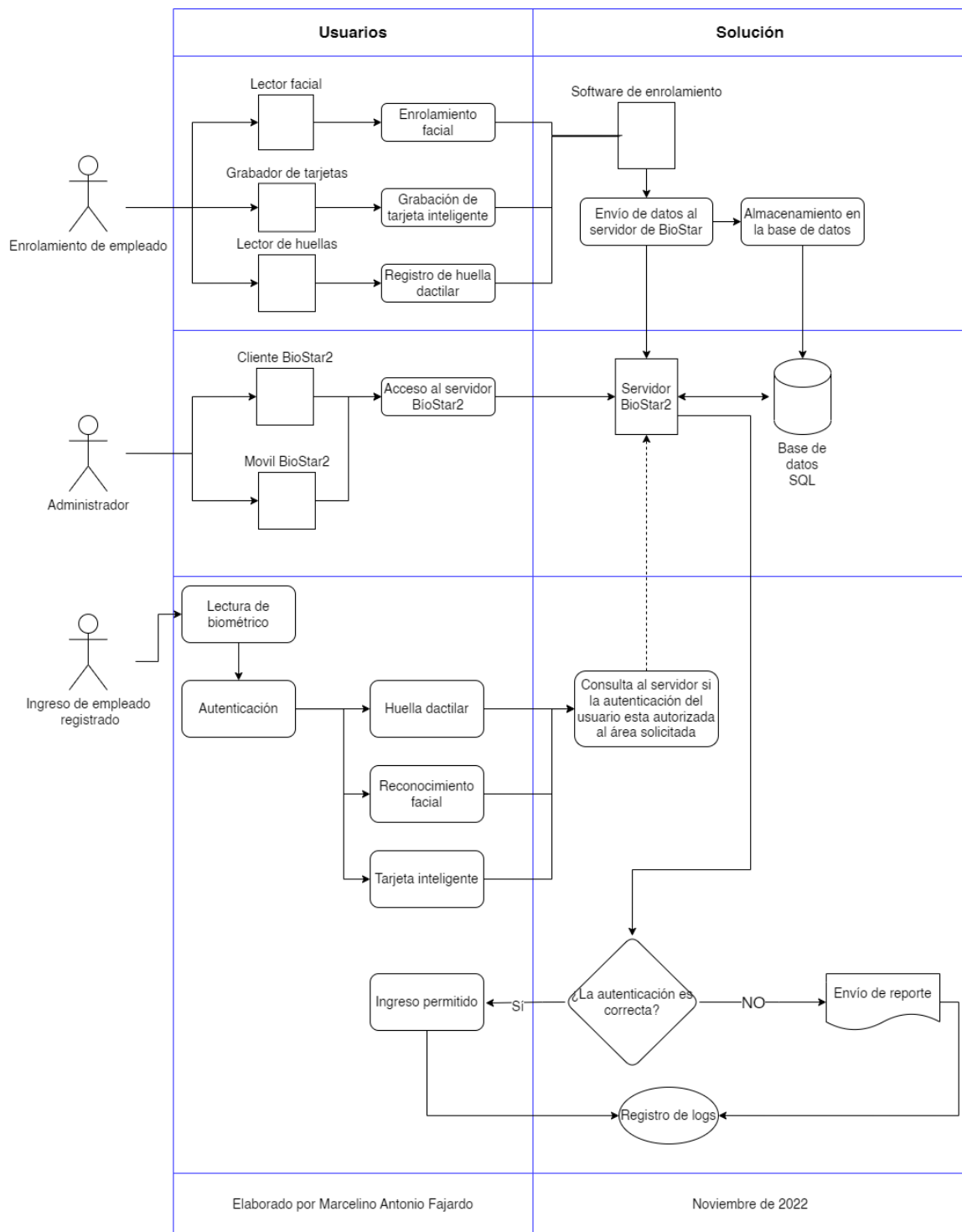


Ilustración 10 Diagrama UML de prototipo de solución

Fuente: Elaboración propia utilizando la herramienta web <https://app.diagrams.net/>

## E.6. Diagrama de red actual

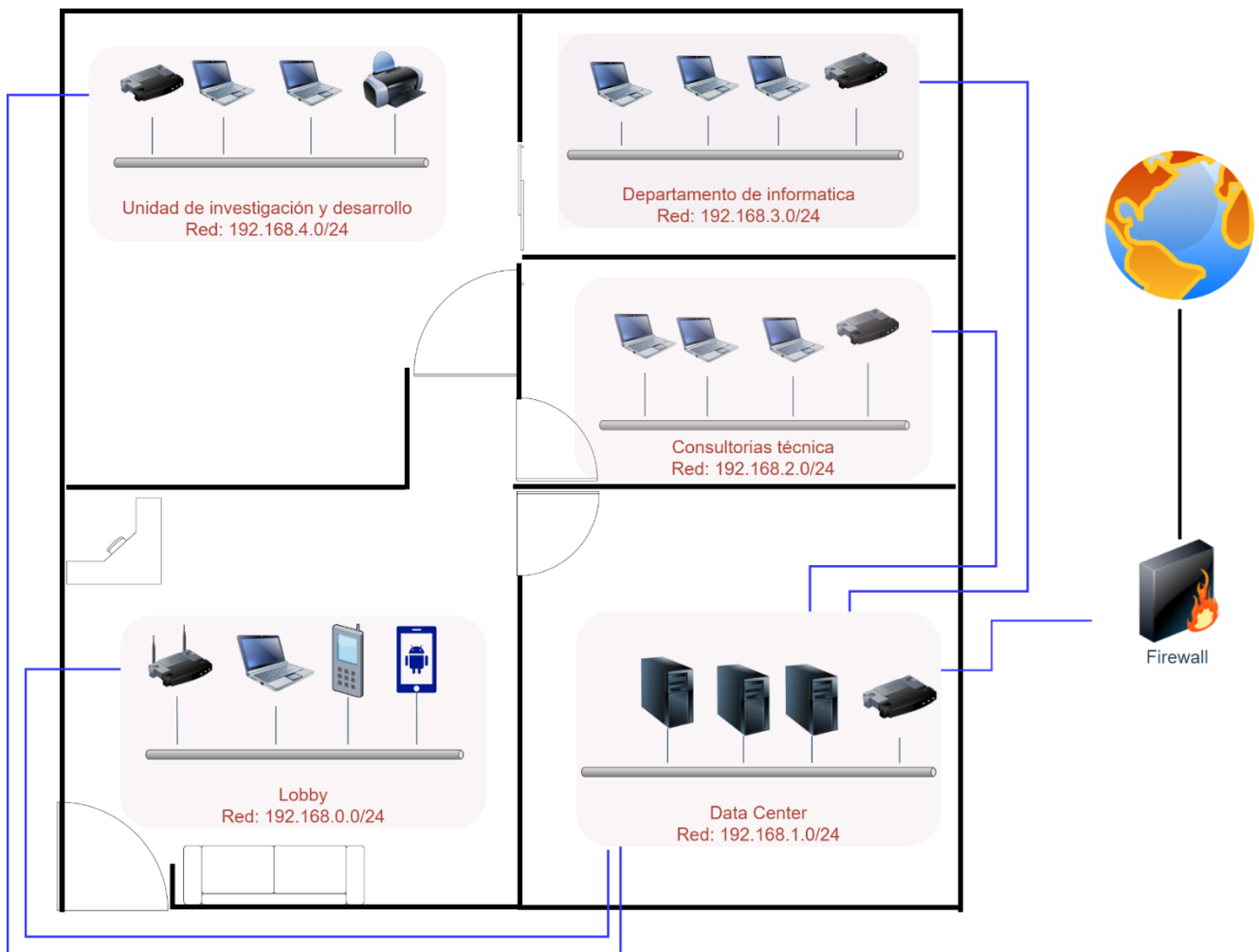


Ilustración 11 Diagrama de red actual

Fuente: Departamento de informática elaborado con la herramienta web <https://app.diagrams.net/>

## E.7. Diagrama de red con solución propuesta

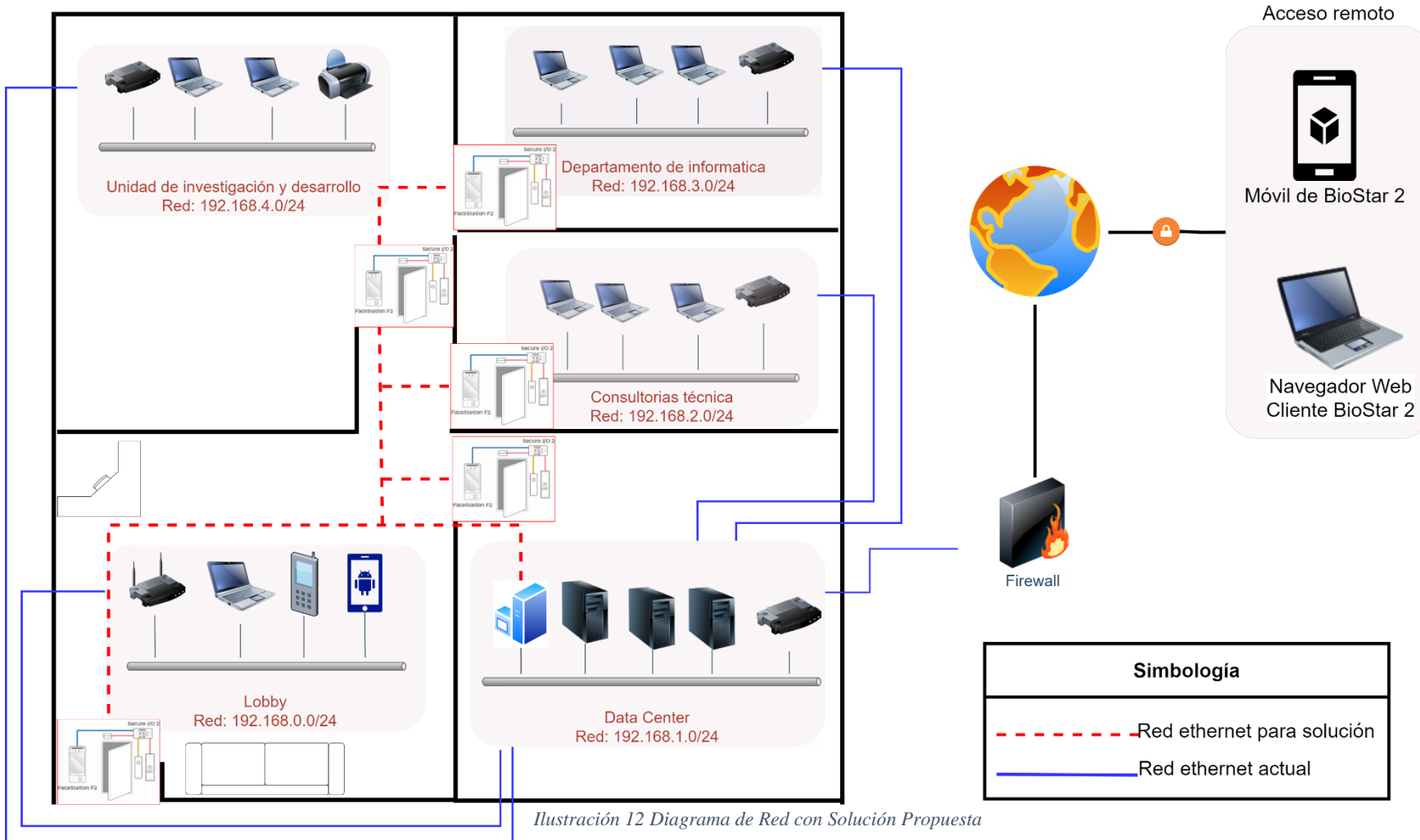


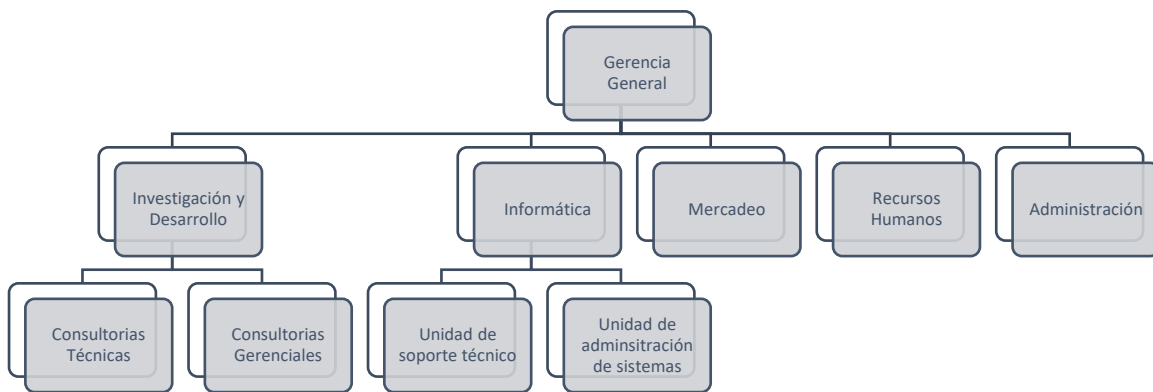
Ilustración 12 Diagrama de Red con Solución Propuesta

Fuente: Elaboración propia con base a diagrama de red proporcionado por departamento de informática utilizando la herramienta web <https://app.diagrams.net/>

## F. Factibilidad administrativa

### F.1. Organigrama propuesto

El organigrama propuesto no sufre modificaciones ya que el encargado de ejecutar y gestionar el proyecto es el departamento de informática, tampoco se planea crear nuevos puestos de trabajo derivado que las funciones de la gestión corresponden dentro de las responsabilidades de la unidad de administración de sistemas atendidas por el Especialista nivel I.



30

---

<sup>30</sup> Fuente: Recursos humanos, Elite solutions

## F.2. Manual de funciones

<b>I. identificación del puesto</b>	
<b>Ubicación administrativa:</b> Departamento de Informática	
<b>Puesto nominal:</b> Especialista nivel I	
<b>Puesto funcional:</b> Especialista para la gestión de los sistemas del departamento de informática	
<b>Inmediato superior:</b> Especialista nivel II	
<b>Subalternos:</b> Ninguno	

<b>II. Descripción del puesto</b>	
<b>1. Naturaleza</b>	
Verificación y análisis de los sistemas implementados dentro del departamento, velando por el buen funcionamiento de cada uno, así como también realizar mantenimientos nivel O y creación de informes de las actividades de manera semanal y mensual.	
<b>2. Atribuciones</b>	
2.1 Ordinarias	
<ul style="list-style-type: none"><li>• Mantenimiento al sistema operativo y base de datos</li><li>• Actualizaciones a dispositivos</li><li>• Elaboración de manuales de uso</li><li>• Enrolamiento de nuevo personal</li></ul>	
2.2 Periódicas	
<ul style="list-style-type: none"><li>• Mantenimiento preventivo a los dispositivos</li><li>• Monitoreo del estado del servicio y servidor de alojamiento</li><li>• Elaboración de reportes de los eventos ordinarios y extraordinarios</li></ul>	

31

<sup>31</sup> Fuente: Recursos humanos, Elite solutions

### F.3. Factibilidad operativa

#### F.3.1 Diagrama de Gantt. Implementación

N°	Actividad	Ant.	Semanas														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
<b>Fase I - Propuesta</b>																	
1	Presentación de propuesta	0	x														
2	Aprobación de proyecto	0	x														
<b>Fase II - Cotización</b>																	
3	Biométricos	2		x	x												
4	Cable de red	2			x												
5	Conectores RJ45 cat 6	2			x												
6	Software	2		x	x												
<b>Fase III - Compra de equipo</b>																	
7	Adquisición de equipo tecnológico	2				x	x	x	x								
8	Adquisición de accesorios técnicos	2				x	x	x	x								
<b>Fase IV - Instalación de equipo</b>																	
9	Instalación de cableado de red	8							x	x							
10	Instalación de biométricos	7									x						
<b>Fase V - Configuración</b>																	
11	Configuración de servidor virtual.	10										x					
12	Configuración de software de biométricos.	10											x	x			
<b>Fase VI - Pruebas</b>																	
13	Periodo de prueba de sistemas de biométricos	12														x	
<b>Fase VII - Entrega de proyecto</b>																	
14	Entrega de Proyecto Finalizado	13														x	

Fuente: Elaboración propia

#### F.3.2 Diagrama de Gantt. Capacitación

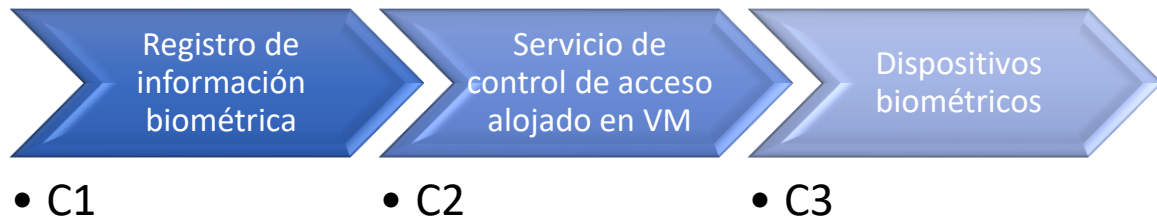
N°	Actividad	Ant.	Horas								
			H1	H2	H3	H4	H5	H6	H7	H8	
1	Presentación general		x								
2	Capacitación personal técnico	1		x	x	x	x				
3	Capacitación personal administrativo	1							x	x	
4	Finalización de capacitación	2,3									x

Fuente: Elaboración propia



## F.4. Planes de contingencia

### F.4.1 Análisis de riesgos y establecimiento de controles



Puntos de Control		
Control	Tipo	Descripción
C1	Detectivo	Verificación de las fichas del personal registrado contrastando con los datos de recursos humanos
C2	Preventivo	Realizar monitoreo del software de virtualización donde este alojado el servidor virtual que provee el servicio del sistema de control.
C3	Detectivo	Verificar dentro del sistema de gestión el estado y buen funcionamiento de los biométricos

Fuente: Elaboración propia

Tabla de análisis de contingencia				
Paso	Descripción	Contingencia	Solución	Tipo
P1	Usuario con denegación de acceso a oficinas	Usuario con permisos limitados	Verificación con el administrador del sistema los permisos registrados al usuario	Inspección
P2	Acceso al sistema de control de acceso no disponible	Problemas de red que impidan poder acceder al servicio	Comprobar estado de la red con soporte técnico y a su vez el estado del servidor virtual, el cual cuenta con una copia de seguridad que permite restablecer el servicio.	Inspección
P3	Dispositivo con desperfectos de funcionamiento	Conexiones del dispositivo dañadas o colocadas de manera incorrecta	Reportar a soporte técnico la revisión de conexiones y estado del dispositivo, en caso de que lo amerite se procede a realizar el reclamo de garantía.	Inspección

Fuente: Elaboración propia

Tabla de llamadas				
P#	A quién	Puesto	Teléfono	Correo
1	Técnico en servicio	Especialista nivel I	9999-9999	nivel1@empresa.com
2	Supervisor de técnicos	Especialista nivel II	8888-8888	nivel2@empresa.com

Fuente: Elaboración propia

## F.5. Análisis de factibilidad legal

- La constitución de 1985 incorporó la protección de datos personales informatizados, así mismo recoge el derecho de acceso, unido a los de rectificación o cancelación en su artículo 31. Reforma de 1993.<sup>32</sup>
- De acuerdo con el Artículo 4 de la Ley de Derecho de Autor y Derechos Conexos, el Decreto 33-98 del Congreso de la República de Guatemala (la "Ley de Derecho de Autor), el software o programa de ordenador es: "La obra constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma, que, al ser incorporadas a un soporte legible por máquina, es capaz de hacer que un ordenador ejecute determinada tarea u obtenga determinado resultado". Por lo tanto, se puede inferir que la Ley considera el software como una obra protegida por los derechos de autor, la cual de conformidad con el artículo 44 de la Ley de Derecho de Autor está protegida por 75 años desde su primera publicación o desde la realización de la obra.<sup>33</sup>

Las leyes actuales referente al proyecto de la implementación de control y monitoreo de accesos a las instalaciones de la empresa Elite hace constar que, haciendo el buen uso de los registros del personal, así como también cumpliendo con los licenciamientos de software del fabricante se cumple con las leyes de la república de Guatemala.

---

<sup>32</sup> <https://www.cijc.org/es/NuestrasConstituciones/GUATEMALA-Constitucion.pdf>

<sup>33</sup> <https://www.lexology.com/library/detail.aspx?g=ef17b55a-36f8-4998-be12-b1a010d1fdec#:~:text=Protecci%C3%B3n%20de%20derecho%20de%20autor%3A&text=Por%20lo%20tanto%2C%20se%20puede,la%20realizaci%C3%B3n%20de%20la%20obra.>

## **F.6. Análisis de factibilidad ambiental**

La producción anual de tarjetas RFID requiere una masa de plástico que es equivalente a 900 sillas familiares, las tarjetas, los cordones y los porta tarjetas son difíciles de reciclar y la mayoría termina en vertederos de basura o en los océanos.<sup>34</sup>

La nueva tecnología biométrica y de reconocimiento facial como credenciales de acceso permite remover completamente el costo en tarjetas RFID generando un impacto laboral y ambiental de la emisión que se genera en la fabricación de estas por lo tanto se concluye que el proyecto es factible

---

<sup>34</sup> [https://www.supremainc.com/en/hardware/new-door-access-experience-biostation3.asp?iHARDWARE\\_NO=268&iPage=1&iCTG\\_No=&sOPT\\_CRDENTIAL\\_CD=&sOPT\\_BASIC\\_CD=&sOPT\\_SPECTIAL\\_CD=&iPageSize=20#bookmark](https://www.supremainc.com/en/hardware/new-door-access-experience-biostation3.asp?iHARDWARE_NO=268&iPage=1&iCTG_No=&sOPT_CRDENTIAL_CD=&sOPT_BASIC_CD=&sOPT_SPECTIAL_CD=&iPageSize=20#bookmark)

## F.7. Factibilidad financiera

### Costos

Cantidad	Descripción	Valor unitario	Valor total
5	Lector biométrico con reconocimiento facial y RFID	Q 3,052.21	Q 15,261.07
5	Cables de poder	Q 678.77	Q 3,393.83
1	Licencia de software	Q 1,956.55	Q 1,956.55
5	Botón de apertura para puerta	Q 149.72	Q 748.58
5	Capa electromagnética para cierre de puerta	Q 439.21	Q 2,196.03
5	Kit de fuentes de poder	Q 559.02	Q 2,795.12
1	materiales	Q 2,495.62	Q 2,495.62
1	instalación	Q 4,695.71	Q 4,695.71
Inversión total implementación de proyecto			Q 33,542.50 <sup>35</sup>

Fuente: Elaboración propia en base a cotización número 16112022 empresa G4S

Descripción	Periodicidad	Unidad de medida individual mensual	Unidad de medida total	Valor promedio	Total
Consumo eléctrico por equipos biométricos	Anual	259.2 KW	1296 KW	Q 1.346 kWh <sup>36</sup>	Q 1,744.50
Mantenimiento de equipos	Anual	375 mantenimiento trimestral	1875	1	Q 1,875.00
Inversión total anual					Q 3,619.50

Fuente: Elaboración propia

<sup>35</sup> Tipo de cambio al 25 de noviembre del 2022 [https://www.banguat.gob.gt/tipo\\_cambio/](https://www.banguat.gob.gt/tipo_cambio/)

<sup>36</sup> <https://www.energuate.com/cuanto-cuesta-la-luz>

## Beneficio

Descripción	Periodicidad	Unidad de medida Individual	Valor promedio unitario	Total
Guardia de seguridad para control de acceso a instalaciones	Mensual	1 agente de seguridad	Q 4500 <sup>37</sup>	Q 4,500.00
Mejoramiento para la generación de informes de asistencia de personal por parte de recursos humanos <sup>38</sup>	Mensual	10 horas	Q 50 / hora <sup>39</sup>	Q 500.00
Inversión total mensual				Q 5,000.00

## Matriz costo – beneficio

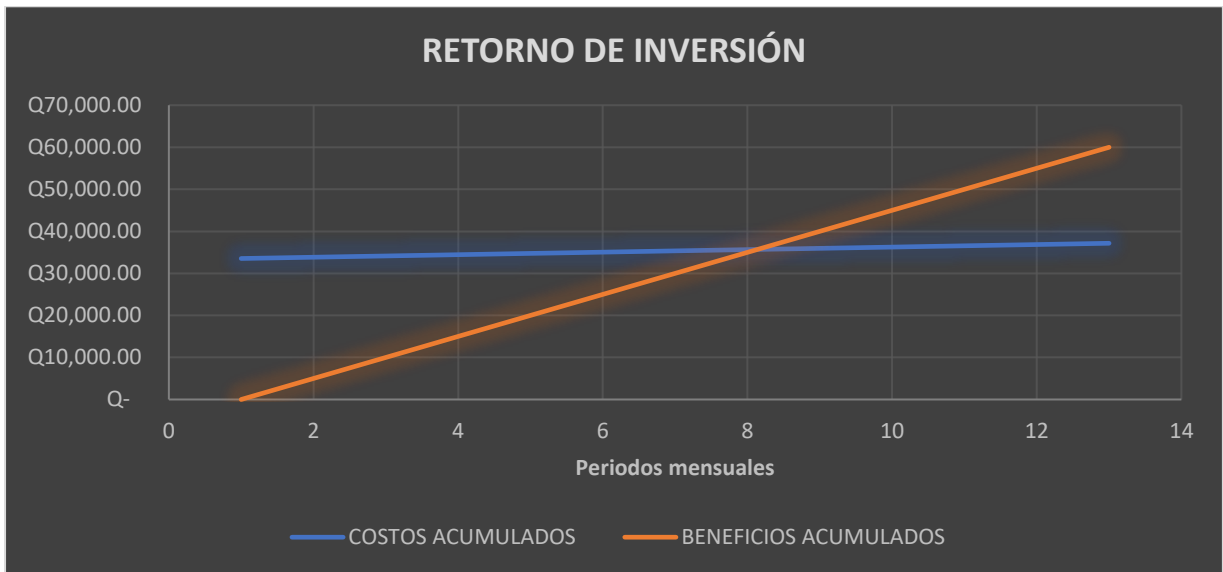
PERIODO	COSTO	COSTOS ACUMULADOS	BENEFICIO	BENEFICIOS ACUMULADOS	UTILIDAD (BA-CA)
Mes 0	Q 33,542.50	Q 33,542.50	Q -	Q -	-Q 33,542.50
Mes 1	Q 301.625	Q 33,844.13	Q 5,000.00	Q 5,000.00	(28,542.50)
Mes 2	Q 301.625	Q 34,145.75	Q 5,000.00	Q 10,000.00	(23,542.50)
Mes 3	Q 301.625	Q 34,447.38	Q 5,000.00	Q 15,000.00	(18,542.50)
Mes 4	Q 301.625	Q 34,749.00	Q 5,000.00	Q 20,000.00	(13,542.50)
Mes 5	Q 301.625	Q 35,050.63	Q 5,000.00	Q 25,000.00	(8,542.50)
Mes 6	Q 301.625	Q 35,352.25	Q 5,000.00	Q 30,000.00	(3,542.50)
Mes 7	Q 301.625	Q 35,653.88	Q 5,000.00	Q 35,000.00	1,457.50
Mes 8	Q 301.625	Q 35,955.50	Q 5,000.00	Q 40,000.00	6,457.50
Mes 9	Q 301.625	Q 36,257.13	Q 5,000.00	Q 45,000.00	11,457.50
Mes 10	Q 301.625	Q 36,558.75	Q 5,000.00	Q 50,000.00	16,457.50
Mes 11	Q 301.625	Q 36,860.38	Q 5,000.00	Q 55,000.00	21,457.50
Mes 12	Q 301.625	Q 37,162.00	Q 5,000.00	Q 60,000.00	26,457.50

<sup>37</sup> Salario mensual fuente RRHH empresa Elite

<sup>38</sup> Tiempos de entrega consultados al departamento de RRHH empresa Elite

<sup>39</sup> Salario por hora personal de recursos humanos fuente RRHH empresa Elite

**Punto de equilibrio**



Fuente: Elaboración propia  
**Mes de equilibrio:** periodo 8

**Movimiento de fondos**

Ingresos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	0	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00

Gastos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	33,542.50	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625

Movimiento de fondos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	-33,542.50	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38	4,698.38

<b>Tasa rentabilidad</b>	12%
<b>VAN</b>	Q519.17
<b>TIR</b>	12%
<b>Periodo de recuperación</b>	17



## Conclusiones

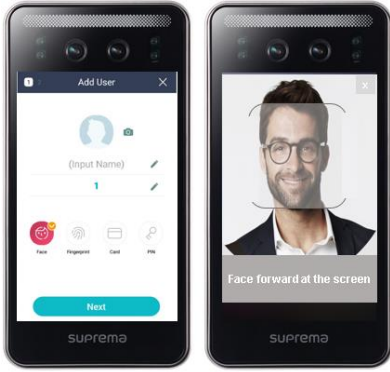

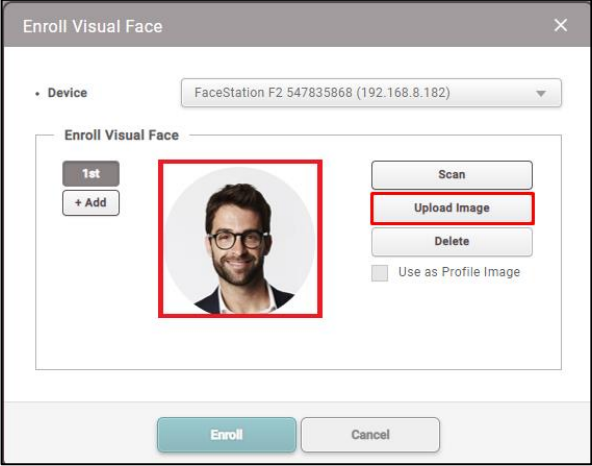
- De acuerdo con los resultados obtenidos por la encuesta más del 70% de los encuestados de la empresa Elite Solutions concuerdan en que no se tiene un sistema de monitoreo, registro de visitas o un protocolo que permita autorizar o denegar el ingreso de visitas o personal ajeno a una oficina.
- La mayor parte de los encuestados desconoce o indica que no existen medidas que restrinjan accesos o el uso de dispositivos electrónicos o de almacenamiento en las áreas de trabajo.
- Demostrando que los pocos controles existentes son inutilizados, el uso de protocolos de seguridad física y compartimentación de la información permitirá proyectar una mejor imagen ante colaboradores y visitas, además de que favorece reducir los riesgos de seguridad que conlleva un libre acceso por las instalaciones.
- En consecuencia de la implementación del proyecto permitirá reducir los costos que conlleva la contratación mensual de personal externo que se encargue de velar por la seguridad de las instalaciones de la empresa.
- Por lo tanto, los sistemas de la solución permiten generar bitácoras que permitan controlar internamente el flujo de personal y además proporciona reportes de las entradas por parte de los empleados a cada área y de las visitas a las instalaciones.
- Lo cierto es que la implementación del proyecto proporciona diversas herramientas que permiten autenticar, validar identidades, auditar y generar reportes que ayudan a obtener información de

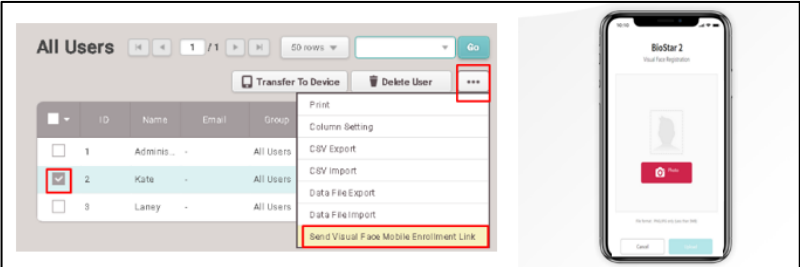
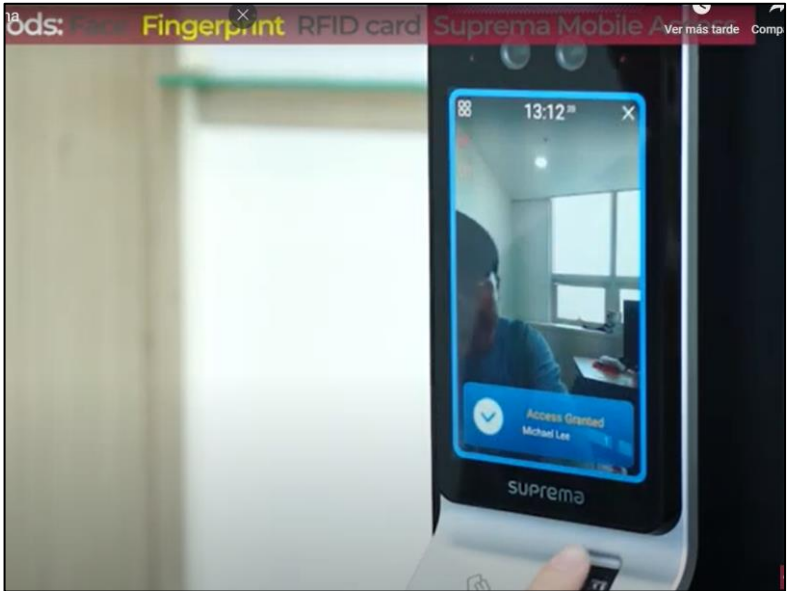
## Recomendaciones

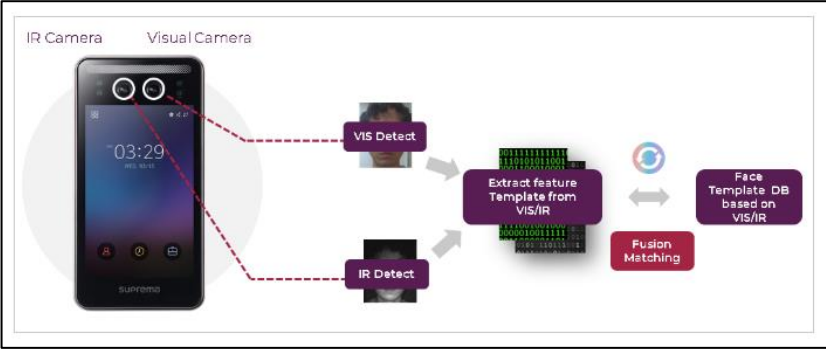
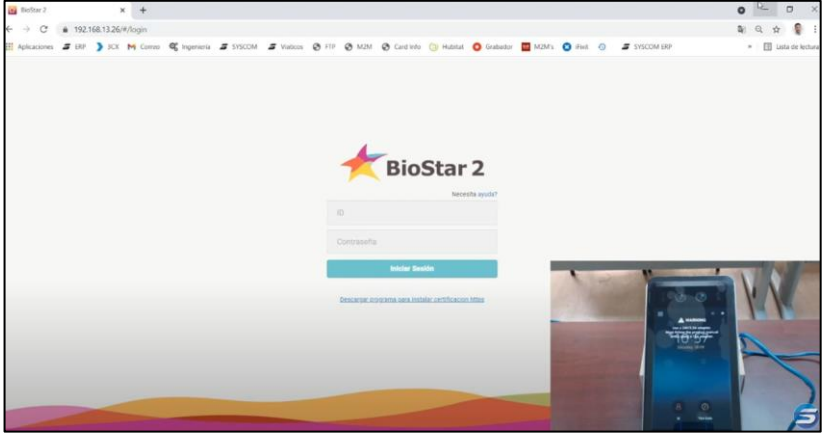
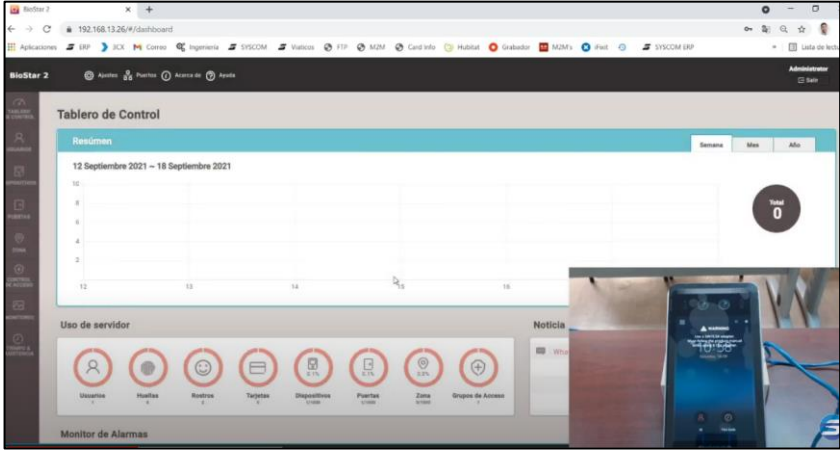
- La implementación del proyecto de control y monitoreo de accesos a las instalaciones de la empresa Elite es un sistema que permitirá proteger la compartimentación de información, además de reducción costos por contrataciones externas y una mejora significativa en tiempo y esfuerzo para la generación de informes de asistencia de personal por lo que es factible su ejecución.
- Fomentar una cultura de correcto uso y cuidado de los insumos de la empresa, esto para prevenir daños a los equipos de la solución implementada, así como hacer conciencia de los protocolos de seguridad a implementar para que sean percibidos como una herramienta tecnológica de ayuda a la empresa y no como una herramienta de control invasivo a los empleados.
- Realizar evaluaciones y mantenimientos periódicos de los equipos de la solución, previniendo posibles daños o errores que pueden ser gestionados a tiempo.
- Implementar respaldos de la base de datos automatizados y almacenarlos en una unidad con resguardo seguro a prueba de fallos en caso de que un disco duro o varios del almacenamiento pueda afectar por completo toda la información.
- Realizar auditorías que permitan validar la información obtenida y procesada con el objetivo de velar por el buen uso del sistema.

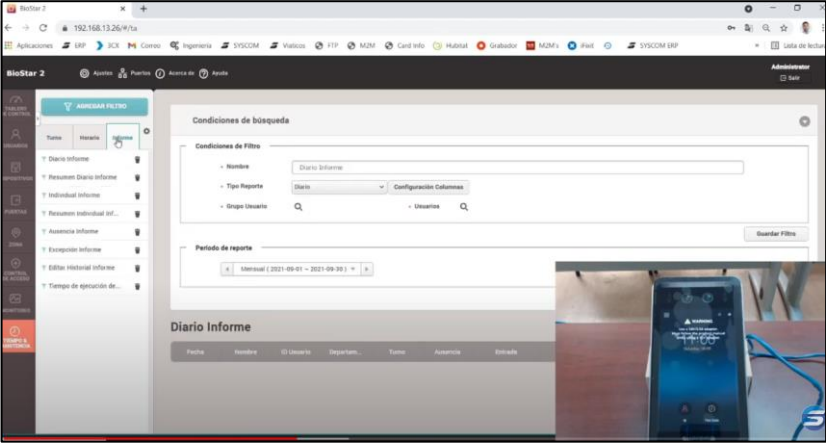
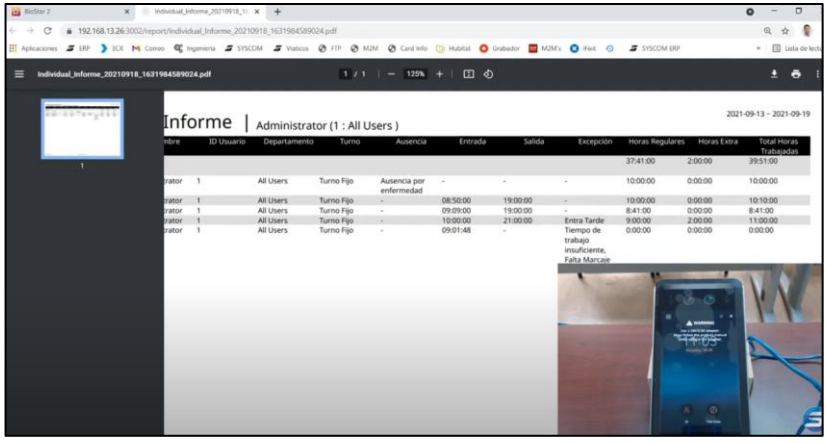
# Anexo

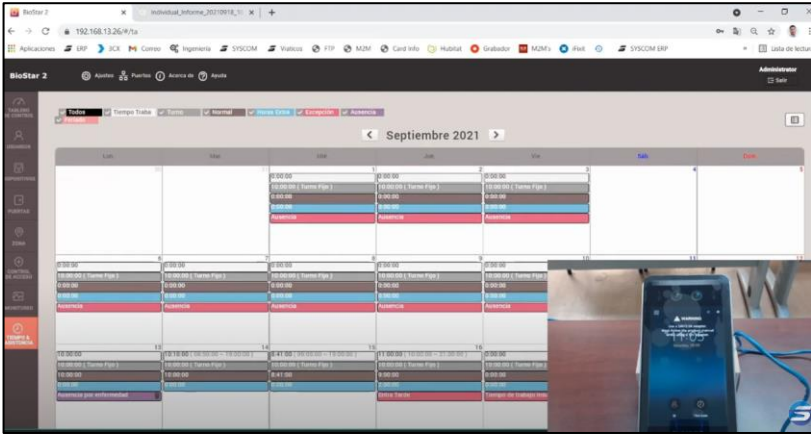
## Manual de uso

Paso	Descripción	Referencia
1	Enrolamiento de empleados	
2	Registro de datos del empleado	
3	Ingreso de fotografía del empleado	

Paso	Descripción	Referencia
4	Enrolamiento adicional con teléfono móvil	
5	Enrolamiento de huella	
6	Registro de usuario exitoso y es almacenado en la base de datos	

Paso	Descripción	Referencia
7	Usuarios utilizan el sistema para acceso a las oficinas	
8	Ingreso a sistema para monitoreo	
9	Verificación del tablero de controles de acceso del personal	

Paso	Descripción	Referencia																																																																		
10	Búsquedas personalizadas dentro del panel	 <p>The screenshot shows the BioStar 2 web application interface. On the left is a navigation menu with options like 'Inicio', 'Reportes', 'Usuarios', 'Turnos', 'Asistencia', and 'Excepciones'. The main area is titled 'Condiciones de búsqueda' (Search Conditions) and includes a search bar for 'Nombre' (Name) with 'Diario Informe' entered. Below the search bar are filters for 'Tipo Reporte' (Report Type) set to 'Diario' and 'Grupo Usuario' (User Group). A 'Período de reporte' (Report Period) is set to 'Meses (2021-09-01 - 2021-09-30)'. At the bottom, there is a 'Diario Informe' section with a table header: 'Fecha', 'Nombre', 'ID Usuario', 'Reporte...', 'Turno', 'Asistencia', and 'Entrada'.</p>																																																																		
11	Generación de informes	 <p>The screenshot shows a PDF report titled 'Informe   Administrator (1 : All Users)' for the period '2021-09-13 - 2021-09-19'. The report contains a table with the following columns: 'Nombre', 'ID Usuario', 'Departamento', 'Turno', 'Ausencia', 'Entrada', 'Salida', 'Excepción', 'Horas Regulares', 'Horas Extra', and 'Total Horas Trabajadas'. The data rows show attendance records for 'Administrator' with various statuses like 'Ausencia por enfermedad' and 'Entrada Tardía'.</p> <table border="1"> <thead> <tr> <th>Nombre</th> <th>ID Usuario</th> <th>Departamento</th> <th>Turno</th> <th>Ausencia</th> <th>Entrada</th> <th>Salida</th> <th>Excepción</th> <th>Horas Regulares</th> <th>Horas Extra</th> <th>Total Horas Trabajadas</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td>1</td> <td>All Users</td> <td>Turno Fijo</td> <td>Ausencia por enfermedad</td> <td>-</td> <td>-</td> <td>-</td> <td>37:41:00</td> <td>2:00:00</td> <td>39:41:00</td> </tr> <tr> <td>Administrator</td> <td>1</td> <td>All Users</td> <td>Turno Fijo</td> <td>-</td> <td>08:50:00</td> <td>18:00:00</td> <td>-</td> <td>10:00:00</td> <td>0:00:00</td> <td>10:10:00</td> </tr> <tr> <td>Administrator</td> <td>1</td> <td>All Users</td> <td>Turno Fijo</td> <td>-</td> <td>09:09:00</td> <td>19:00:00</td> <td>-</td> <td>8:41:00</td> <td>0:00:00</td> <td>8:41:00</td> </tr> <tr> <td>Administrator</td> <td>1</td> <td>All Users</td> <td>Turno Fijo</td> <td>-</td> <td>10:00:00</td> <td>21:00:00</td> <td>-</td> <td>11:00:00</td> <td>0:00:00</td> <td>11:00:00</td> </tr> <tr> <td>Administrator</td> <td>1</td> <td>All Users</td> <td>Turno Fijo</td> <td>-</td> <td>09:01:48</td> <td>-</td> <td>Insuficiente, Faltas Marzaje</td> <td>0:00:00</td> <td>0:00:00</td> <td>0:00:00</td> </tr> </tbody> </table>	Nombre	ID Usuario	Departamento	Turno	Ausencia	Entrada	Salida	Excepción	Horas Regulares	Horas Extra	Total Horas Trabajadas	Administrator	1	All Users	Turno Fijo	Ausencia por enfermedad	-	-	-	37:41:00	2:00:00	39:41:00	Administrator	1	All Users	Turno Fijo	-	08:50:00	18:00:00	-	10:00:00	0:00:00	10:10:00	Administrator	1	All Users	Turno Fijo	-	09:09:00	19:00:00	-	8:41:00	0:00:00	8:41:00	Administrator	1	All Users	Turno Fijo	-	10:00:00	21:00:00	-	11:00:00	0:00:00	11:00:00	Administrator	1	All Users	Turno Fijo	-	09:01:48	-	Insuficiente, Faltas Marzaje	0:00:00	0:00:00	0:00:00
Nombre	ID Usuario	Departamento	Turno	Ausencia	Entrada	Salida	Excepción	Horas Regulares	Horas Extra	Total Horas Trabajadas																																																										
Administrator	1	All Users	Turno Fijo	Ausencia por enfermedad	-	-	-	37:41:00	2:00:00	39:41:00																																																										
Administrator	1	All Users	Turno Fijo	-	08:50:00	18:00:00	-	10:00:00	0:00:00	10:10:00																																																										
Administrator	1	All Users	Turno Fijo	-	09:09:00	19:00:00	-	8:41:00	0:00:00	8:41:00																																																										
Administrator	1	All Users	Turno Fijo	-	10:00:00	21:00:00	-	11:00:00	0:00:00	11:00:00																																																										
Administrator	1	All Users	Turno Fijo	-	09:01:48	-	Insuficiente, Faltas Marzaje	0:00:00	0:00:00	0:00:00																																																										

Paso	Descripción	Referencia
12	Generación de informe por mes	

4041

<sup>40</sup> <https://www.youtube.com/watch?v=SrPuNovUB-U>

<sup>41</sup> <https://support.supremainc.com/en/support/solutions/articles/24000060469--biostar-2-new-product-introduction-facestation-f2>

# Cotización



Wackenhut Electrónica, S.A.  
 AVENIDA PETAPA 42-51 ZONA 12, GUATEMALA, GUATEMALA  
 PBX: (502) 2328-7600 FAX: (502) 2328-7601  
 EMAIL: electronica@wacktron.com

## G4S SYSTEMS

<b>COTIZACIÓN</b>	<b>16112022</b>
NUMERO:	16112022
REVISIÓN:	1
FECHA:	11/16/2022
IMPRESIÓN:	16/11/2022 10:52 a. m.

Cliente		Contacto G4S	
Razón Social		Puesto	Ingeniero Comercial
Dirección		Celular	
Atención		Tasa de Cambio	\$ 7.90
Puesto		Segmento	VIP
Forma de Pago	CONTRA FACTURA 100%		

### DESCRIPCIÓN DEL PROYECTO CONTROL DE INGRESO BIOMETRICO FACIAL

CANTIDAD	CÓDIGO	PRODUCTOS	DESCRIPCIÓN	PRECIO UNITARIO	TOTAL
		CONTROL DE ACCESO			
5	BS3DB	BIO STATION 3 Lector Facial Multitecnologias uso con BIOSTAR2 / SOPORTA RFID(125KHZ EM & 13.56MHZ MIFARE		\$390.00	\$1,950.00
5	PWR	POWER ADAPTER FOR BS3		\$86.73	\$433.67
1	BioStar2	BioStar 2 Standard Edition with S/W License		\$250.00	\$250.00
5	No/Touch	Boton de apertura para puerata No Touch		\$19.13	\$95.66
5	Mag	Capa electromagnetica para cierre de puerta		\$56.12	\$280.61
5	Pwr KIT	Kit de fuente de poder de 1.5 Amp para cierre magnetico.		\$71.43	\$357.14
1	Material	Incluye materiales de sujecion y materiales emergentes, no incluye cableados mayores a 3 metros.		\$318.88	\$318.88
1	Mano de obra	Incluye mano de obra calificada y certificada para los trabajos necesarios de instalacion y configuracion de equipos horarios en horarios habiles.		\$600.00	\$600.00
<b>Nota: Pendiente de evaluacion para materiales necesarios en instalacion fisica.</b>				Total +IVA	\$4,285.93

### CONDICIONES GENERALES DE NEGOCIACIÓN

**PRECIOS:** Cotizador en dólares americanos e incluyen impuestos locales e internacionales, validez 15 días.

**FACTURACIÓN:** En Dolares o Quetzales a la TASA DE CAMBIO del día de la facturación

**FORMA DE PAGO: CONTRA FACTURA 100%**

**NO INCLUYE:** Obra civil, trabajos de albañilería, carpintería, herrería o instalaciones eléctricas, únicamente los trabajos necesarios para la instalación, programación de los equipos cotizados, a menos que lo incluya esta propuesta.

**MATERIALES DE INSTALACIÓN:** No incluye MATERIALES DE INSTALACIÓN a menos que se encuentre descrito en las condiciones de la NEGOCIACIÓN.

**TIEMPO DE ENTREGA:** El tiempo de entrega será determinado por cronograma enviado despues de recibida la orden de compra por parte del cliente.

**GARANTÍA DE INSTALACIÓN:** No cubre daños por mal uso o negligencia por personas ajenas a WACKENHUT ELECTRÓNICA, S.A., Daños causados por fenómenos naturales o cualquier otra causa no directamente imputable a G4S.

**GARANTÍA DE EQUIPO:** Toda garantía por defecto de fabrica tiene la duracion de 3 años, el tiempo de reposicion dependera del defecto que presente y sera repuesto despues de realizar las pruebas pertinentes

**SERVICIO TÉCNICO:** Toda solicitud tecnica debere de llevar por escrito en un correo electronico al encargado del area, esta sera programada según disponibilidad o sera despachado en caso de emergencia con un cobro reflejado en boleta

**ENTREGA DE EQUIPO:** Todo el equipo descrito en la cotización sera entregado entre 40 dias despues de recibida la orden de compra.

**CHEQUE A NOMBRE DE:** Wackenhut Electrónica, S.A.

EDGAR PEREZ MARQUEZ  
 Asesor Comercial  
 WACKENHUT ELECTRONICA, S.A.

Armando Gonzalez  
 Gerente General  
 WACKENHUT ELECTRONICA, S.A.

\_\_\_\_\_  
 FIRMA DE ACEPTACIÓN  
 CLIENTE



## Movimiento de fondos optimista

Ingresos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	0	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00	5,500.00

Gastos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	33,542.50	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625

Movimiento de fondos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	-33,542.50	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38	5,198.38

<b>Tasa rentabilidad</b>	12%
<b>VAN</b>	Q4,144.00
<b>TIR</b>	14%
<b>Periodo de recuperación</b>	17

## Movimiento de fondos pesimista

Ingresos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	0	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00	4,500.00

Gastos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	33,542.50	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625	301.625

Movimiento de fondos	Periodo 0	Periodo 1	Periodo 2	Periodo 3	Periodo 4	Periodo 5	Periodo 6	Periodo 7	Periodo 8	Periodo 9	Periodo 10	Periodo 11	Periodo 12	Periodo 13	Periodo 14	Periodo 15	Periodo 16	Periodo 17	Periodo 18
	-33,542.50	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38	4,198.38

<b>Tasa rentabilidad</b>	12%
<b>VAN</b>	-Q3,105.67
<b>TIR</b>	10%
<b>Periodo de recuperación</b>	17

## Glosario

**Antivirus:** programas cuyo objetivo es detectar y eliminar virus informáticos

**Biométrico:** dispositivo electrónico de huella que realiza un análisis de los puntos distintivos (minucias) de las huellas para verificar o identificar una persona a través de su dedo.

**Enrolamiento:** momento en que se toma la muestra digital de la huella o rostro de una persona.

**End point disk encryption:** encriptación de datos para resguardo de la información.

**Firewall:** dispositivo de seguridad informática utilizado para el control del tráfico de la red.

**Protocolo:** conjunto formal de estándares y normas. Estos rigen tanto el formato como el control de la interacción entre los distintos dispositivos dentro de una red o sistema de comunicación.

**Servidor proxy:** es un servidor (programa o dispositivo), que hace de controlador intermediario en las peticiones de recursos que realiza un cliente hacia internet.

**Software:** programas de aplicación que permiten que la computadora o cualquier dispositivo electrónico inteligente pueda desempeñar tareas, dirigiendo a los componentes físicos o hardware con instrucciones y datos solicitados por el usuario.

**RFID:** identificación por radiofrecuencia (del inglés Radio Frequency Identification) es un sistema de almacenamiento y recuperación de datos remotos utilizado en biometría para la identificación sin contacto en controles de acceso.

**VPN:** red privada virtual es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet

## G. E-grafía

*AI Facial Recognition with Body Temperature Detection Access Control and Time Attendance Terminal* | Anviz Global. (2021, 29 octubre). Recuperado 21 de octubre de 2022, de <https://www.anviz.com/es/facepass7pro-smart-face-recognition-terminal.html>

*Bienvenido a Banco de Guatemala* | Banco de Guatemala. (s. f.). Recuperado 21 de octubre de 2022, de <https://www.banguat.gob.gt/>

*Cámaras de seguridad Guatemala*. (s. f.). <https://camarasdeseguridad.com.gt/>

*Chipcom - Chipcom*. (s. f.). Recuperado 4 de noviembre de 2022, de <https://chipcom.com.gt/>

*Constitución de Guatemala*. (s. f.). Congreso de la república de Guatemala. <https://www.cijc.org/es/NuestrasConstituciones/GUATEMALA-Constitucion.pdf>

DUALi. (s.f.). *Reader & Terminal - Desktop reader*. Obtenido de <http://www.duali.com/en/product/reader/desktop-reader/de-620--de-620r/>

Guide, B. 2. (s.f.). *Installing BioStar 2*. Obtenido de The default values for the ports used by BioStar 2: [https://spm.biostar2.com/help/en/index.html?install\\_server.htm](https://spm.biostar2.com/help/en/index.html?install_server.htm)

Guide, B. 2. (s.f.). *Minimum System Requirements*. Obtenido de [https://spm.biostar2.com/help/en/index.html?install\\_systemrequirement.htm](https://spm.biostar2.com/help/en/index.html?install_systemrequirement.htm)

Guide, B. 2. (s.f.). *Network*. Obtenido de [https://spm.biostar2.com/help/en/device\\_edit\\_network.htm](https://spm.biostar2.com/help/en/device_edit_network.htm)

Guide, B. 2. (s.f.). *Security*. Obtenido de [https://spm.biostar2.com/help/en/index.html?settings\\_security.htm](https://spm.biostar2.com/help/en/index.html?settings_security.htm)

Hernández, I. (2019, 1 abril). *Aspectos básicos de la Protección de software en Guatemala*. Lexology. <https://www.lexology.com/library/detail.aspx?g=ef17b55a-36f8-4998-be12-b1a010d1fdec>

ID, S. (s.f.). *Lectores De Autenticación*. Obtenido de BioMini Plus 2: <https://www.supremainc.com/es/contents/detail.php?code=010104>

*Inalarm*. (s. f.). Recuperado 4 de noviembre de 2022, de <https://inalarm.gt/>

*Innovative Fingerprint & RFID Reader | Anviz Global*. (2017, 19 octubre). Recuperado 21 de octubre de 2022, de <https://www.anviz.com/es/product/t5s-access-control.html>

Microsoft. (s.f.). *Configuración de Firewall de Windows para permitir el acceso a SQL Server*. Obtenido de <https://learn.microsoft.com/es-es/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver16>

*Productos de control de acceso*. (s. f.). hiknow. Recuperado 4 de noviembre de 2022, de <https://www.hikvision.com/es-la/products/Access-Control-Products/>

*Suprema | Security & Biometrics*. (s. f.). Recuperado 4 de noviembre de 2022, de <https://www.supremainc.com/es/hardware/biometric-products.asp>

Suprema, S. t. (23 de Mayo de 2021). *Using DE-620 with Suprema Integration Options*.

Obtenido de

<https://support.supremainc.com/en/support/solutions/articles/24000068279--faqs-using-de-620-with-suprema-integration-options>

*Suprema | Security & Biometrics*. (s. f.-b). [https://www.supremainc.com/en/hardware/new-door-access-experience-biostation3.asp?iHARDWARE\\_NO=268](https://www.supremainc.com/en/hardware/new-door-access-experience-biostation3.asp?iHARDWARE_NO=268)

SYSCOM. (2021, 21 septiembre). *Suprema - Así Funciona - Generación de Reportes en Biostar2*. YouTube. <https://www.youtube.com/watch?v=SrPuNovUB-U>

Support, S. T. (s.f.). *Server and Device Port Usage*. Obtenido de

<https://support.supremainc.com/en/support/solutions/articles/24000005909--biostar-2-server-and-device-port-usage>

*Technical Support / Suprema.* (s. f.).  
<https://support.supremainc.com/en/support/solutions/articles/24000060469--biostar-2-new-product-introduction-facestation-f2>

*Tipo de Cambio - Banco de Guatemala.* (s. f.). [https://www.banguat.gob.gt/tipo\\_cambio/](https://www.banguat.gob.gt/tipo_cambio/)

*¿Cuánto cuesta la luz? | Energuate.* (s. f.). <https://www.energuate.com/cuanto-cuesta-la-luz>

*ZKTeco Latinoamérica - Soluciones Biométricas.* (2022, 17 agosto). ZKTeco Latinoamerica.  
<https://www.zktecolatinoamerica.com/>

## H. Bibliografía

Esau Cifuentes, Ing. R. (2019). *Seminario de Telecomunicaciones*.

Ing. Nidia Giorgis de Orozco, M. (2019). *Implementación y evaluación administrativa I*.

Serviprensa, S.A.

Orozco, D. N. (2020). *Automatización de procesos administrativos casos empresariales*.

Serviprensa, S.A.

Ovando, L. S. (2017). *Finanzas administrativas I*. Serviprensa, S.A.

Wathen, W. G. (2015). *Estadística aplicada a los negocios y la economía I*. C.P. 01376,

México, D.F.: McGraw-Hill Interamericana editores, S.A. de C.V.

**Carta de aprobación Proyecto de Seminario de Especialidad**

**Datos del Alumno (a):**

Nombre completo: MARCELINO ANTONIO FAJARDO SOSA

No. de Carné: IDE0812344

Nombre Proyecto: "Proyecto para la Implementación de Control y Monitoreo de Accesos a las Instalaciones de la Empresa Elite"

Observaciones:

Nota  Aprobado  Reprobado

**Coordinador Académico: Ing. Rodrigo Cifuentes MSc.**  
**Especialidad: ADMINISTRACIÓN DE LAS TELECOMUNICACIONES**

**Fecha: 12/01/2023**

**Firma:** \_\_\_\_\_



**Uso interno de Atención Alumnos y Evaluación:**

1.  Promedio mayor o igual a 70 Pts. acumulado.
2.  Proyecto integrado aprobado.
3.  Curso pendiente por aprobar. \_\_\_\_\_
4.  Seminario de Informática.
5. **Tener papelería completa según Artículo 38 según Reglamento Académico:**
  1.  Fotocopia completa y legible del documento OFICIAL DE IDENTIFICACIÓN DPI autenticado (La Auténtica deberá indicar número de CUI, nombre completo a quien pertenece).
  1.  Fotocopia de anverso y reverso del TÍTULO DE NIVEL MEDIO, deberá contar con los sellos correspondientes de la Contraloría General de Cuentas de la Nación y estar debidamente autenticada (Indicando nombre completo de quien pertenece y nombre del título que obtuvo).

Foto digital en el sistema.





Guatemala, 13 de enero de 2023

Señores:  
Universidad Galileo  
IDEA  
Presente.

Por este medio de la presente YO Marcelino Antonio Fajardo Sosa que me identifico con número de carné 0812344 y con DPI 1686648950108 actualmente asignado (a) en la carrera: Licenciatura en Tecnología y Administración de las Telecomunicaciones

**"Autorizo a Instituto de Educación Abierta (IDEA) a la publicación, en el Tesario virtual de la Universidad, de mi proyecto de Graduación titulado:"**

Proyecto para la Implementación de Control y Monitoreo de Accesos a las Instalaciones de la Empresa Elite

Como autor (a) del material de la investigación sustentada mediante el protocolo de IDEA.

Expreso que la misma es de mi autoría y con contenido inédito, realizado con el acompañamiento experto del coordinador de área y por tanto he seguido los parámetros éticos y legales respecto de las citas de referencia y todo tipo de fuentes establecidas en el Reglamento de la Universidad Galileo

Sin otro particular, me suscribo.

F. 