Resumen – Trabajo De Grado

Autores	Michel Mateo Vargas Diaz
Facultad	Ingenierías
Plan De Estudios	Ingeniería de sistemas
Director	Henrry Eliseo Navarro Chinchilla
Título De La Tesis	Diseño de un plan de seguridad Informática en la Alcaldía de la Jagua de Ibirico-Cesar
Título En Ingles	Design of a security plan IT in the Mayor's Office of Jagua de Ibirico-Cesar

RESUMEN
(70 Palabras)

El siguiente trabajo de grado modalidad pasantías corresponde al diseño de un plan de seguridad informática en la alcaldía de la jagua de ibirico, basada en la metodología magerit y la norma ISO: 27001 del 2013, la cual se trabajó mediante los esquemas de vulnerabilidad y diseño de un plan de implementación así tener una vista lógica a los problemas presentados en la alcaldía a la hora de ataques, riesgos y amenazas.

RESUMEN EN INGLES

The following degree work internship modality corresponds to the design of a computer security plan in the mayor's office of La Jagua de Ibirico, based on the magerit methodology and the ISO: 27001 standard of 2013, which was worked through vulnerability and design schemes of an implementation plan to have a logical view of the problems presented to the mayor's office when it comes to attacks, risks and threats.

Palabras Claves	Política de seguridad, Análisis de riesgos, Ciberseguridad, riesgos y amenazas
Palabras Claves En Ingles	Security policy, Risk analysis, Cybersecurity, risks and threats

Características

Páginas: 57	Planos:	Ilustraciones: 17	Cd-Rom:

Diseño un plan de seguridad informática en la Alcaldía de la Jagua de Ibirico-Cesar

Michel Mateo Vargas Diaz

Facultad de Ingenierías, Universidad Francisco de Paula Santander Ocaña

Ingeniería de Sistemas

MSc. Henrry Eliseo Navarro Chinchilla

Julio de 2023

Índice

Listas de figuras

Listas de tablas

1. Diseño un plan de seguridad informática en la Alcaldía de la Jagua de Ibirico-Cesar

1.1 Descripción de la Empresa.

La Alcaldía Municipal de la Jagua de Ibirico, es una entidad pública encargada de dirigir la acción administrativa del municipio, brindando a sus habitantes trámites y servicios oportunos, promoviendo el mejoramiento social y cultural, a través de programas dirigidos a la comunidad, gestionando los recursos de tal manera que se puedan solucionar las necesidades básicas de salud, educación, servicios públicos, recreación y vivienda. Cumpliendo y haciendo cumplir la Constitución Política, las leyes, decretos y acuerdos del Gobierno (Alcaldía la Jagua de Ibirico, 2022).

1.1.1 Misión

Potenciar y promover el desarrollo integral del Municipio, mediante una apuesta de intervención concertada con la comunidad, orientando el gasto social a superar los desequilibrios existentes en el territorio e impulsando la solidaridad, la equidad, la transparencia en la gestión pública, la garantía de los derechos humanos y la seguridad ciudadana como mecanismos para generar bienestar social; y el impulso a la diversificación de los diferentes sectores de la economía, que estimule la generación de empleo e incremente la capacidad productiva y competitiva; y la protección de los recursos naturales y del potencial ambiental, de manera que el territorio avance hacia un desarrollo sostenible.

1.1.2 Visión

En el 2030, La Jagua de Ibirico será un municipio integrado social y territorialmente, solidario y equitativo, con un capital humano con capacidades para su realización individual y colectiva, un desarrollo económico sostenible y competitivo y un ambiente seguro y sano, que

contribuyan a disminuir los niveles de pobreza y los desequilibrios, y a consolidar una sociedad reconciliada, respetuosa de los derechos humanos y viviendo en paz.

1.1.3 Objetivos de la empresa

Implementar estrategias para apoyar el emprendimiento en las industrias culturales: (i) identificar y desarrollar procesos de emprendimiento cultural, (ii) elaborar estrategias para la promoción de inversiones en las industrias culturales, (iii) apoyar técnica y financieramente a las empresas culturales de menor tamaño, y (iv) desarrollar programas de formación del sector artístico y cultural.

Diseñar e implementar programas culturales para la primera infancia: (i) desarrollar programas de sensibilización y formación artística, (ii) promover la infraestructura cultural con servicios para la primera infancia, (iii) proveer formación artística a los agentes cuidadores y educativos, entre otros.

Fortalecer el Programa de Lectura y Escritura: realizar un inventario del estado actual y la dotación de las bibliotecas públicas, incluyendo su conectividad; e implementar esquemas de cofinanciación territorial para la infraestructura cultural municipal, entre otras.

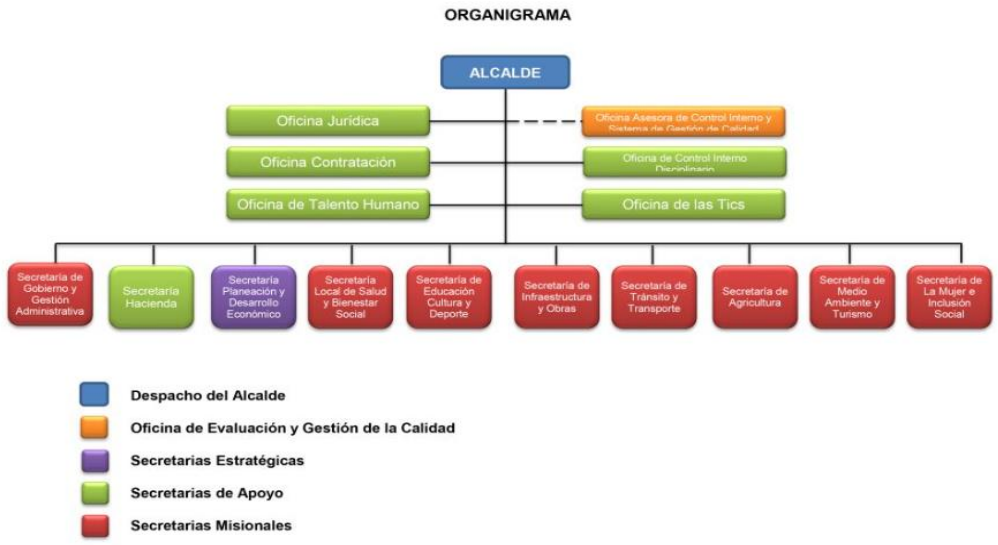
Desarrollar estrategias y programas para la búsqueda efectiva de empleo, el mejoramiento del perfil ocupacional y la orientación profesional: profundizar la interrelación y complementariedad entre el Sistema de Intermediación Laboral, los Sistemas de Protección al Cesante y de Formación de Capital Humano, y la Estrategia de Gestión del Recurso Humano.

Incorporar a las responsabilidades de las entidades del Gobierno Nacional el seguimiento del empleo que generen y la definición de las necesidades de recurso humano que requiera su respectivo sector.

Desarrollar estrategias de prevención para atacar las causas del fenómeno y disminuir los desplazamientos nuevos. (Alcaldía la Jagua de Ibirico, 2022)

1.1.4 Descripción de la estructura organizacional

Figura 1 Estructura organizacional de la empresa



Fuente. Sistema de información de la Alcaldía de la Jagua de Ibirico-Cesar

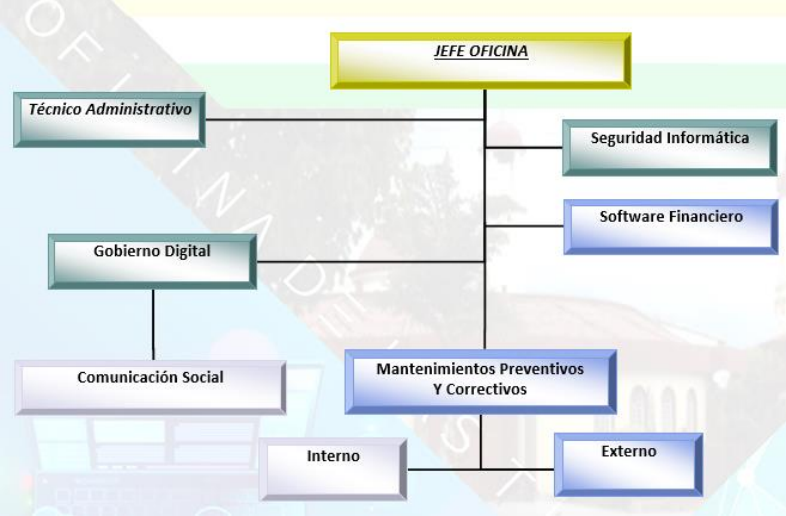
1.1.5 Descripción del área

La oficina de las Tic, es una dependencia de la Alcaldía de la Jagua de Ibirico que se encarga de realizar las acciones encaminadas a la generación de nuevos y mejores procesos de tecnología e innovación para el funcionamiento del Municipio, garantizando el soporte de la infraestructura y arquitectura Tic, atendiendo las normas y requerimientos de la alcaldía.

De igual manera, se encarga de recolectar, revisar, editar e informar a la comunidad de manera veraz, ágil y oportuna las acciones y gestión realizada por la Administración Municipal, garantizando el acceso a la información a través de los medios tecnológicos e informáticos y de

comunicación, mediante la formulación de políticas, planes, programas y proyectos, con el fin de contribuir en el acercamiento permanente de la Administración Municipal con los Ciudadanos.

Figura 2 Estructura de la oficina de las Tic



Fuente. Alcaldía de la Jagua de Ibirico, Cesar

1.2 Diagnóstico inicial del área asignada.

Tabla 1 Matriz DOFA (Debilidades- Oportunidades- Fortalezas- Amenazas)

Análisis DOFA Alcaldía de la Jagua de Ibirico	**OPORTUNIDADES**	**AMENAZAS**
	Oportunidades de colaboración con otras empresas y organizaciones para fortalecer la seguridad de la información. Oportunidades de formación y capacitación para el personal de seguridad informática.	Ataques externos cibernéticos y hackeos Malware y virus que intentan dañar o alterar la información existente. Fraude y robo de datos

	Proyectos del Gobierno para el fortalecimiento de la Tecnologías.	Rápida evolución tecnológica Corrupción
FORTALEZAS	**ESTRATEGIAS FO**	**ESTRATEGIAS FA**
Disposición de contraseñas y cifrado de datos Procesos de autenticación Firewall y protección contra virus y malware Conciencia sobre la importancia de mantener la información protegida.	Participar en las convocatorias del Gobierno en temas de formación en aspectos tecnológicos**.** Intercambiar experiencias con otras empresas, frente al manejo de la seguridad de la información. Presentar proyectos en los que se puedan adquirir recursos que fortalezcan las TIC en la alcaldía.	Mantener actualizados los mecanismos de protección de seguridad de la información (Firewall, antivirus, contraseñas seguras), para evitar ataques cibernéticos. Disponer de medidas drásticas contra funcionarios o personas que cometan algún tipo de fraude en la alcaldía.
DEBILIDADES	**ESTRATEGIAS DO**	**ESTRATEGIAS DA**
Personal de seguridad informática con poca	Capacitar constante en temas de seguridad informática.	Realizar campañas de concientización sobre la importancia de mantener

experiencia o sin la capacitación necesaria. Falta de inversión en tecnología de seguridad de última generación. Falta de políticas y procedimientos de seguridad óptimos. Inestabilidad de la conectividad de la red de datos.	Diseñar políticas acordes a lineamientos nacionales, que garanticen la seguridad de la información. Articular la alcaldía con las universidades para que mediante proyectos de grado se fortalezcan los aspectos de seguridad de la información y red de datos	las medidas de seguridad de la información Divulgar las consecuencias que acarrea cometer delitos informáticos contra la alcaldía.

1.2.1 Planteamiento del problema

En el municipio de la Jagua de Ibirico, Cesar, específicamente en la alcaldía del mismo, luego de entrevistas informales con el personal de la dirección de informática, utilizando un encuestador llamado Microsoft Security Assessment Tooll, encuestando a los funcionarios de la alcaldía, se pudo constatar que, aunque poseen algunas medidas de seguridad, éstas no son suficientes, ni robustas. Adicionalmente, se observó que mantienen sus políticas de seguridad de la información fuera de los estándares internacionales, tomando en cuenta que se procesa y se almacena un alto volumen de información, recursos de hardware y software, así como una gran cantidad de usuarios que acceden a la red, utilizando los servicios de internet y telefonía IP.

De igual manera, el personal no dispone de las competencias suficientes, teniendo en cuenta que la tecnología avanza rápidamente y surgen nuevos ataques, nuevas medidas de seguridad, con los que no se cuenta por falta de capacitación constante.

La situación planteada ha provocado que, hayan recibido varios ataques, los cuales afortunadamente y hasta el momento no han causado daños mayores. De continuar la problemática planteada, los servidores continuarán recibiendo ataques que pueden causar filtración, pérdida de información e interrupciones en los servicios de red.

Siguiendo el orden de ideas, la presente investigación evaluará los diferentes tipos de medidas y estándares de seguridad existentes, para escoger las prácticas más adecuadas que permitan mantener los tres pilares de la seguridad de la información, y así determinar la factibilidad de un sistema de gestión de seguridad de la información de la alcaldía, con el fin de proponer una solución técnica a la problemática planteada, adaptada al cumplimiento de la seguridad informática.

Actualmente en la alcaldía de la Jagua de Ibirico, la oficina de Tecnologías de la Información y las Comunicaciones – TIC, está direccionada a su fortalecimiento en la gestión, formulación y ejecución de proyectos de impacto que sean estratégicos y de apoyo para el desarrollo socio cultural, económico, tecnológico e institucional. Es importante mejorar las deficiencias que se han diagnosticado y establecido actualmente, esto debido a un alto nivel de desinterés y poca gestión en rescatar y poner en marcha la verdadera finalidad de la Oficina de las TIC en el Municipio de La Jagua de Ibirico, Cesar.

1.3 Objetivos de la pasantía.

1.3.1 General

Diseñar un plan de seguridad informática para la Alcaldía de la Jagua de Ibirico, Cesar.

1.3.2 Específicos

- Realizar un diagnóstico sobre las medidas de seguridad de la información con los que cuentan la alcaldía municipal de la Jagua de Ibirico, Cesar a través de la herramienta Microsoft Security Assessment Tool (MSAT).
- Diseñar el análisis de riesgos de la Alcaldía de la Jagua de Ibirico, mediante la metodología MAGERIT.
- Definir los controles a través de la Declaración de Aplicabilidad (SOA), de acuerdo con la norma ISO 27001:2013.

1.4 Descripción de las actividades a desarrollar en la misma. (Ver el cuadro).

Tabla 2 Descripción de las actividades a desarrollar por cada objetivo específico

Objetivo general	**Objetivo especifico**	**Actividades a desarrollar en la empresa para cumplir los objetivos específicos**
Diseñar un plan de seguridad informática para la Alcaldía de la Jagua de Ibirico	Realizar un diagnóstico sobre las medidas de seguridad de la información con los que cuentan la alcaldía municipal de la jagua de Ibirico, Cesar, a través de la herramienta	Se empleará la herramienta Microsoft Security Assessment Tool (MSAT), a partir de una serie de preguntas a los funcionarios de la alcaldía, la cual permitirá tener un conocimiento de las diferentes áreas de la entidad que presentan riesgos de seguridad y vulnerabilidades específicas.

	Microsoft Security Assessment Tool (MSAT).	Realizar un informe de acuerdo a los hallazgos identificados, luego de aplicar la herramienta.
	Diseñar el análisis de riesgo de la Alcaldía de la Jagua de Ibirico mediante la metodología MAGERIT.	Realizar el inventario de activos Identificar las amenazas existentes Determinar el impacto Hacer la estimación del riesgo
	Definir los controles a través de la Declaración de Aplicabilidad (SOA), de acuerdo con la norma ISO 27001:2013	Se elaborará el manual de seguridad informática con sus respectivas políticas acordes al perfil actual de cada dependencia de la Alcaldía, en la cual contaremos con las siguientes etapas requeridas por la política Revisión: la primera revisión de la política será por parte de los implicados en este proceso en donde se pasará a segunda revisión por parte del asesor jurídico de la Secretaría General, para garantizar que se cuente con todos los estándares

	Aprobación: la política se pasará a la Asesoría Jurídica de la Alcaldía de la Jagua de Ibirico para la revisión legal y posterior aprobación por parte del alcalde o jefe del área de las TIC con lo cual se establecerá la obligatoriedad de cumplimiento de las mismas.

2 Enfoques referenciales

2.1 Tipo de investigación

Con base en las características del plan de trabajo, se utilizó el desarrollo del método investigación de tipo descriptivo, ya que, corresponde al análisis y desarrollo de una propuesta

para diseñar un plan de seguridad informática para la Alcaldía de la Jagua de Ibirico, de acuerdo al alcance definido, las necesidades de la entidad y tomando para base para ello, el modelo de referencia de seguridad de la norma ISO/IEC 27001:2013.

En este tipo de investigación, la información de interés fue recogida de forma directa de la fuente, mediante encuestas, cuestionario, entrevista o reuniones.

Así mismo, se tuvo un enfoque cuantitativo ya que, se utilizaron técnicas pertinentes para la recolección de datos, como la observación, las encuestas y la revisión de documentos generalizando los resultados encontrados en un grupo (muestra), en este caso los funcionarios de la oficina de tecnología de la alcaldía (Hernández, Fernández, & Baptista, 2010).

La herramienta diseñada, es una encuesta que se aplicó a 30 funcionarios de la Alcaldía, principalmente a los del área de Hacienda, con el fin de saber, qué tan enterados están de la seguridad de la información en la entidad, así como su percepción sobre los servicios recibidos.

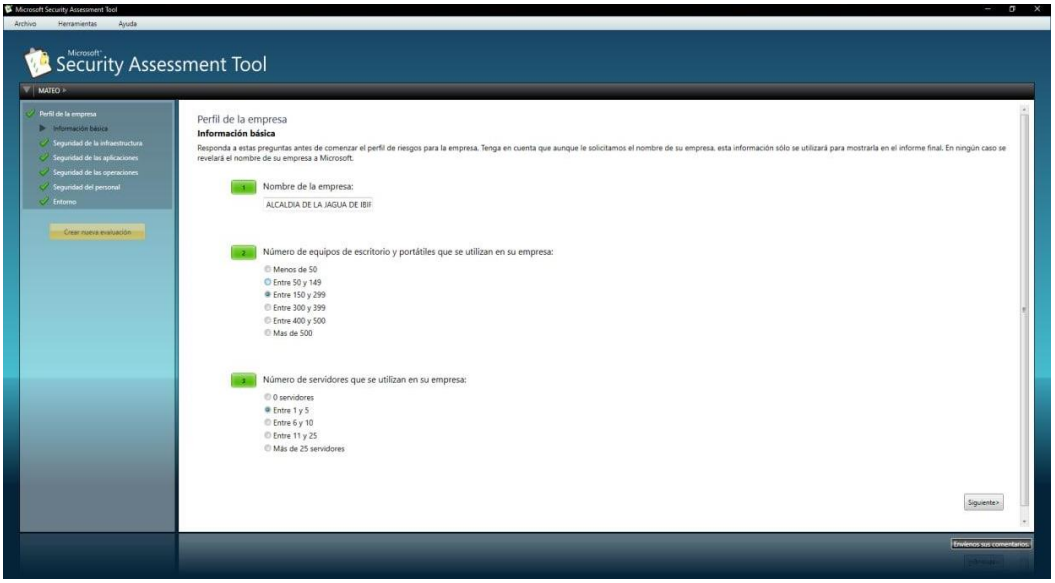
3 Informe de cumplimiento de trabajo

3.1 Presentación de resultados

Realizar un diagnóstico sobre las medidas de seguridad de la información con los que cuentan la Alcaldía Municipal de la Jagua de Ibirico, Cesar a través de la herramienta Microsoft Security Assessment Tool (MSAT).

Se realizó una encuesta a los funcionarios de la alcaldía de la Jagua de Ibirico, para conocer el índice de confiabilidad de la seguridad informática, a través del sistema MSAT 4.0 (Security Assessment Tool).

Figura 3 Encuesta a los funcionarios



Se realizó la encuesta, y en el presente informe se van a colocar algunos de los resultados obtenidos. Esta herramienta tecnológica, permite aplicar la encuesta de manera organizada, es decir, se presenta por secciones, facilitando la comprensión a los encuestados, por lo tanto, como se puede observar en la figura anterior, se cuenta con el perfil de la empresa, seguridad de la infraestructura, seguridad de las aplicaciones, seguridad de las operaciones, seguridad del personal y entorno. Suministrando información fundamental para el desarrollo de los objetivos planteados.

Figura 4 Pregunta de Infraestructura

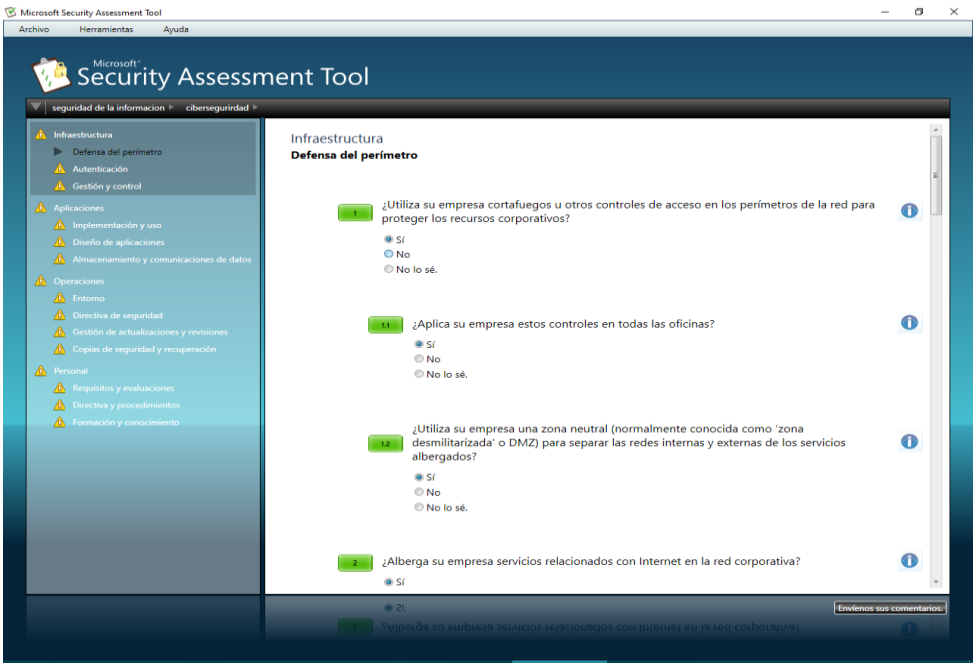
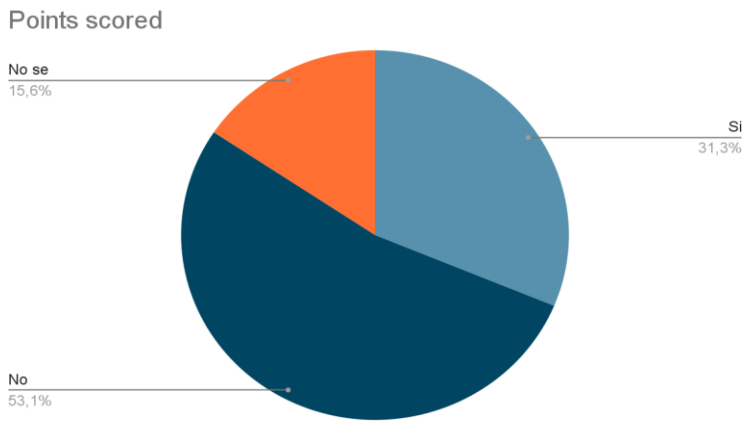


Figura 5 Gráfica de la pregunta sobre infraestructura



Para este interrogante, se contaba con 3 opciones de respuesta, los encuestados se inclinaron por la opción NO, con un 53%, si con un 31.3% y no saben un 15.6%. Demostrando el desconocimiento en el tema en su gran mayoría.

Se presentan a continuación, otros ejemplos de preguntas con su respectiva gráfica para evidenciar la utilización y aplicación de la herramienta para este primer objetivo.

Figura 6 Pregunta de infraestructura-internet

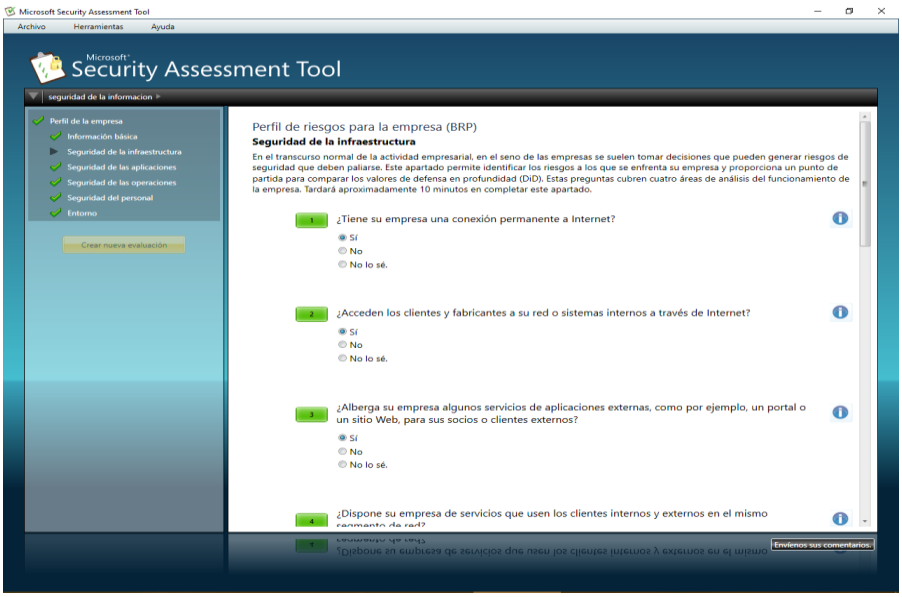
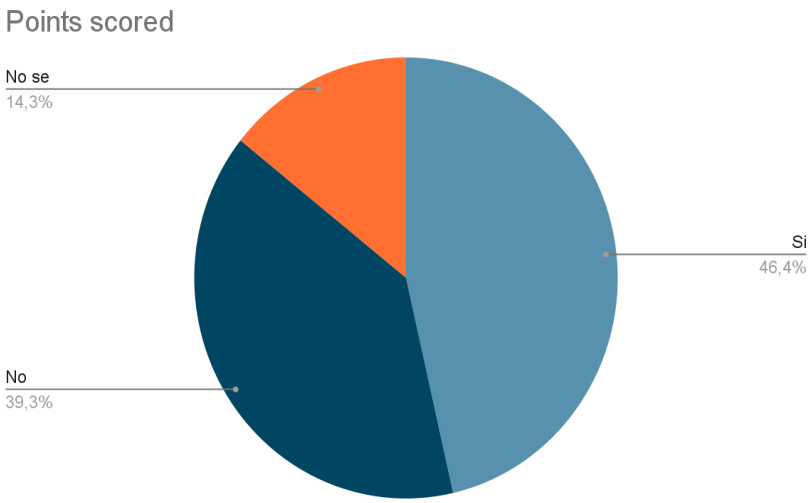


Figura 7 Gráfica pregunta infraestructura- internet



Se presenta un ejemplo de las preguntas realizadas en el tema de seguridad personal.

Figura 8 Preguntas de seguridad personal

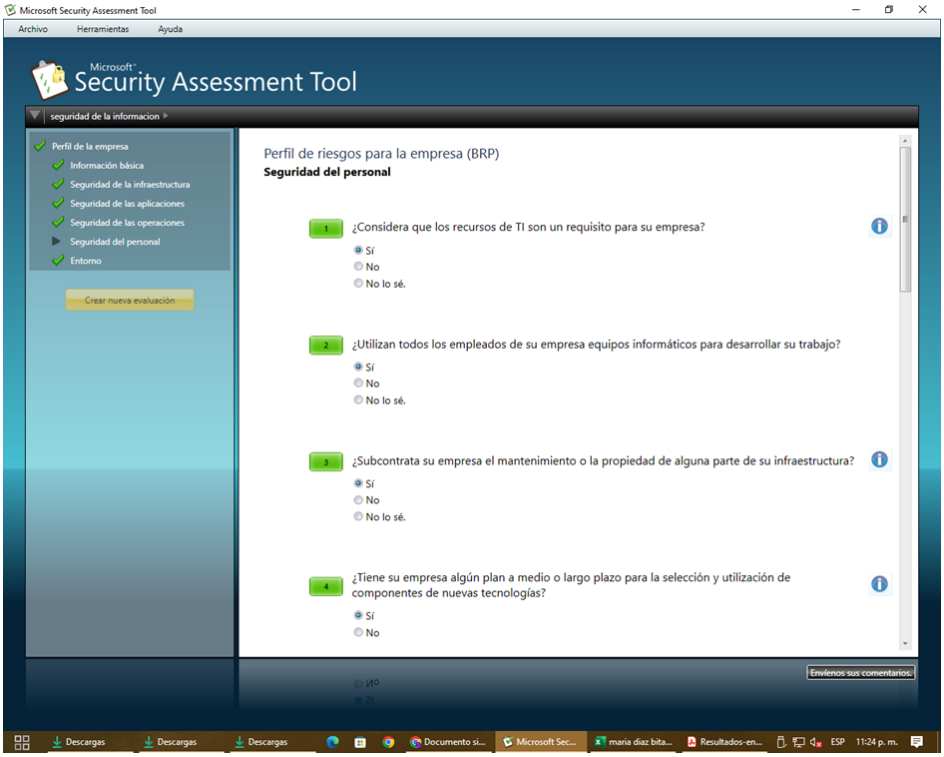
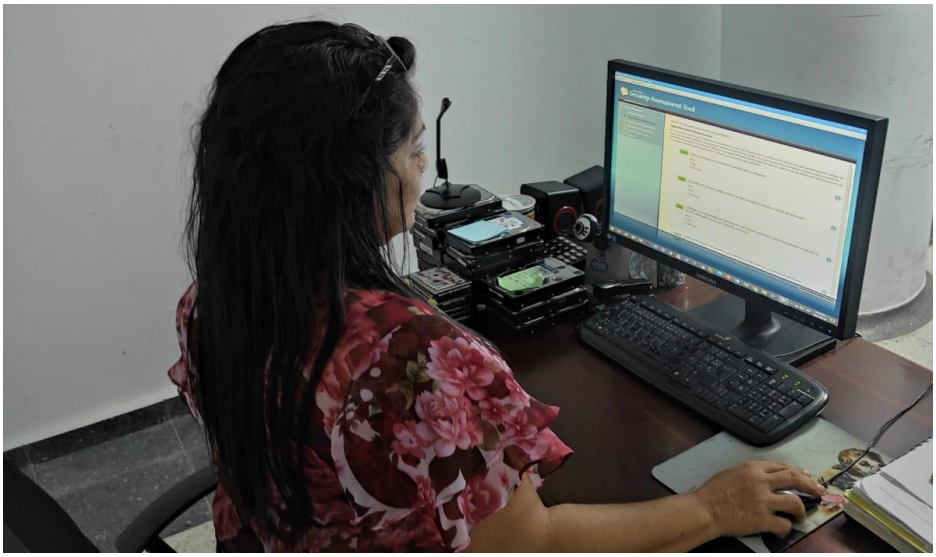
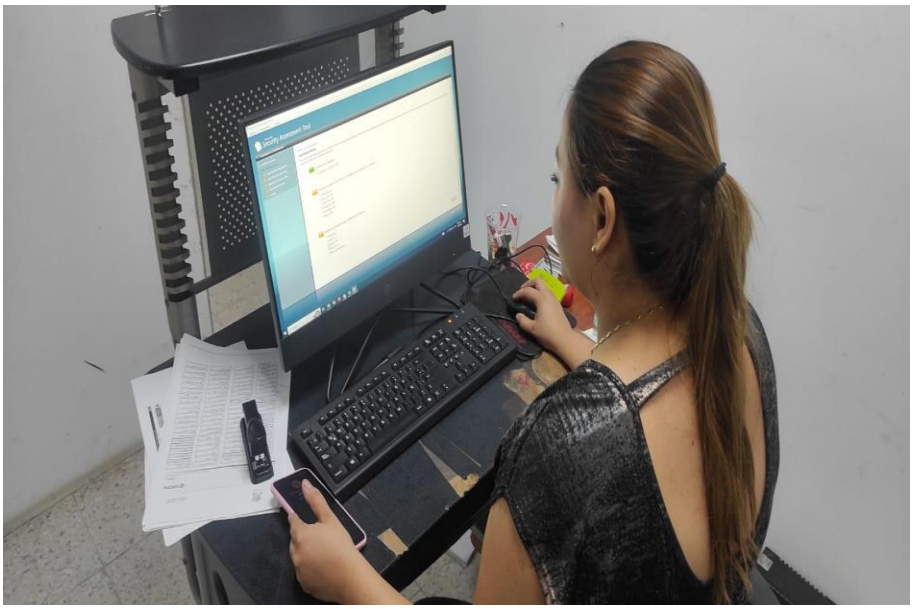


Figura 9 Fotografías evidencia de la aplicación de la encuesta a funcionarios





Frente al diagnóstico, a continuación, se presenta un balance general de los hallazgos encontrados luego de analizar los datos obtenidos de los directamente implicados, como son los funcionarios de la Alcaldía de la Jagua de Ibirico, Cesar.

1. Los empleados en su gran mayoría (90%), no están familiarizados con los términos de seguridad informática, lo que dificulta, al momento de aplicar controles para mitigar los riesgos.

2. En cuanto a las normas de seguridad planteadas en la entidad, son prácticamente nulas, pues, aunque disponen de un software con antivirus legal, no proporciona mucha seguridad a la hora de ataques informáticos como suplantación de identidad por el correo.

3. Con relación a infraestructura tecnológica, manejan una red con topología en árbol y conexiones directas a los cuartos del rack, con cableado UTP, hasta las entidades financieras.

4. La red principal se subdivide en dos redes, una con dirección 10.90.1.90; y la otra con dirección 192.168.1.1, no se cuenta con normas de cableado estructurado.
5. Frente a las normas, no se manejan ninguna, razón por la que, a través de la presente pasantía se implementaron algunos controles de la Norma ISO 27001.
6. Se encuentra en proceso de implementación de las políticas de seguridad de la información, el cual están diseñadas y se requiere mejoras continuas.
7. Se podría decir que están expuestos a todas las vulnerabilidades y amenazas posibles como ataques a la información, riesgos por daños por agua o por fuego, virus, gusanos, errores de configuración, entre otros.
8. No existen protocolos para prevenir cualquier tipo de ataque, aunque la entidad es consciente de la importancia de disponer de medidas que mitiguen los riesgos.

3.2 Diseñar el análisis de riesgos

3.2.1 Inventario de activos

Según la metodología Magerit, los activos son todos los elementos que la empresa tiene para el procesamiento de su información, por ejemplo, el recurso humano, hardware, software, instalaciones etc. Con la metodología Magerit, se clasificaron los activos de acuerdo a la función que cumplen en el tratamiento de la información.

Tabla 3 Activos con Magerit

Código	Nombre Grupo	Código Activo	Nombre Activo	Tipo Tecnología
[host]	Grandes equipos	[serv]	Servidores	Equipos Informáticos
[Mobile]	Informática móvil	[portátiles]	Computadores portátiles y otros dispositivos móviles	Equipos Informáticos
[pc]	Informática personal	[secAcienda]	Secretaria De Hacienda	Equipos Informáticos
[pc]	Informática personal	[SecEduc]	Secretaria De Educación	Equipos Informáticos
[pc]	Informática personal	[SecGob]	Secretaria De Gobierno	Equipos Informáticos
[pc]	Informática personal	[SecPLanea]	Secretaria De Planeación	Equipos Informáticos
[pc]	informática personal	[secEstruc]	Secretaria De Infraestructura.	Equipos Informáticos
[pc]	Informática personal	[thumano]	Oficina Talento H.	Equipos Informáticos
[pc]	Informática personal	[SecDesp]	Secretaria Despacho	Equipos Informáticos
[pc]	informática personal	[secSalud]	Secretaria De Salud	Equipos Informáticos
[pc]	informática personal	[controlDicip]	Control Interno Disciplinario	Equipos Informáticos
[pc]	Informática personal	[controlInt]	Control Interno	Equipos Informáticos
[pc]	informática personal	[Sistemas]	Sistemas	Equipos Informáticos

[pc]	Informática personal	[Contrata]	Contratación	Equipos Informáticos
[pc]	Informática personal	[gesSoc]	Gestión Social	Equipos Informáticos
[scan]	Escáner	[E_platteryEscanner]	Equipos de plotter y escanners	Equipos Informáticos
[HW]	Equipos que son fácilmente transportados	[PC_portatiles]	Equipos Portátiles	Equipos Informáticos
[print]	medios de impresión	[E_Impresoras]	Impresoras Lasser	Equipos Informáticos
[print]	Medios de impresión	[E_ImpresorasT]	Impresoras de inyección de tinta	Equipos Informáticos
[router]	Encaminadores	[R_enrutadores]	Enrutadores	Equipos Informáticos
[wifi]	Red inalámbrica	[R_ap]	Ap para Red Inalámbrica	Redes de Comunicaciones
[Lan]	Red local	[R_local]	Red local	Redes de comunicaciones
[Internet]	Internet	[Internet]	Internet	Redes de comunicaciones
[LAN]	Red local	[c_switch]	Switche de 24 puertos	Redes de Comunicaciones
[LAN]	Red local	[c_patch]	Patch Panel	Redes de Comunicaciones
[os]	Sistema operativo	[winxp]	Windows XP	Software
[os]	Sistema operativo	[win7]	Windows 7	Software
[os]	Sistema operativo	[winServ]	Windows Server	Software
[os]	Sistema operativo	[linux]	Linux	Software

[office]	Ofimática	[officce]	Microsoft Office	Software
[office]	Ofimática	[WEB1]	CUTEPDF	Software
[app]	Servidor de aplicaciones	[CONVENIO GOBERNACION DEL CESAR]	SIIAF Área Financiera (Módulos, Presupuesto Gastos, Presupuesto de Ingresos, Integración, Apropiación, Contabilidad, Egresos,	Software
[app]	Servidor de aplicaciones	[SICEP]	Contraloría G	Software
[app]	Servidor de aplicaciones	[SIDEF]	Contraloría G	Software

Fuente. Alcaldía de la Jagua de Ibirico

3.2.2 Identificación de amenazas

Para la realización de esta tabla, se determinaron 20 amenazas que se ven reflejadas en los activos de la alcaldía municipal de la Jagua de Ibirico

Tabla 4 Identificación de amenazas en la alcaldía de la Jagua de Ibirico

Amenazas	**Activos**
[N.1] Fuego	[host] servidores [Mobile] dispositivos móviles [pc] Equipo de cómputo de mesa [scan] Equipos de plotter y escanners [HW] Equipos Portátiles [print] Impresoras Lasser [print] Impresoras de inyección de tinta

	[router] Enrutadores
	[host] servidores
	[pc] Equipo de cómputo de mesa
	[scan] Equipos de plotter y escanners
[N.2] Daños por agua	[wifi] Ap para Red Inalámbrica
	[LAN] Red local Switche de 24 puertos
	[printed] Carpetas con la documentación de cada proyecto en ejecución
	[building] Instalación física de la entidad
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.
	[usb] Almacenamientos en Disco Duro
[N.7] Desastres naturales. Fenómeno sísmico.	[printed] Carpetas con la documentación de cada proyecto en ejecución
	[ui] Personal de soporte TI
	[adm] Administrador de sistemas
	[host] servidores
	[mobile] dispositivos móviles
	[pc] Equipo de cómputo de mesa
	[scan] Equipos de plotter y escanners
[I.5] Avería de origen físico o lógico.	pc] Equipo de cómputo de mesa [print] Impresoras Lasser
	[router] Enrutadores
	[backup] sistema de backup
	[file] Servicio de almacenamiento de información en el Servidor de bases de datos.
	[building] Instalación física de la entidad
[I.6] Corte del suministro eléctrico	[host] servidores
	[pc] Equipo de cómputo de mesa
	[scan] Equipos de plotter y escanners
	[HW] Equipos Portátiles
	[app] Servidor de aplicaciones

[I.7] Condiciones inadecuadas de temperatura o humedad	[host] servidores [pc] Equipo de cómputo de mesa [print] Impresoras Lasser [wifi] Ap para Red Inalámbrica [LAN] Red local Switche de 24 puertos [app] Servidor de aplicaciones [printed] Carpetas con la documentación de cada proyecto en ejecución [ui] Personal de soporte TI adm] Administrador de sistemas
[I.8] Fallo de servicios de comunicaciones	[wifi] Ap para Red Inalámbrica [LAN] Red local Switche de 24 puertos [Intranet] intranet [www] Servicio de internet al que pueden acceder los funcionarios [email] Manejo de correos electrónicos [file] Servicio de almacenamiento de información en el servidor de bases de datos.
[I.10] Degradación de los soportes de almacenamiento de la información	[backup] sistema de backup Base de datos [backup]Archivo de Copias de seguridad de la información [file] Servicio de almacenamiento de información en el servidor de bases de datos. [usb] Almacenamientos en Disco Duro
[E.1] Errores de los usuarios.	[pc] Equipo de cómputo de mesa [scan] Equipos de plotter y escanners [HW] Equipos Portátiles [print] Impresoras Lasser

	[print] Impresoras de inyección de tinta
	[os] sistema operativo
	[office] Microsoft Office
	[email] Manejo de correos electrónicos
	[printed] Carpetas con la documentación de cada proyecto en ejecución
[E.2] Errores del administrador	[host] servidores
	[router] Enrutadores
	[wifi] Ap para Red Inalámbrica
	[LAN] Red local Switche de 24 puertos
	[Intranet] intranet
	[os] sistema operativo
	[app] Servidor de aplicaciones
	[password] Contraseñas de acceso de usuarios del sistema
	[encrypt] Claves de cifra de Los bancos
[E.8] Difusión de software dañino	[host] servidores
	[pc] Equipo de cómputo de mesa
	[HW] Equipos Portátiles
	[os] sistema operativo
	[dbms] Oracle motor de base datos
	[www] Servicio de internet al que pueden acceder los funcionarios
	[email] Manejo de correos electrónicos
[E.15] Alteración accidental de la información	[office] Microsoft Office
	[dbms] Oracle motor de base datos

	[files] Información de Contribuyentes [backup]Archivo de Copias de seguridad de la información [password] Contraseñas de acceso de usuarios del sistema [email] Manejo de correos electrónicos [file] Servicio de almacenamiento de información en el servidor de bases de datos. [usb] Almacenamientos en Disco Duro [printed] Carpetas con la documentación de cada proyecto en ejecución
[E.18] Destrucción de información	[office] Microsoft Office [dbms] Oracle motor de base datos [files] Información de Contribuyentes [backup]Archivo de Copias de seguridad de la información [password] Contraseñas de acceso de usuarios del sistema [email] Manejo de correos electrónicos [file] Servicio de almacenamiento de información en el servidor de bases de datos. [usb] Almacenamientos en Disco Duro [printed] Carpetas con la documentación de cada proyecto en ejecución
[E.24] Caída del sistema por agotamiento de recursos	[host] servidores [pc] Equipo de cómputo de mesa [HW] Equipos Portátiles [os] sistema operativo [app] Servidor de aplicaciones [dbms] Oracle motor de base datos [HW] Equipos Portátiles

[E.25] Pérdida de equipos-Robo	[usb] Almacenamientos en Disco Duro
	[printed] Carpetas con la documentación de cada proyecto en ejecución
	[files] Información de Contribuyentes
	[backup]Archivo de Copias de seguridad de la información
	[password] Contraseñas de acceso de usuarios del sistema
[A.5] Suplantación de la identidad del usuario	[pc] Equipo de cómputo de mesa
	[HW] Equipos Portátiles
	[dbms] Oracle motor de base datos
	[password] Contraseñas de acceso de usuarios del sistema
[A.11] Acceso no autorizado	[host] servidores
	[adm] Administrador de sistemas
	[printed] Carpetas con la documentación de cada proyecto en ejecución
	[backup]Archivo de Copias de seguridad de la información
[A.24] Denegación de servicio	[host] servidores
	[app] Servidor de aplicaciones
	[www] Servicio de internet al que pueden acceder los funcionarios
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.
[A.26] Ataque destructivo	[host] servidores
	[wifi] Ap para Red Inalámbrica
	[LAN] Red local Switche de 24 puertos
	[dbms] Oracle motor de base datos
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.

Fuente. Libro Metodología Magerit versión 3

3.2.3 Resultado Plan de pruebas (vulnerabilidades)

Para la realización del plan de pruebas se procedió con dos metodologías descritas así:

Primera metodología: Plan de pruebas para detectar las vulnerabilidades mediante las pruebas aplicadas (pruebas documentales, fotográficas, con software).

Tabla 5 Vulnerabilidades y riesgos inicialmente identificados

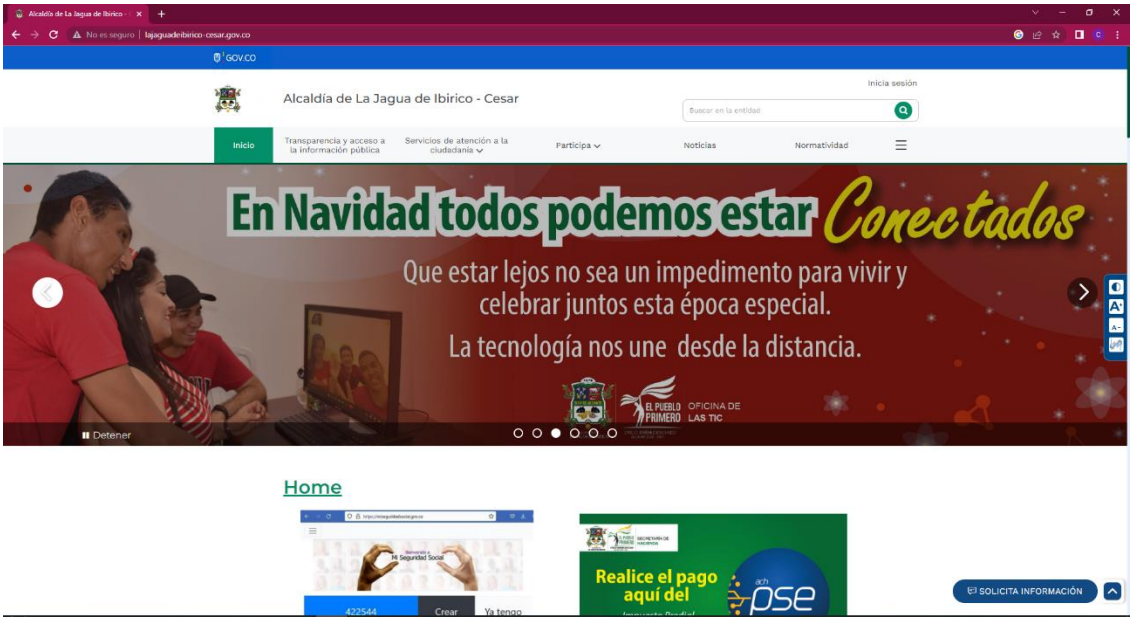
Código	**Vulnerabilidad**	**Riesgo**
V1	Falta de equipos UPS's para contingencias, cortes de energía o sobrecargas en los equipos	Pérdida de información, daños en los equipos, pérdida de tiempo en procesos repetidos.
V2	Software con problemas de seguridad en el desarrollo	Pérdida o modificación de información, robo de claves de usuario. modificación de datos, bases de datos inseguras por permisos y privilegios no definidos, Perdida de la información de la página web.
V3	No existe control de acceso físico a las oficinas y equipos informáticos	Robo, destrucción, modificación o borrado de información, destrucción o desarticulación física de equipos.
V4	Deficiente control de acceso facilitando la suplantación de identidad	Robo de datos, suplantación de identidad de usuarios, robo de claves de usuarios
V5	Falta de una política de seguridad clara	Ataques no intencionados, ingeniería social, phishing. Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal

V6	Manipulación de la Configuración	No existe manual de configuración donde se expongan los posibles problemas

Fuente. Metodología Margerit

Para la realización de estas pruebas se utilizaron herramientas de software libre (Matriux, Kali Linux, otros), para identificar las vulnerabilidades, amenazas y riesgos de seguridad de los portales web del municipio seleccionado.

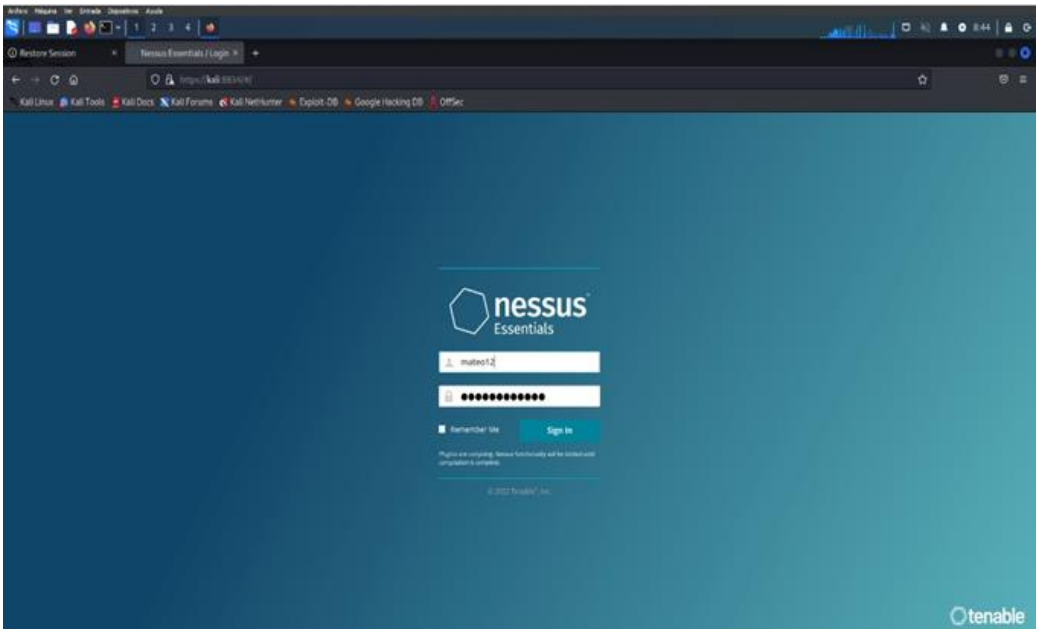
Figura 10 Página web de la Alcaldía de la Jagua de Ibirico



Fuente. (Alcaldia la Jagua de Ibirico, 2022)

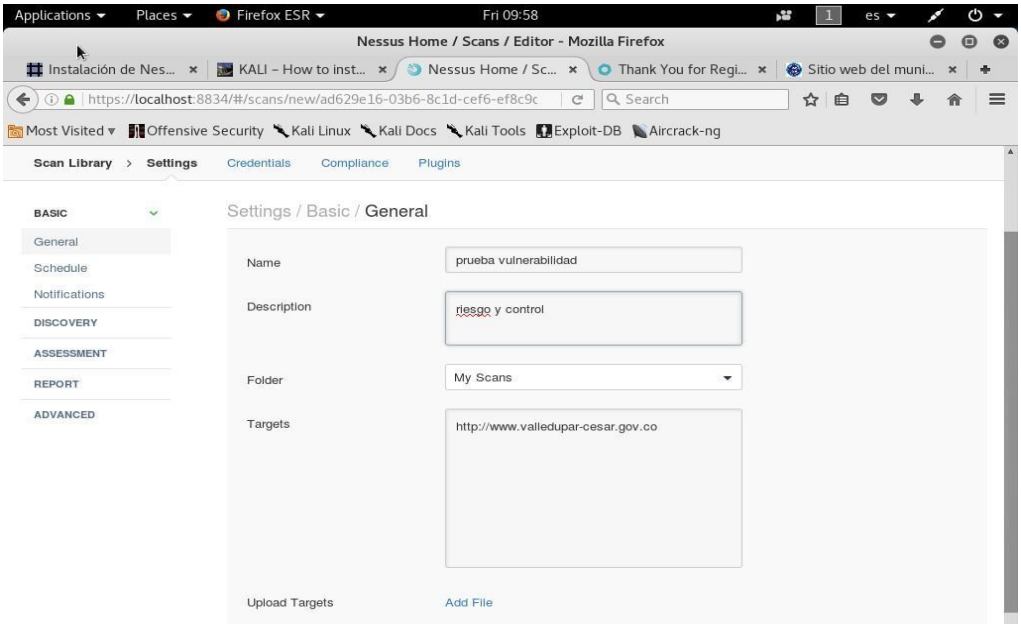
Para encontrar las vulnerabilidades se instaló NESSUS en una máquina virtual de Kali Linux.

Figura 11 Instalación del scanner Nessus



Nota. Escaneo del sitio http://lajaguadeibirico-cesar.gov.co

Figura 12 Pruebas de vulnerabilidad web



Fuente. Nessus máquina virtual

La vulnerabilidad arrojó tipo alto **MTA Open Mail Reenvío permitido**. El servidor SMTP remoto parece permitir la retransmisión de correo. Esto significa que un usuario remoto no autenticado podría usar el servidor de correo para enviar mensajes al mundo, con lo que se

desperdicia el ancho de banda de la red y los recursos informáticos. Tales servidores son el objetivo de los spammers para el envío de correo electrónico no solicitado (UBE).

Figura 13 Resultado de las pruebas de vulnerabilidad web

Summary

Critical	High	Medium	Low	Info	Total
0	1	0	0	16	17

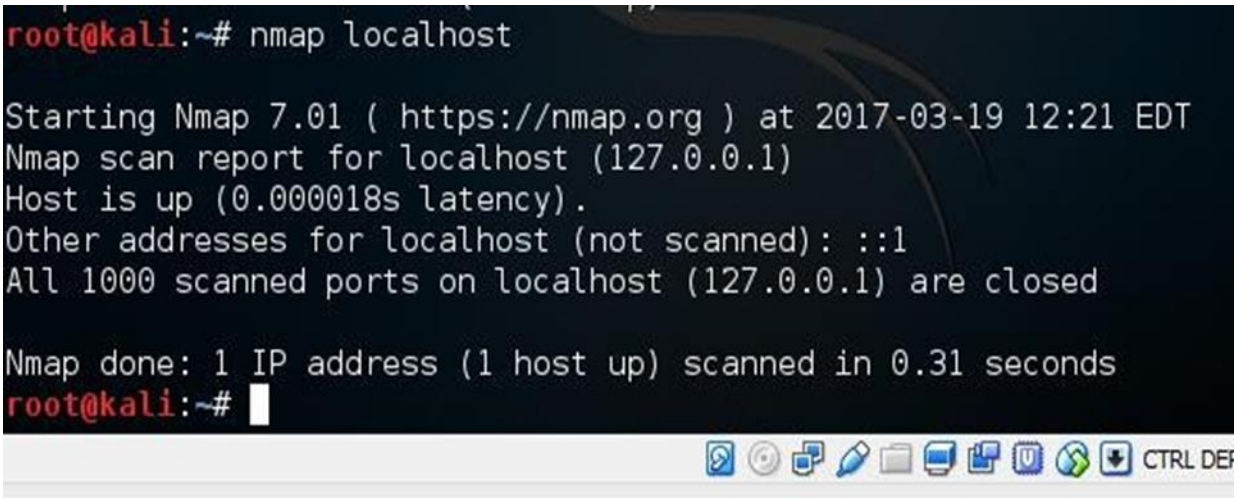
Details

Severity	Plugin Id	Name
High (7.8)	10262	MTA Open Mail Relaying Allowed
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10919	Open Port Re-check
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	19601	HP Data Protector Detection
Info	22964	Service Detection
Info	31422	Reverse NAT/Intercepting Proxy Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	54580	SMTP Authentication Methods
Info	54615	Device Type
Info	91000	BMC BladeLogic Server Automation RSCD Agent Detection

Se determinó mediante pruebas y usando herramientas de software (Matriux, Kali Linux, otros), las vulnerabilidades, amenazas y riesgos de seguridad del sitio web de la alcaldía de la Jagua de Ibirico. Las pruebas se realizaron con fines educativos, por lo cual, no se modificará nada en el sitio web, utilizando la herramienta software Kali Linux:

Primero se debe saber cuál es la Ip del sitio web de la alcaldía Jagua de Ibirico, para ello ingresamos a CMD y escribimos ping lajaguadeibirico-cesar.gov.co, la cual arroja la siguiente IP portal web: 190.7.108.19, como se muestra a continuación:

Figura 14 Ejecución de pruebas con Nmap



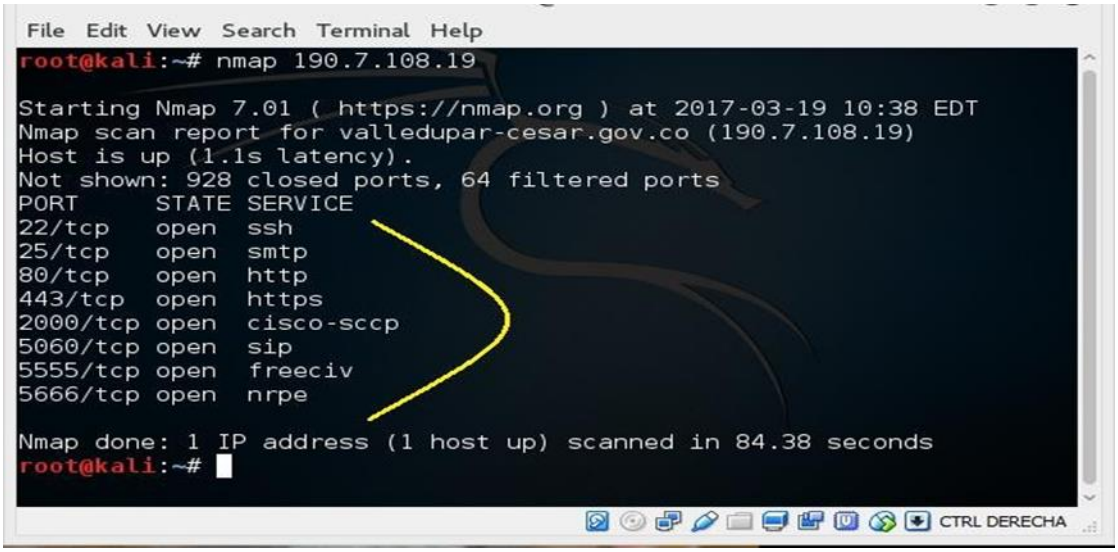
Fuente. Terminal Kali Linux

Se realiza el escaneo de vulnerabilidades, se escanean los puertos del cliente host para verificar los servicios que se están ejecutando y cuáles están abiertos. Primero se realiza un Nmap localhost para saber qué servicios están abiertos y cuáles cerrados.

Se observó que el sitio web de la alcaldía de la Jagua de Ibirico, tiene 928 puertos cerrados, tiene el puerto 22/TCP abierto, con servicio ssh, el 25/TCP abierto con servicio SMTP, 80/TCP abierto con el servicio HTTP, 443/TCP abierto con el servicio HTTPS, 2000/TCP abierto con el servicio CISCO-SCCP, 5060/TCP abierto con el servicio SIP, 5555 TCP abierto con el servicio FREECIV y 5555 TCP abierto con el servicio NRPE.

Se procede a realizar el escáner NMAP, para conocer el sistema operativo donde se está ejecutando el sitio web, para esto utilizamos el comando NMAP -0 190.7.108.19, se observa que se está ejecutando en un Linux 2.6:

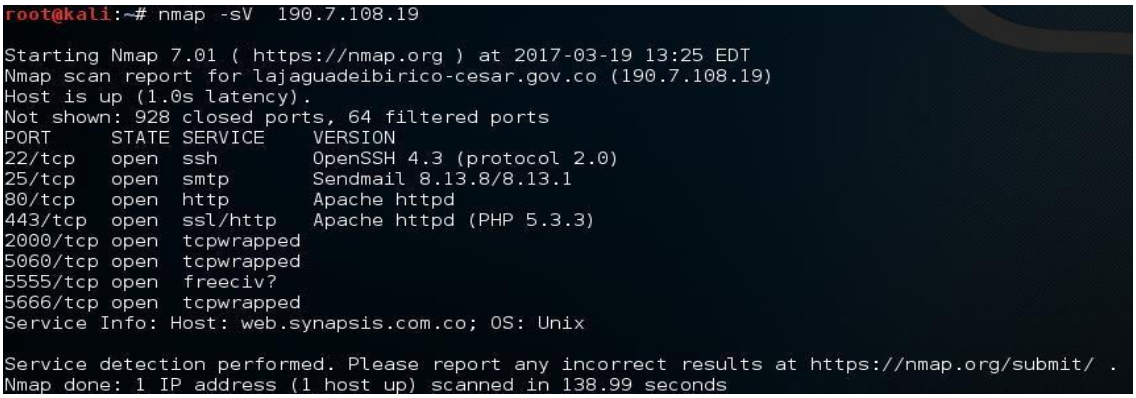
Figura 15 Resultados arrojados Nmap



Fuente. Terminal Kali Linux

Se buscan las versiones de los servicios que se están ejecutando:

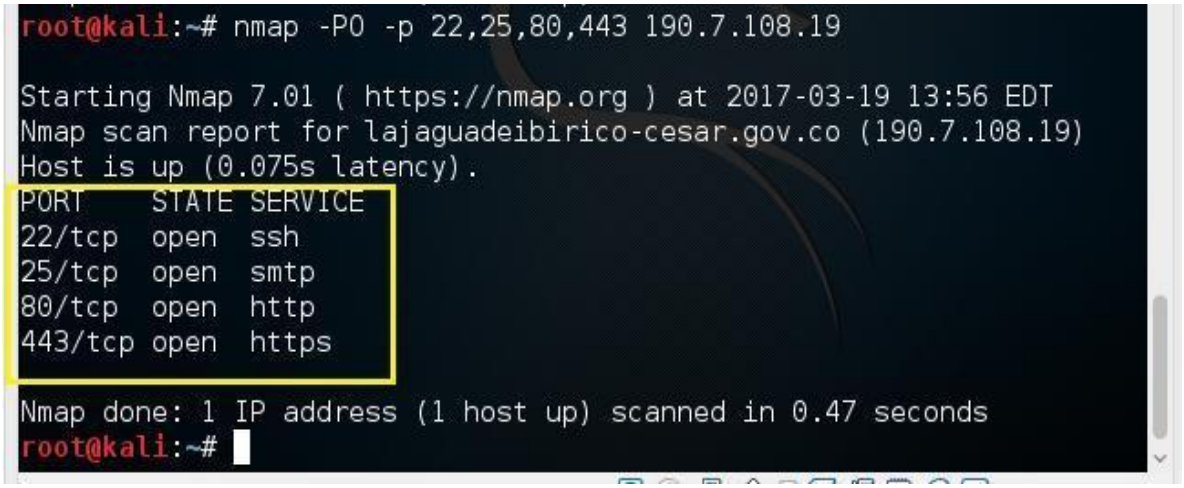
Figura 16 Versión servicios Nmap



Fuente. Terminal Kali linux

Se realizó un escaneo sólo a los puertos 80, 777, 3000 con el comando NMAP- PO-P 80:777:3000 de la IP 190.7.108.19, así:

Figura 17 Escaneos de puertos con Nmap



Fuente. Terminal Kali Linux.

3.2.4 Determinación del impacto

Para determinar el impacto, se midió con las siguientes tablas:

Tabla 6 Nivel de degradación de activos

Valor	Abreviatura	Nivel de Degradación
1	(MB)	MUY BAJO
2	(B)	BAJO
3	(M)	MODERADO
4	(A)	ALTO
5	(MA)	MUY ALTO

Fuente. Libro Metodología Magerit Versión 3.

Tabla 7 Probabilidad de ocurrencia de las amenazas

Valor	Abreviatura	Frecuencia
1	(MPF)	MUY POCO FRECUENTE

2	(PF)	POCO FRECUENTE
3	(N)	NORMAL
4	(F)	FRECUENTE
5	(MF)	MUY FRECUENTE

Fuente. Libro Metodología Magerit Versión 3.

3.2.5 Estimación del riesgo

Dentro de un sistema informático, se denomina riesgo a la magnitud del daño probable que pueda afectar los activos involucrados en el procesamiento de la información. Por tal motivo, la frecuencia de ocurrencia y el impacto generado por las amenazas, determinarán conjuntamente los riesgos existentes en los procesos informáticos. *Riesgo = Impacto x probabilidad;* por ello se hace la siguiente valoración para la estimación del riesgo:

Tabla 8 Valoración del riesgo

Clase de riesgo	**Valoración cualitativa**	**Valoración cuantitativa**
Crítico	Muy Alto	15 – 25
Grave	Alto	10 – 14
Moderado	Medio	5 – 9
Menor	Bajo	1 – 4

Fuente. Libro Metodología Magerit Versión 3.

Es por ello que, mediante la implementación de ésta, tendremos que la matriz referente para la estimación del riesgo será la siguiente:

Tabla 9 Implementación de la valoración del riesgo en la Alcaldía

Estimación del riesgo	**Vulnerabilidad (frecuencia)**				
	Muy poco frecuente	**Poco frecuente**	**Normal**	**Frecuente**	**Muy frecuente**

	Muy alto	21	22	23	24	25
Impacto	Alto	16	17	18	19	20
	Moderado	11	12	13	14	15
	Bajo	6	7	8	9	10
	Muy bajo	1	2	3	4	5

Fuente. Libro Metodología Magerit Versión 3.

A continuación, se hace la clasificación y el riesgo que se ha establecido por medio del presente estudio, plasmado en este documento, para la Alcaldía de la Jagua de Ibirico, Cesar y se muestra en la siguiente tabla:

Tabla 10 Clase y estimación de riesgo

CLASE DE RIESGO Y ESTIMACION DEL RIESGO			
Amenaza	**Activo**	**Clase Riesgo**	**Impacto**
	[host] servidores	8	6
	[mobile] dispositivos móviles	4	5
[N.1] Fuego	[pc] Equipo de cómputo de mesa	4	5
	[scan] Equipos de plotter y escanners	8	5
	[HW] EquiposPortatiles	8	6
	[print] Impresoras Lasser	5	5
	[print] Impresoras de inyección de tinta	8	6
	[router] Enrutadores	9	5
[N.2] Daños por agua	[host] servidores	9	5
	[pc] Equipo de cómputo de mesa	7	6
	[scan] Equipos de plotter y escanners	5	7
	[wifi] Ap para Red Inalámbrica	5	5

	[LAN] Red local Switche de 24 puertos	5	5
	[building] Instalación física de la entidad	4	6
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	9	7
[N.7] Desastres naturales. Fenómeno sísmico.	[usb] Almacenamientos en Disco Duro	6	5
	[printed] Carpetas con la documentación de cada proyecto en ejecución	7	8
	[ui] Personal de soporte TI	5	8
	[adm] Administrador de sistemas	7	6
	[host] servidores	9	10
	[mobile] dispositivos móviles	8	
	[pc] Equipo de cómputo de mesa	8	8
	[scan] Equipos de plotter y escanners	8	
	[pc] Equipo de cómputo de mesa	8	8
	[print] Impresoras Lasser	9	
	[router] Enrutadores	9	10
	[backup] sistema de backup	5	
[I.5] Avería de origen físico o lógico.	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5	10
	[building] Instalacion física de la entidad	9	10
	[host] servidores	7	

[I.6] Corte del suministro eléctrico	[pc] Equipo de cómputo de mesa	7	
	[scan] Equipos de plotter y escanners	9	12
	[HW] EquiposPortatiles	9	5
	[app] Servidor de aplicaciones	7	5
[I.7] Condiciones inadecuadas de temperatura o humedad	[host] servidores	8	5
	[pc] Equipo de cómputo de mesa	8	7
	[print] Impresoras Lasser	8	5
	[wifi] Ap para Red Inalámbrica	9	6
	[LAN] Red local Switche de 24 puertos	5	4
	[app] Servidor de aplicaciones	5	5

3.3 Definir los controles a través de la Declaración de Aplicabilidad (SOA), de acuerdo con la norma ISO 27001:2013.

Antes de poder definir los controles, es necesario, realizar la declaración de aplicabilidad (SOA), de acuerdo con la norma, para determinar el cumplimiento de estos, y así diseñar las estrategias más óptimas.

SOA, es un documento donde se relacionan los controles de seguridad, establecidos en el Anexo A del estándar ISO/IEC 27001(consta de 114 controles concentrados en 35 objetivos de control, en la versión de 2013)

Para efectos de la Declaración de Aplicabilidad, se han definido los siguientes Estados de Control:

Implementado. Control que está planificado, desarrollado, ejecutado, documentado y debidamente difundido, en algunos casos se encuentra revisado o auditado.

No implementado. Control que, si bien puede estar planificado, no se encuentra desarrollado ni documentado.

Implementado parcialmente. Control que está planificado, desarrollado, pero está parcialmente ejecutado y/o documentado y/o difundido.

Aplica a una posterior fase del ciclo del SGSI. Control que se va a implementar en una fase posterior del ciclo del SGSI, debido al grado actual de madurez de la organización.

Implementación a cargo de externo. Es un control que, debido a las condiciones del negocio y de la organización, no puede ser implementado por la división de sistemas, sino por una entidad externa.

No aplica. Control que en la actualidad no aplica, por el tipo de negocio del servicio de verificación o por el contexto que se tiene actualmente, pero que pueden ser contemplados en el futuro.

Estados de Control SOA. De acuerdo a los numerales antes mencionados, en este informe se han considerado dos tipos de estados de los controles de la ISO 27001:2013.

- Grupo de Controles que aplican:
    - Implementados (6 controles)
    - No implementados (36 controles)
    - Implementados parcialmente (52 controles)
    - Aplica en una posterior fase del ciclo del SGSI (24 controles)

- Implementación a cargo de externo (1 controles)

- Grupo de Controles que no aplican. (14 controles).

Tabla 11 Controles SOA

Estado del control	Controles
Implementado	6
No implementado	36
Implementado parcialmente	52
Aplica a una posterior fase del ciclo del SGSI	24
Implementación a cargo de externo	1
No aplican	14
Total	133

Fuente. Anexo A NTC-ISO/IEC 27001

Tabla 12 Estados controles SOA

Nivel	Estado	Definición
A0	No existe	La directiva (o el proceso) no está documentada y la organización, anteriormente, no ha tomado conciencia del riesgo de negocios asociado a esta administración de riesgos.
A1	Ad hoc	Es evidente que algunos miembros de la organización han llegado a la conclusión de que la administración de riesgos tiene valor. No obstante, los esfuerzos de administración de riesgos se han llevado a cabo de un modo ad hoc. No hay directivas o procesos documentados y el proceso no se puede repetir por completo. En general, los proyectos de administración de riesgos parecen caóticos y sin coordinación; los resultados no se han medido ni auditado.

A2	Repetible	Hay una toma de conciencia de la administración de riesgos en la organización. El proceso de administración de riesgos es repetible, aunque inmaduro. El proceso no está totalmente documentado; no obstante, las actividades se realizan periódicamente y la organización está trabajando en establecer un proceso de administración de riesgos exhaustivo con la participación de los directivos. No hay cursos formales ni comunicados acerca de la administración de riesgos; la responsabilidad de la implementación está en manos de empleados individuales.
A3	Proceso definido	La organización ha tomado una decisión formal de adoptar la administración de riesgos incondicionalmente con el fin de llevar a cabo su programa de seguridad de información. Se ha desarrollado un proceso de línea de base en el que se han definido los objetivos de forma clara con procesos documentados para lograr y medir el éxito.
A4	Administrado	Hay un conocimiento extendido de la administración de riesgos en todos los niveles de la organización. Los procedimientos de administración de riesgos existen, el proceso está bien definido, la comunicación de la toma de conciencia es muy amplia, hay disponibles cursos rigurosos y se han implementado algunas formas iniciales de medición para determinar la efectividad.
A5	Optimizado	La organización ha dedicado recursos importantes a la administración de riesgos de seguridad y los miembros del personal miran al futuro intentando determinar los problemas y soluciones que habrá en los meses y años venideros. El proceso de administración de riesgos se ha comprendido. La causa principal de todos los problemas de seguridad se ha identificado y se han adoptado medidas adecuadas para minimizar el riesgo.

Fuente. NTC-ISO/IEC 27001

Tabla 13 Declaración A1

Control ISO	**Requerimiento**	**Estado**	**Proceso de implantación**	**Razones para la selección**
5.1	Política de Seguridad de la Información	Para proporcionar a la dirección de gestión y apoyo a la seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.		
5.1.1	Se tiene documento de la política de	Implementado parcialmente	Se está realizando un documento	Dentro de los pasos para la implementación de un SGSI es necesario definir

	seguridad de la Información			unas políticas para aplicar a la organización.
5.1.2	Se hace revisión y evaluación de este documento y se promulga su lectura y aplicación.	No Implementado	Aún no se ha documentado.	Es necesario que el manual de políticas sea revisado, autorizado y comunicado.
6.1	Organización Interna	Para gestionar la seguridad de la información dentro de la organización		
6.1.1	Compromiso de las Directivas con la seguridad de la información	Implementado parcialmente	Se realizó un documento	La oficina de sistemas debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información
6.1.2	Coordinación de la Seguridad	No implementado	Aún no se ha documentado.	Típicamente, la coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de los gerentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo.

Tabla 14 Declaración A2

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
6.1.3	Asignación de responsabilidades	No implementado	Aún no se ha documentado	Se debieran definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos.
6.1.4	Proceso de Autorización a áreas de procesamiento de información	No aplica	No aplica	Aún no se ha presentado la necesidad de nuevos servicios de procesamiento de información.
6.1.5	Se realizan acuerdos de confidencialidad	Implementado parcialmente	Aún no se ha documentado	Los acuerdos de confidencialidad o no divulgación, debieran tener en cuenta el requerimiento de proteger la información confidencial utilizando términos legalmente ejecutables.
6.1.6	Contacto con las autoridades	No aplica	No aplica	No hay definido un procedimiento claro en la organización y no hay claridad de en quién recae esta función.
6.1.7	Contacto con grupos de especial interés	No aplica	No aplica	En la actualidad el seguimiento y gestión de SGSI está a cargo de personal interno de la organización.
6.1.8	Se realiza auditoría interna	Aplica a una posterior fase del ciclo del SGSI	No aplica	En la actualidad el SGSI está en etapa de planificación, aún no se ha puesto en marcha para poder auditarlo.

6.2	Terceros	Para mantener la seguridad de la información y de las instalaciones de procesamiento de información de la organización que se tiene acceso, procesan, comunican a, o administrados por entidades externas.

Tabla 15 Declaración A3

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
6.2.1	Identificación de riesgos	Implementado parcialmente	Aún no se ha documentado	Grupo externo tenga acceso a los medios de samiento de la información o la mación de una organización, se era llevar a cabo una evaluación iesgo paraidentificar cualquier requerimiento de controles
6.2.2	Aproximación a la seguridad al tratar con clientes	Implementado parcialmente	Aún no se ha documentado	Se debieran considerar dependiendo del tipo y extensión de acceso dado antes de proporcionar a los clientes, acceso a cualquier activo de la organización
6.2.3	Aproximación a la seguridad en acuerdos con terceros	Implementado parcialmente	Aún no se ha documentado	El acuerdo debiera asegurar que no existan malos entendidos entre la organización y la otra parte.
7.1	Responsabilidad por recursos críticos	Para lograr y mantener la protección adecuada de los activos de la organización.		
7.1.1	Inventario de activos tecnológicos y de la información.	Implementado	Se realizó un documento	Se identificó y se documentó todos los activos de la organización
7.1.2	Responsables de los activos tecnológicos	Implementado parcialmente	Aún no se han aplicado	Identificar persona o entidad que cuenta con la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

7.1.3	Uso aceptable de los activos tecnológicos	Implementado parcialmente	Aún no se han aplicado	El acuerdo debiera asegurar que no existan malos entendidos entre la organización y la otra parte.
7.2	Clasificación de la Información	Para asegurar que la información reciba un nivel adecuado de protección.		
7.2.1	Normas para clasificación de la información	No implementado	Aún no se ha documentado	Las clasificaciones y los controles de protección asociados para la información debieran tomar en cuenta las necesidades comerciales de intercambiar o restringir información y los impactos comerciales asociados con dichas necesidades.
7.2.2	Identificación y manejo de la información	No aplica	No aplica	Los procedimientos para el etiquetado de la información necesitan abarcar los activos de información en formatos físicos y electrónicos.
8.1	Previo a la contratación	Para asegurarse de que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades, y son adecuados para las funciones que se consideran para, y para reducir el riesgo de robo, fraude o mal uso de las instalaciones.		
8.1.1	Roles y responsabilidades	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo dela oficina de RH	Aún no se han definido los requerimientos de los perfiles del personal relacionado con el SGSI.
8.1.2	Investigación del personal que va a ser contratado	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo dela oficina de RH	Aún no se han definido los requerimientos de los perfiles del personal relacionado con el SGSI.
8.1.3	Términos y condiciones laborales	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo dela oficina de RH	Aún no se han definido los requerimientos de los perfiles del personal relacionado con el SGSI.

Tabla 16 Declaración A4

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
8.2	Durante el empleo	Para asegurar que todos los empleados, contratistas y usuarios de terceras partes son conscientes de la información amenazas y preocupaciones, sus responsabilidades y obligaciones de seguridad, y están equipados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de error humano.		
8.2.1	Responsabilidades de las directivas	**i**mplementado parcialmente	Aún no se han aplicado.	Se debiera proporcionar a todos los usuarios empleados, contratistas y terceras personas un nivel adecuado de conocimiento, educación y capacitación en procedimientos de seguridad y uso correcto de los medios de procesamiento de información para minimizar los posibles riesgos de seguridad
8.2.2	Conciencia de la seguridad, educación y entrenamiento	No implementado	Aún no se han aplicado.	La capacitación y el conocimiento debieran comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios.
8.2.3	Procesos disciplinarios	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la oficina de RH	El proceso disciplinario formal debiera asegurar el tratamiento correcto y justo para los empleados sospechosos de cometer incumplimientos de la seguridad.
8.3	Terminación del contrato o cambio de empleo	Para asegurarse de que los empleados, contratistas y usuarios de terceras partes salen de una organización o el cambio de empleo de una manera ordenada.		

3.4 Plan de seguridad informática

A continuación, se especifica una lista general de controles que se derivan de la norma ISO 27001:2013, los cuales son aplicables a la mayoría de las organizaciones. Es importante tener en cuenta que, para establecer los controles adecuados, para lo cual se tendrá en cuenta la evaluación de riesgos realizada, de acuerdo a lo anterior, y con base en el diagnóstico y los riesgos identificados, se listan algunos controles que se pueden aplicar en la entidad.

Política de seguridad de la información: Definir una política que establezca los principios y objetivos de la seguridad de la información en la organización.

Evaluación de riesgos: Identificar, analizar y evaluar los riesgos de seguridad de la información que afectan a la Alcaldía.

Gestión de riesgos: Establecer un proceso para tratar y mitigar los riesgos identificados.

Asignación de responsabilidades: Definir las responsabilidades y roles de las personas involucradas en el manejo de la seguridad de la información que sean claras y orientada al complimiento de los objetivos de la Alcaldía.

Capacitación y concienciación: Implementar programas de formación y sensibilización al personal de la alcaldía generando en ellos conciencia sobre la seguridad de la información para el personal, por tal motivo se deben buscar las mejores estrategias.

Control de accesos: Se debe garantizar que el acceso a los sistemas de cómputo y datos relevantes para la alcaldía se cuente con usuarios autorizados y se controle de manera adecuada.

Gestión de activos: Identificar y mantener un inventario de activos de información y asegurar su protección, estos inventarios deben contar con un formato adecuado para cada

situación, por ejemplo, formato de inventario físicos de hardware, formato de inventario de software instalado en cada equipo de cómputo con sus respectivas actualizaciones o configuraciones.

Seguridad física y del entorno: Implementar controles para proteger los activos físicos y la infraestructura de TI, se debe contar con controles que evidencien la seguridad física y del entorno.

Control de operaciones: Establecer procedimientos y controles para asegurar el correcto funcionamiento de los sistemas de información, en dichos controles es importante mantener un plan de mantenimientos adecuados ya sean preventivos o correctivos tanto para hardware como para software.

Seguridad en el desarrollo de software: Implementar controles en el ciclo de vida del software para garantizar su seguridad, todo software desarrollado e implementado en la alcaldía debe contar y garantizar el ciclo de vida del software, así mismo el ciclo de visa seguro del software.

Gestión de incidentes de seguridad: Definir un proceso para la notificación y respuesta a incidentes de seguridad.

Cumplimiento legal y contractual: Asegurar que se cumplan los requisitos legales y contractuales relacionados con la seguridad de la información.

Continuidad del negocio y recuperación ante desastres: Establecer planes de contingencia para asegurar la continuidad de las operaciones en caso de eventos adversos.

Gestión de proveedores: Evaluar y gestionar la seguridad de los proveedores que tengan acceso a información sensible.

Auditorías internas y revisiones: Realizar auditorías periódicas para evaluar la eficacia de los controles y procesos implementados.

Es importante destacar que la implementación de los controles requerirá una colaboración entre los departamentos de TI y la alta dirección, así como una cultura organizacional orientada a la seguridad de la información. Además, se debe asegurar la revisión y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), del mismo modo es esencial que la alcaldía realice constantes evaluación de riesgos identificando los activos críticos, las amenazas según su nivel de riesgo, las vulnerabilidades específicas de su entorno, y, a partir de eso, diseñe un plan de implementación de controles adecuados.

De acuerdo a lo anterior, se puede definir un plan de seguridad de la información para la alcaldía municipal, que se sugiere se realice de forma anual y seguimiento trimestral, con la siguiente estructura:

1. **Evaluación de riesgos:**

- Identifica y clasifica los activos de información crítica (datos confidenciales, propiedad intelectual, registros financieros, etc.).
- Evalúa las amenazas potenciales que podrían afectar la seguridad de los datos (ciberataques, malware, robo, desastres naturales, etc.).
- Determina las vulnerabilidades presentes en tu infraestructura, sistemas y procedimientos.

2. **Políticas y procedimientos:**
    - Desarrolla políticas claras y directrices para el uso adecuado de los activos de información y el acceso a ellos.
    - Establece procedimientos para manejar incidentes de seguridad, como brechas o filtraciones.
    - Define las responsabilidades y roles de las personas que estarán involucradas en la implementación y seguimiento del plan.
3. **Acceso y control de la información:**
    - Implementa controles de acceso basados en roles y niveles de privilegios para garantizar que solo las personas autorizadas tengan acceso a la información confidencial.
    - Encripta datos sensibles tanto en tránsito como en reposo.
    - Implementa medidas de autenticación seguras, como autenticación multifactor (MFA).

4 **Capacitación y concienciación:**

- Capacitar a todos los empleados y contratistas sobre las mejores prácticas de seguridad de la información y los riesgos asociados.
- Fomenta una cultura de seguridad donde todos los miembros del personal estén comprometidos a proteger la información de la organización.

5 Monitoreo y detección:

- Instala soluciones de monitoreo de seguridad para detectar y prevenir ataques cibernéticos.
- Establece un sistema de alerta temprana para detectar y responder rápidamente a incidentes de seguridad.

6 Copias de seguridad y recuperación:

- Implementa un plan de respaldo regular y almacenamiento seguro para garantizar que los datos críticos se puedan recuperar en caso de pérdida o corrupción.
- Realiza pruebas periódicas de recuperación de datos para asegurarse de que el proceso funcione correctamente.

7 Cumplimiento normativo y legal:

- Asegúrate de cumplir con todas las leyes y regulaciones aplicables relacionadas con la protección de datos y la privacidad.
- Mantén actualizados tus sistemas y procesos para reflejar cualquier cambio en los requisitos legales.

8 Evaluación y mejora continua:

- Realiza auditorías y evaluaciones periódicas de seguridad para identificar áreas de mejora.
- Actualiza y mejora regularmente tu plan de seguridad de la información según las últimas amenazas y tecnologías.

4 Conclusiones

La norma ISO/IEC 27001 es un marco amplio y ampliamente aceptado para la gestión de la seguridad de la información, que puede ser utilizado por cualquier tipo de organización, independientemente de su tamaño o sector.

Al cumplir con la norma ISO/IEC 27001, se establecen procesos y medidas para proteger la confidencialidad, integridad y disponibilidad de la información de una organización. El proceso de cumplimiento de la norma ISO/IEC 27001 incluye la identificación y valoración de los activos de información, el establecimiento de un marco de seguridad de la información, la implementación de medidas de seguridad adecuadas y el monitoreo y evaluación del desempeño de la seguridad.

En la Alcaldía de la Jagua de Ibirico, todavía hay mucho desconocimiento, sobre normas de seguridad, se aplicó una herramienta tecnológica, que permitió realizar un diagnóstico. De igual manera, se diseñó un análisis de los riesgos, mediante la metodología Magerit, permitiendo tener un panorama más amplio de la forma como están manejando la seguridad de la información. Finalmente se definieron los controles a través de la Declaración de Aplicabilidad (SOA), de acuerdo con la norma ISO 27001:2013 y diseñando un plan de seguridad.

Cumplir con la norma ISO/IEC 27001 puede mejorar la confianza de los clientes, los socios y otros interesados en la organización, y puede ser un requisito para ciertas industrias o para cumplir con ciertas regulaciones.

Referencias

Alcaldia la Jagua de Ibirico. (Diciembre de 2022). *Alcaldia la Jagua de Ibirico- Cesar*. http://www.lajaguadeibirico-cesar.gov.co/

AMUTIO GÓMEZ, Miguel Ángel. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Madrid España), 2012. www.Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630- 12-171-8.pdf

APA. (s.f.). Normas APA. Obtenido de http://normasapa.com/formato-apapresentacion-trabajos-escritos/

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la investigación* . México: McGRAW-HILL.

Ibirico, A. l. (Diciembre de 2022). *Alcaldia la Jagua de Ibirico- Cesar*. Obtenido de http://www.lajaguadeibirico-cesar.gov.co/

SHRIVASTAVA, A., Kumar, A., Rai, A., Payal, N., & Tiwari, A. (2013). ISO 27001 compliance via Artificial Neutral Network. In computal intelligence and communication Network (CICN), (págs. 339-342).