

**DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA PARA
LA ALCALDIA MUNICIPAL DE LA JAGUA DE IBIRICO – CESAR BASADO EN
LA NORMA ISO 27001:2013**

MARTHA LUCIA BRIÑEZ BAUTISTA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CEAD VALLEDUPAR
LA JAGUA DE IBIRICO
2017**

**DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA PARA
LA ALCALDIA MUNICIPAL DE LA JAGUA DE IBIRICO – CESAR BASADO EN
LA NORMA ISO 27001:2013**

MARTHA LUCIA BRIÑEZ BAUTISTA

**Propuesta de grado para optar por el título de Especialista en Seguridad
Informática**

**ASESOR
HENRY ALDEMAR GUERRERO ERAZO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
CEAD VALLEDUPAR
LA JAGUA DE IBIRICO
2017**

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

DEDICATORIA

Dedico este trabajo a Dios, por llenarme de bendiciones y brindarme la capacidades para alcanzar un nuevo logro en mi vida.

A mis padres por el apoyo incondicional que me brindan durante el transcurso de mi carrera como profesional y próximamente como especialista, porque gracias al esfuerzo que hicieron, soy una persona de bien, con valores, principios y criterios razonables.

También Lo dedico a todos aquellos impulsores del Software Libre y el Código Abierto, que buscan una manera diferente de crear y transmitir el conocimiento, ya que gracias a ellos se pudo realizar y poner en práctica este proyecto.

AGRADECIMIENTO

Agradezco principalmente a Dios por darme su bendición y sabiduría cada día de mi vida, a mis padres José Ignacio Briñez y Cecilia Bautista por traerme a este mundo y por apoyarme en todas las metas que me he propuesto, a mis hermanos que han sido de gran apoyo, y a Henry morales por estar conmigo durante el proceso de este proyecto.

Agradezco, de igual manera a mi tutor de la universidad nacional abierta y a distancia UNAD CEAD Valledupar por compartir con nosotros su experiencia y conocimiento y quien me brindo toda su colaboración para poder llevar a cabo la culminación de este trabajo de grado.

TABLA DE CONTENIDO

	pág.
GLOSARIO	13
RESUMEN	16
INTRODUCCION	17
1. DESCRIPCION DEL PROBLEMA	188
1.2. FORMULACIÓN DEL PROBLEMA	18
2. OBJETIVOS	19
2.2. OBJETIVO GENERAL	199
2.3. 2OBJETIVOS ESPECÍFICOS	19
3. JUSTIFICACIÓN DEL PROYECTO	20
4. ALCANCE Y DELIMITACION DEL PROYECTO	22
4.1. ALCANCE	22
4.2. DELIMITACION	22
5. MARCO REFERENCIAL	23
5.1. ANTECEDENTES	233
5.2. MARCO CONTEXTUAL	244
5.3. MARCO TEORICO	277
5.3.1. Sistema de Gestión de la Seguridad de la Información SGSI.	277
5.3.1.1 Para qué sirven SGSI.	277
5.3.1.2 Implementación del sistema de gestión de seguridad informática.	27
5.3.2. Aplicación web.	33
5.3.3. Seguridad informática.	333
5.3.4. Seguridad de la Información.	333
5.3.5. Análisis de Riesgos Informáticos.	34
5.3.6. Control de riesgo.	35
5.3.6.1 Servicio de Seguridad.	35
5.3.6.2 Mecanismo de Seguridad.	35
5.3.7. NORMAS ISO/IEC 27000.	36
5.3.8. ¿Qué es una Declaración de Aplicabilidad?.	38
5.3.8.1 ¿En qué fase del proceso de gestión se sitúa el SOA?.	38
5.3.8.2 Características De Una Declaración De Aplicabilidad SOA.	38
5.4. MARCO CONCEPTUAL	399
5.4.1. Definiciones	40
5.5. MARCO LEGAL	40
6. MARCO METODOLOGICO	42

	pág.
6.1. METODOLOGIA DE INVESTIGACIÓN	42
6.1.1. Metodología cuantitativa.	42
6.1.2. Tipo de investigación.	42
6.2. METODOLOGÍA DE DESARROLLO	42
6.3. UNIVERSO Y MUESTRA	43
6.3.1. Universo o Población	43
6.3.2. Muestra	43
6.4. FUENTES DE INFORMACIÓN	43
6.4.1. Fuentes primarias.	43
6.4.2. Fuentes Secundarias.	43
7. RESULTADO A ENTREGAR	45
7.1. La Declaración de Aplicabilidad o SOA (Statement of Applicability)	45
7.2. Diseñar el análisis de riesgo mediante la metodología de Magerit	77
7.2.1. Inventario de activos	77
7.2.2. Identificación de amenazas.	83
7.2.3. Valoración de amenazas.	88
7.2.4. Resultado plan de pruebas.	97
7.2.5. Determinación del impacto.	105
7.2.5.1 Estimacion del riesgo.	106
7.3. CONTROLES EXISTENTES CON QUE CUENTA LA ENTIDAD	113
7.4. MANUAL DE POLÍTICA Y PROCEDIMIENTOS	113
7.4.1. Políticas de seguridad de recursos humanos.	113
7.4.2. Normas relacionadas con la vinculación de nuevos Empleados.	113
7.4.3. Personal provisto por terceras partes.	113
7.4.4. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros.	119
7.4.5. Políticas de control de cambios de datos.	1199
7.4.6. Normas relacionadas con el control de cambios de los datos.	119
7.4.7. Inventario de activos.	119
7.4.8. Política de Clasificación y Manejo de la Información.	120
7.4.9. Política de Gestión de copias de respaldo.	121
7.4.10. Normas para la Gestión de copias de respaldo.	121
7.4.11. Política de Control de acceso a áreas seguras.	122
7.4.12. Normas Control de acceso a áreas seguras.	122
7.4.13. Políticas de Desarrollo de aplicaciones.	123
7.4.14. Normas de Desarrollo de aplicaciones.	123

	pág.
7.4.15. Política De Seguridad De La Información.	124
7.4.16. Roles De Seguridad De La Información.	124
7.4.17. Políticas De Seguridad Y Privacidad De La Información.	124
7.4.18. Política De Teletrabajo.	124
7.4.19. Política Para Dispositivos Móviles.	125
7.4.20. Política Gestión De Activos.	12626
7.4.21. Política De Control De Acceso.	12726
7.4.22. Política Sobre El Uso De Controles Criptográficos	12827
7.4.23. Política De Escritorio Y Pantalla Limpia.	12827
7.4.24. Políticas De Seguridad Para Protección De Activos Informáticos.	12928
7.4.25. Clasificación de la información de la Empresa o de Terceros manejada Internamente	1298
7.4.26. Responsabilidad sobre los activos.	1298
7.4.27. Mantenimiento del Inventario de Activos de Información.	130
7.4.28. Manejo de Información Financiera.	130
7.4.29. Etiquetado de información.	130
7.4.30. Grabación periódica de datos por usuarios.	130
7.5. POLITICAS DE SEGURIDAD PARA LA ADMINISTRACIÓN DEL HARDWARE Y DEL PROCESAMIENTO DE LA INFORMACIÓN	130
7.5.1. Especificación de los requisitos para los nuevos equipos.	130
7.5.2. Instalación de nuevos equipos.	131
7.5.3. Prueba de equipos y sistemas.	131
7.5.4. Gestión y uso de documentación de hardware.	131
7.5.5. Desarrollo y Mantenimiento de Software Aplicativo.	131
7.5.6. Compra de Software Aplicativo Comercial.	131
7.5.7. Políticas De Seguridad De Las Aplicaciones Del Sistema	132
7.5.7.1. Validación de los datos de entrada	132
7.5.7.2. Control del proceso interno	132
7.5.7.3. Validación de los datos de salida	132
7.5.7.4. Uso de los controles criptográficos	132
7.5.7.5. Uso de técnicas de encriptación.	132
7.5.7.6. Firmas digitales.	132
7.5.7.7. Seguridad de los archivos del sistema	132
7.5.8. Políticas De Control De Acceso Lógico A La Información De Los Usuarios.	133
7.5.8.1. Asignación de identificador de usuario a nuevos empleados	133

	pág.
7.5.8.2. Privilegios de acceso.	133
7.5.8.3. Uso de contraseñas alfanuméricas de usuarios o de números.	133
7.5.8.4. Consideraciones para el manejo de clave de accesos.	133
7.5.8.5. Control de acceso al sistema operativo.	134
7.5.8.6. Aislamiento de sistemas sensibles o altamente confidenciales.	134
7.5.8.7. Seguimiento de accesos y usos del sistema.	134
7.5.8.8. Monitoreo de accesos y uso del sistema	134
7.5.8.9. Uso de equipos portátiles de cómputo	134
7.5.8.10. Difusión de las políticas a contratistas y trabajadores temporales	135
7.5.8.11. Brechas de confidencialidad de terceros.	135
7.5.9. Políticas Sobre Capacitación En Seguridad De La Información.	135
7.5.9.1 Capacitación en Seguridad de la Información a trabajadores.	135
7.5.9.2 Capacitación en Seguridad de la Información a personal nuevo.	135
7.5.9.3 Capacitación en Seguridad de la Información al personal técnico.	135
7.5.9.4 Respuesta ante incidentes y malos funcionamientos de la seguridad.	136
7.5.9.5 Reporte de incidentes de seguridad.	136
8. RECURSOS NECESARIOS	13737
9. CRONOGRAMA DE ACTIVIDADES	13838
10. CONCLUSIONES	13939
11. RECOMENDACIONES	14040
BIBLIOGRAFIA	141

LISTA DE TABLAS

	pág.
Tabla 1. Inventario de activos de información de tecnología	266
Tabla 2. Controles SOA	466
Tabla 3. Estados Controles SOA.	477
Tabla 4. Declaración De Aplicabilidad	488
Tabla 5. Activos con Magerit	777
Tabla 6. Identificación de amenazas en la Alcaldía de la Jagua de Ibirico.	83
Tabla 7. Escala de Rango de frecuencia de amenazas.	888
Tabla 8. Dimensiones de seguridad	888
Tabla 9. Escala de Rango porcentual de impactos en los activos	899
Tabla 10. Metodología Magerit.	90
Tabla 11. Vulnerabilidades y riesgos inicialmente identificados	977
Tabla 12. Nivel de degradación.	105
Tabla 13. Probabilidad de Ocurrencia	106
Tabla 14. Valoración del riesgo.	106
Tabla 15. Implementación de la valoración del riesgo en la Alcaldía	107
Tabla 16. Clase y estimación de riesgo	1077

	pág.
Tabla 17. Evaluar controles	113
Tabla 18. Valoración de controles	114
Tabla 19. Recursos Humanos	13737
Tabla 20. Recursos Tecnológicos	13737
Tabla 21. Cronograma de Actividades	13738

LISTA DE FIGURA

	pág.
Figura 1. Organigrama Oficina de las TIC.	255
Figura 2. Sistema De Gestión De La Seguridad Informática	277
Figura 3. Utilidad de un SGSI	288
Figura 4. Ciclo PDCA	299
Figura 5. Dominios ISO 27001:2013.	377
Figura 6. Página web de la Alcaldía de la Jagua de Ibirico.	988
Figura 7. Instalación del scanner Nessus.	999
Figura 8. Pruebas de vulnerabilidad web	999
Figura 9. Resultado de las pruebas de vulnerabilidad web	100
Figura 10. Ejecución de pruebas con Nmap.	103
Figura 11. Resultados arrojadas Nmap	104
Figura 12. Versión servicios Nmap.	104
Figura 13. Escaneos de puertos con Nmap	105

GLOSARIO

ACTIVOS: Son aquellos recursos (hardware/software), que tiene explota una empresa.

APLICACIÓN WEB: aquellas herramientas que los usuarios pueden utilizar accediendo a un servidor web a través de Internet o de una intranet mediante un navegador.

AMENAZA: Una amenaza informática es un posible peligro del sistema.

ATAQUE: es un método por el cual un individuo intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

AUDITORIA INFORMATICA: La auditoría informática es un proceso que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

CONFIDENCIALIDAD: La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

CONTRASEÑAS: Una contraseña o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso.

DATOS: El dato es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa.

DEBILIDAD: Las debilidades se refieren a todos aquellos elementos, recursos, habilidades y actitudes que la empresa ya tiene y que constituyen barreras para lograr la buena marcha de la organización.

DISPONIBILIDAD: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

ESTANDARES DE SEGURIDAD INFORMATICA: son herramienta que apoya la gestión de la seguridad informática, por medio de modelos que administren las tecnologías de manera integral.

FALLOS: Es un estado o situación en la que se encuentra un sistema formado por dispositivos, equipos, aparatos y/o personas en el momento que deja de cumplir la función para el cual había sido diseñado.

IMPACTO: son las consecuencias de una o más amenazas sobre los activos, es decir los daños causados.

INTEGRIDAD: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

ISO/IEC 27000: Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación.

ISO/IEC 27001: Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

NAVEGADOR WEB: es un software que permite el acceso a Internet, interpretando la información de archivos y sitios web para que éstos puedan ser leídos.

OWASP: El proyecto OWASP (Open Web Application Security Project) es un proyecto abierto dedicado a la seguridad en aplicaciones web. Consiste en una comunidad a nivel mundial enfocada en la mejora de la seguridad en las aplicaciones de software.

PAGINAS WEB GUBERNAMENTALES: son sitios web pertenecientes a Entidades Públicas colombianas que se deben encontrar alineados con las políticas de la Agenda de Conectividad y el Programa Gobierno En Línea.

POLÍTICA DE SEGURIDAD: Toda intención y directriz expresada formalmente por la Dirección, Su objetivo es proporcionar a la gerencia la dirección y soporte para la seguridad de la información, en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

PROTOCOLO DE SEGURIDAD: Un protocolo de seguridad define las reglas que gobiernan estas comunicaciones, diseñadas para que el sistema pueda soportar ataques de carácter malicioso.

PRUEBAS DE INTRUSION (PENTEST): sistemas de información de una organización (ya sea una red, sistema y/o aplicación) con el objetivo de determinar su nivel de seguridad y, por tanto, el grado de acceso que tendría un atacante con intenciones malintencionadas en los mismos.

RIESGO: es el grado de pérdidas esperadas, debido a la ocurrencia de un suceso particular y como una función de la amenaza y la vulnerabilidad

SERVIDOR WEB: es un programa informático que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente.

SEGURIDAD INFORMATICA: La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

SGSI: Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información.

TICs: Las Tecnologías de la Información y la Comunicación.

RESUMEN

Los sistemas de información están expuestos cada vez a un mayor número de amenazas que constituyen un riesgo sobre uno de los activos más críticos y vulnerables de las organizaciones como la información.

Asegurar la disponibilidad, la confidencialidad y la conservación de los datos, es un servicio que debe brindar la organización por lo que la gestión de la seguridad de la información debe realizarse mediante un proceso documentado y conocido.

Este proyecto describe un diseño metodológico para la implementación de un sistema de seguridad de la información SGSI en la alcaldía municipal de la jagua de ibirico cesar que garantice el nivel de seguridad y permita obtener la certificación ISO/IEC 27001:2013. Finalmente, se concluye que la seguridad es un proceso de implantación que exige un cambio cultural y organizativo en las empresas.

La implementación de un SGSI es una opción fundamental cuando se trata de proteger la información, ya que este tiene como objetivo esencial proteger dicho activo a través de controles y políticas de seguridad que deben ser aplicadas en una organización en cabeza de la gerencia.

Palabras Clave: Sistema de gestión de seguridad informática (SGSI), metodología de Magerit, Seguridad informática, Tics.

INTRODUCCION

Lo más importante con que cuenta una organización es su información, de esta manera mantenerla segura es una tarea ardua para cualquier empresa, los beneficios que le pueden generar a sus clientes son muchos; puesto que dicha organización debe ser segura, confiable y satisfactoria. El estar en la evolución de la tecnología, el solo hecho de compartir información a diario a través de los diferentes sistemas tecnológicos y electrónicos es una necesidad pero también convierte la información en un activo vulnerable por lo tanto cada organización asume el reto de proteger su activo máspreciado.

La seguridad es un proceso que debe ser vigilado, gestionado y monitoreado para que pueda ser utilizado como una estrategia de seguridad de la información para proteger sus datos e información tomando como base fundamentado en la norma ISO/IEC 27001

Por lo anterior se debe hacer un análisis más profundo, y determinar si la información que se cuenta esta segura, para que de esta manera se puede evitar posibles problemas de vulnerabilidad que cause la perdida de la información confidencial, por lo tanto no se puede dejar de hablar de la seguridad, ya que a partir de ella se puede tener una base más concreta y alcanzar un mayor beneficio, sin afectar la información.

Una vez identificado claramente los activos que se encuentran en riesgo y que generarían mayor impacto en caso de sufrir un ataque, se procede a definir políticas de seguridad, la declaración y aplicabilidad de los controles, para cada uno de estos activos teniendo en cuenta lo expuesto por la Norma ISO/IEC 27001. Para cumplir el objetivo fundamental del SGSI que es proteger la información y disminuir los riesgos.

1. DESCRIPCION DEL PROBLEMA

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, por lo cual cuenta con diferentes medidas que se realizan con el único fin de mejorar la Seguridad de la Información en la entidad, pero existen situaciones internas que demoran dichos avances y es el no tener un sistema de información que mitigue los riesgos, otro punto es que algunos funcionarios de la entidad no tiene sentido de pertenecía, ni de conciencia en temas de seguridad, que piensan de que este tipo de información no es impórtate para sus departamentos.

La alcaldía no cuenta con sistema de información adecuado, lo que entorpece establecer el estado actual de seguridad, información de los funcionarios, procesos y tecnología, y de esta manera no se ve reflejado una planeación e identificación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

También hay que mencionar que se realiza publicaciones periódicas de todo lo relacionados noticias, eventos etc, dichas publicaciones en un corto tiempo desaparecen, sin que las personas a cargo de alimentar o actualizar la página, borren dicha información.

De acuerdo con lo anterior es necesario diseñar una metodología para la implementación de un sistema de gestión de la seguridad de la información SGSI, teniendo en cuenta la norma ISO 27001, para garantizar su disponibilidad, integridad y confidencialidad.¹ Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información por la organización, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo Un Sistema de Gestión de Seguridad de la Información le proveerá a la alcaldía municipal de la jagua de Ibirico, mejorar la seguridad de la información de

¹ <http://www.iso27000.es/iso27000.html>

la entidad y la gestión de los riesgos asociados al uso de la información?

2. OBJETIVOS

2.2. OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad informática de la alcaldía de La Jagua de Ibirico mediante la aplicación con la norma ISO 27001:2013

2.3. 2OBJETIVOS ESPECÍFICOS

- Describir mediante la Declaración de Aplicabilidad (SOA) la situación actual de la alcaldía municipal de la jagua de Ibirico.
- Diseñar el análisis de riesgo mediante la metodología de MAGERIT de la alcaldía municipal de la jagua de Ibirico.
- Identificar los controles existentes con que cuenta la entidad con la norma ISO 27001:2013.
- Definir un manual de política y procedimientos a seguir en pro de mitigar posibles amenazas en los recursos informáticos de la alcaldía.

3. JUSTIFICACIÓN DEL PROYECTO

Las tecnologías de información y comunicación en conjunto con el internet han abierto sin números de posibilidades al acceso a la información, manejando un único objetivo y es el de salvaguardar la privacidad de la información obtenida a través de los sistemas, al igual que han ofrecido muchos beneficios ha estado expuesto a nuevos riesgos que abarcan la seguridad de la misma. ²

En la actualidad las empresas u organizaciones de cualquier tipo deben tener en cuenta dentro de su plan la protección de la información, la creación de políticas y controles, en busca de que garanticen la información actual y la de un futuro, de esta manera contar con un sistema seguro libre de riesgos que se puedan convertir en posibles amenazas.

La seguridad de los sistemas informáticos se basa prácticamente en políticas³ bien fijadas y usuarios precavidos, puesto que a la hora del acceso a los entornos informáticos se ha comprobado que los usuarios finales son los más atacados por parte los hackers.

La aplicación de niveles de seguridad, es un factor diferenciador, y claro generador de confianza con un valor incalculable para las empresas, puesto que hoy en día, los servidores web deben ser seguros frente a cualquier tipo de amenazas y estar preparados de cualquier riesgo que se pueda presentar a un futuro.

Para esto es vital contar con herramientas donde se indiquen las maneras de ejecutar acciones que permitan resguardar la información y se eviten vulnerabilidades en la misma y de esta manera determinar el nivel de calidad y seguridad de la página web y de toda la información tangible e intangible de la administración municipal, para así generar recomendaciones que sean viables.

² <http://aprendeonline.udea.edu.co/lms/investigacion/mod/page/view.php?id=3118>

³ <http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Infom%C3%A1tica-2013-GI.pdf>

Es pertinente e importante realizar este estudio puesto que la identificación de amenazas y vulnerabilidades que comprometan la confidencialidad, integridad y disponibilidad del sitio web de la alcaldía municipal, permitirá determinar qué tipo de riesgos tiene y que recomendaciones se puede entregar para no sufrir ataques.

Hasta el momento no se han presentado dificultades referentes a ataques, solo el hecho de que algunas publicaciones de noticias o eventos se borran, sin que la persona administradora lo realice, de esta manera el riesgo puede ser inminente y estas falencias pueden traer inconvenientes desastrosos, puesto que la página web de la alcaldía se publica toda la información del municipio en tiempo real, lo que puede concluir que la información puede ser robada, manipulada, o modificada para fines delictivos.

Por lo anteriormente expuesto es de suma importancia el diseño de un SGSI para el área de informática bajo la norma ISO/IEC 27001 que permita obtener una visión global del estado de los sistemas de información y observar claramente las medidas de seguridad a aplicar para prevenir futuros incidentes.

4. ALCANCE Y DELIMITACION DEL PROYECTO

4.1. ALCANCE

El alcance del proyecto se centra en el diseño un Sistema de Gestión de Seguridad de la información para la alcaldía del municipio de la Jagua de Ibirico. Para el desarrollo del proyecto se utilizará como guía principal la norma NTC-ISOIEC 27001 versión 2013. Y de esta manera definir políticas que mitiguen riesgos.

Este proyecto puede adaptarse entidades públicas prestadoras de servicios siendo una guía para otras alcaldías, atendiendo a nuevos requerimientos.

4.2. DELIMITACION

El proyecto se realizara en la alcaldía municipal de la Jagua de Ibirico - Cesar durante el año 2017.

5. MARCO REFERENCIAL

5.1. ANTECEDENTES

En la actualidad administrar la información, representa un factor importante para la seguridad informática, puesto que por medio del uso de herramientas de penetración, esto posibilita la detección de riesgos y vulnerabilidades de los cuales se encuentran expuestos los sistemas, esto con el único fin de proteger la disponibilidad, confidencialidad e integridad de los datos.

Hoy en día existen muchos planteamientos e inconvenientes de seguridad para la información como virus, acceso no autorizado, contraseñas vulnerables, descuido del personal humano, y el no salvaguardar la información entre otras, mas sin embargo es un problema posible de solucionar, ya que desde un tiempo atrás se han estado desarrollando procesos que puedan cifrar los datos, como el cambio periódico de contraseñas, capacitaciones al equipo de personal, manejo de memorias extraíbles, copias de seguridad y el uso continuo de antivirus.

Estos antecedentes son utilizados para conocer los temas sobre mecanismos de seguridad informática, fundamentándose en herramientas de escaneo de vulnerabilidades de Linux, donde se detectan y se dan recomendaciones que sirvan para posibles riesgos del sistema.

Es de importancia conocer los comandos utilizados y las herramientas para evaluar la seguridad informática, los ingenieros Jesús Cifuentes y Cesar Narváez (2004), de la Universidad del Valle, por la tesis “Manual de Detección de Vulnerabilidades de Sistemas Operativos Linux y Unix en Redes TCP/IP”⁴, tienen como objetivo dar a conocer los conceptos básicos de redes y sistemas operativos, y de igual manera mostrar los diferentes mecanismos de seguridad existentes esto con el fin de proteger la información y contrarrestar los posibles ataques informáticos, esto permitirá explicar los conceptos y comprender la importancia que tiene cada uno de los comandos mencionados en la evaluación de la seguridad de sistemas de información

⁴ <http://docplayer.es/507322-Manual-de-deteccion-de-vulnerabilidades-de-sistemas-operativos-linux-y-unix-en-redes-tcp-ip-jesus-herney-cifuentes-cesar-augusto-narvaez-b.html>

Como los ataques a los diferentes sistemas van en crecimientos, la seguridad del mismo modo aumenta, ya sea por conseguir el control de los mismos, o solo el de denegar el servicio, El ingeniero Andrés Cárdenas (2011), de la Universidad Carlos III de Madrid, por la tesis “Desarrollo de un Entorno para Prácticas de Seguridad Informática”⁵, tiene como objetivo la creación y desarrollo de un entorno controlado para la ejecución de exploits, que permita con total libertad sin afectar los sistemas que lo soportan, permite conocer varias técnicas para la protección de la información.

La seguridad cuenta con unos elementos como son los análisis de riesgos y de recomendaciones utilizado para proteger la información, la ingeniera Hina Garavito (2015), de la Universidad Nacional Abierta y a Distancia, con su tesis “Análisis y Gestión del Riesgo de la Información en los Sistemas de Información Misionales de una Entidad del Estado, Enfocado en un Sistema de Seguridad de la Información”⁶, como objetivo primordial la realización de un análisis de seguridad informática que permita determinar los tipos de riesgos a los cuales están expuestos los sistemas de información misional, donde se da a conocer las distintas herramientas utilizadas en el momento de recolección de vulnerabilidades.

5.2. MARCO CONTEXTUAL

El municipio de la jagua de Ibirico fue creado en el año de 1979 por ramón Ibirico, Está a 125 kilómetros de la capital departamental, Valledupar. En 1985 empieza a realizarse la actividad económica más importante es la explotación de carbón, siendo uno de los grandes centros mineros de Colombia. Es el segundo municipio que tiene más garbón en Colombia, tiene 42.000 habitantes donde su principal fuente de empleo son las minas de garbón.

En año 2008 El Programa Gobierno en línea, del Ministerio de Tecnologías de la Información y las Comunicaciones, tiene por objeto contribuir a la construcción de un Estado más eficiente, más transparente y participativo y que preste mejores servicios mediante el aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC),⁷ esta estrategia tenía el reto de desarrollar plantillas

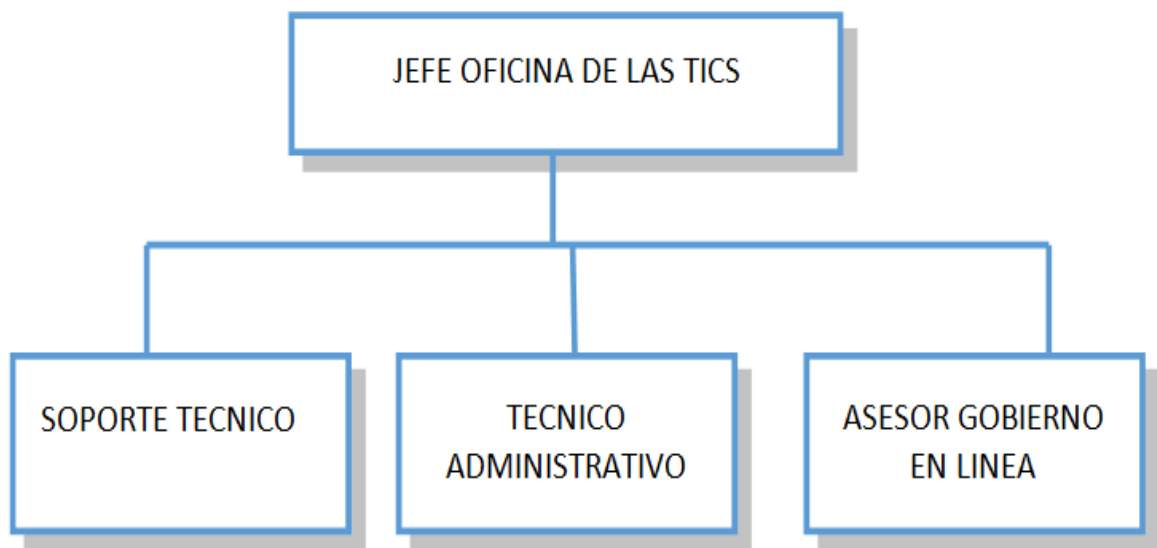
⁵ http://e-archivo.uc3m.es/bitstream/handle/10016/13161/MemoriaPFC_Andres_Cardenas_Parra.pdf?sequence=1

⁶ <http://docplayer.es/744621-Hina-luz-garavito-robles.html>

⁷ http://estrategia.gobiernoenlinea.gov.co/623/articulos-7941_manualGEL.pdf

estáticas inmodificables para sitios web pertenecientes a Entidades Públicas colombianas deben encontrarse alineados con las políticas de la Agenda de Conectividad y el Programa Gobierno En Línea; en base a esto se tiene el conocimiento y la experiencia para la creación de páginas que cumplan estas normativas establecidas.

Figura 1. Organigrama Oficina de las TIC.



Fuente. Alcaldía Municipal de la jagua de Ibirico

Este proyecto se aplicó en el sitio web del municipio de la jagua de Ibirico, este sitio es un plantilla inmodificable que fue asignada por el ministerio de las tecnologías tics y la estrategia de gobierno en línea con el único fin de tener un Estado más eficiente, más transparente y participativo y que preste mejores servicios mediante el aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC).

Tabla 1. Inventario de activos de información de tecnología

No	Cantidad	Nombre del Activo	Tipo de Activo
A1	1	Servidor Financiero PCT	Equipos Informaticos
A2	1	Servidor industria y comercio	Equipos Informaticos
A3	1	Servidor nativos digitales SAGEP	Equipos Informaticos
A4	1	Servidor de BACKUP	Equipos Informaticos
A5	70	Equipo de cómputo de escritorio	Equipos Informaticos
A6	5	Portátiles	Equipos Informaticos
A7	30	Impresoras laser	Equipos Informaticos
A8	3	Impresoras de inyección	Equipos Informaticos
A9	1	Plotter	Equipos Informaticos
A10	29	Windows 7	Sistemas Operativos
A11	18	Windows 8	Sistemas Operativos
A12	7	Windows vista	Sistemas Operativos
A13	3	Windows server	Sistemas Operativos
A14	13	Windows 10	Sistemas Operativos
A15	3	Switches capa 3 con 48 puertos	Redes de comunicaciones
A16	1	router mikrotic	Redes de comunicaciones
A17	1	FIBRA MONO MONO -Transiver	Redes de comunicaciones
A18	1	PCT	Software
A19	1	ZAFIRO	Software
A20	1	SIRCC	Software
A21	1	BDAU	Software
A22	1	SIVIGILA	Software
A23	1	SIPUC	Software
A24	1	SAGEP	Software
A25	1	NOM90	Software
A26	1	RYH	Software
A27	75	Antivirus nod 32	Software
A28	70	Office 2013	Software
A29	1	Sistema Gestor Base de Datos Oracle 11g	Software

Fuente propia.

5.3. MARCO TEORICO

5.3.1. Sistema de Gestión de la Seguridad de la Información SGSI. Un sistema de gestión de la seguridad informática SGSI, se basa en un contexto básico y es que la información es un conjunto de datos establecidos por la entidad de gran valor para esta. La seguridad de la información –según ISO 27001, se basa en protección de sus datos mediante la confidencialidad, integridad y disponibilidad una regla simple dentro de una organización⁸.

Figura 2. Sistema De Gestión De La Seguridad Informática



Fuente: www.iso27000.es

5.3.1.1. Para qué sirven SGSI: Los activos son muy importante para una organización ya que la información, junto a los procesos y sistemas son la base para tenerla de una manera confidencial, integral y disponible.

Cada vez es más elevado el nivel de amenazas en las organizaciones y sus sistemas de información, están expuestos a vulnerabilidades existentes, los cuales pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos,

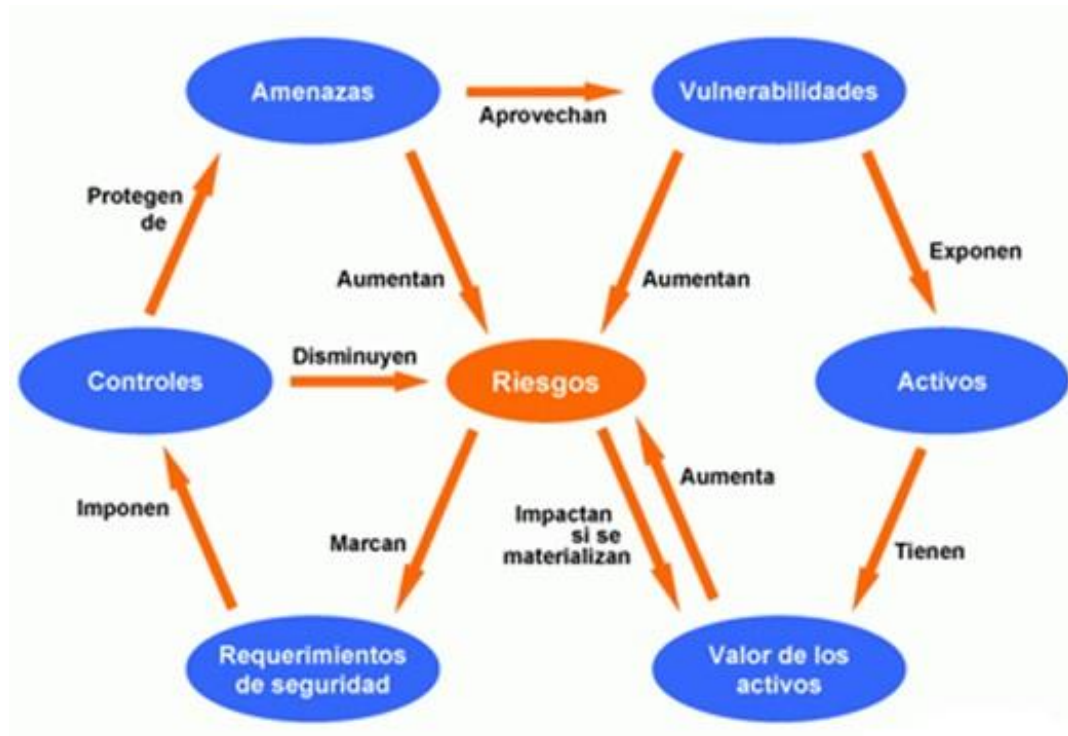
⁸ <http://studylib.es/doc/2091555/ec--especializaci%C3%B3n-en-gesti%C3%B3n-integrada-qhse--1070954687.pdf>

pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI⁹, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Figura 3. Utilidad de un SGSI



Fuente: www.iso27000.es

⁹ http://www.iso27000.es/download/doc_sgsi_all.pdf

5.3.1.2. Implementación del sistema de gestión de seguridad informática.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

- **Plan (planificar):** establecer el SGSI.
- **Do (hacer):** implementar y utilizar el SGSI.
- **Check (verificar):** monitorizar y revisar el SGSI.
- **Act (actuar):** mantener y mejorar el SGSI

Figura 4. Ciclo PDCA



Fuente: www.iso27000.es

• **PLANEAR: Establecer el SGSI**

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

- Definir una política de seguridad que: Incluya el marco general y los objetivos de seguridad de la información de la organización; considere requerimientos legales o contractuales relativos a la seguridad de la información.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.
- Identificar los riesgos: Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios; identificar las amenazas en relación a los activos; identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas; identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Analizar y evaluar los riesgos: Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información; evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados; estimar los niveles de riesgo; determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para: Aplicar controles adecuados; aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos; evitar el riesgo.
- **HACER: Implementar y utilizar el SGSI**
- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- **VERIFICAR: Monitorizar y revisar el SGSI**
 - Ejecutar procedimientos de monitorización y revisión para: Detectar a tiempo los errores en los resultados generados por el procesamiento de la información; identificar brechas e incidentes de seguridad; ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto; detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores; determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
 - Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
 - Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
 - Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles

cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

- **ACTUAR : Mantener y mejorar el SGSI**

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.
- PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

5.3.2. Aplicación web. Una aplicación web es un tipo especial de aplicaciones **cliente/servidor** donde tanto el cliente (el navegador, explorador) como el **servidor web** y el protocolo mediante lo que se comunica **HTTP** están estandarizado y no han de ser creados por el programador de aplicaciones¹⁰.

El servidor web tiene la función de permanecer a la espera de peticiones HTTP de los clientes, que suelen llevarlas a cabo a través de un navegador web. Los clientes realizan peticiones HTTP al servidor, y éste les responde con el/los contenido/s que los clientes solicitan, aunque también se puede configurar el servidor para que no permita más de un cliente simultáneamente.

Las aplicaciones Web son instrumentos indispensables para difundir la información, así como la explotación de otros mercados y de servicios antes impensables como el comercio electrónico a los usuarios por medio de la utilización de la red. Por este motivo se ha ampliado la necesidad de publicar información en la Web, además siempre es necesario que dicha información esté disponible en tiempo real.¹¹

5.3.3. Seguridad informática. La seguridad Informática, es una disciplina que se encargara de la implementación de técnicas sobre la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.¹²

5.3.4. Seguridad de la Información. La seguridad de la información¹³ En los últimos años la seguridad informática comenzaron a expandirse a otras áreas no solo al ente informático si no otros ligados con la información, lo cual trascendió fronteras de la informática, engrandeció de gran manera su responsabilidad y constituyó el nuevo concepto de seguridad de la información.

¹⁰ Sergio Lujan, libro (online), capítulo 4, Programación de aplicaciones web: historia, principios básicos y clientes web

¹¹ <http://www.internetya.co/ventajas-y-beneficios-de-las-aplicaciones-web/>

¹² Jeimy J. Cano, Ph.D., CFE. <https://co.linkedin.com/in/jeimy-cano-ph-d-cfe-3aa253>

¹³ BENCHIMOL, Daniel. Hacking COLECCIÓN: desde Cero (Buenos Aires Argentina), 2011.

Esto se basa en que la información va mucho más allá que determinar equipos informáticos y sistemas. Algunos temas no relacionados directamente con la informática, pero sí con la información, La seguridad de la información se podría definir como el nivel o grado de seguridad que tiene mi información, lo cual se podrá decir que si la información está segura de peligro, daño o riesgo, o por el contrario que es vulnerable y se puede convertir en una amenaza.

Determinar un nivel total de protección de la seguridad de la información es prácticamente imposible porque no existe un sistema ciento por ciento seguros. Puesto que hay distintos tipos de datos ya sea impresa o escrita en papel, almacenada electrónicamente o transmitida por correo etc, este tipo de datos lo hace estar expuesta a un mayor nivel de amenazas y vulnerabilidades.

Cada día más las entidades y sus sistemas de información están expuestos a riesgos cada vez más comunes, ya sean fraudes informáticos, espionaje, sabotaje, vandalismo, incendios, daños como virus informáticos, ataques de intrusos.

La seguridad de la información es importante para sector público para proteger las infraestructuras críticas. La seguridad de información permitirá, lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes.

5.3.5. Análisis de Riesgos Informáticos. El análisis de riesgos determina impactos¹⁴ y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra).

Según Alberto Cancelado Gonzales¹⁵ “El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidades de pérdidas. Así mismo determina que existen tipos de riesgos relacionados con la informática:

¹⁴ AMUTIO GÓMEZ, Miguel Ángel. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Madrid España), 2012.

¹⁵ CANCELADO GONZÁLEZ, Alberto. Administración de riesgos en tecnología informática (España), 2003.

Riesgos de Integridad: (Personas y procesos) este tipo de riesgos se centra con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización

Riesgos de relación: este riesgo se basa en datos correctos de una persona/proceso/sistema con el tiempo preciso y así tomar decisiones correctas.

Riesgos de acceso: Estos riesgos se enfocan al inadecuado acceso a sistemas, datos e información. Y están asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información.

Riesgos de utilidad: Estos riesgos se enfocan en tres diferentes niveles de riesgo: el primero en direccionamiento de sistemas antes de que los problemas ocurran, el segundo Técnicas de recuperación/restauración y Backups y el tercero en planes de contingencia controlan desastres de la información.

Riesgos en la infraestructura: Estos riesgos se refieren a que en las entidades no existe una estructura de información tecnológica (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras.

Riesgos de seguridad general: proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo

5.3.6. Control de riesgo. Una vez se ha realizado el análisis de riesgo tiene que determinar cuáles serán los servicios necesario para conseguir un sistema de información seguro

5.3.6.1. Servicio de seguridad

- **Integridad:** asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido de los mensajes ¹⁶
- **Confidencialidad:** proporciona protección de datos y de la información contra la revelación deliberada de la comunicación.

¹⁶ <https://infosegur.wordpress.com/tag/integridad/>

- **Disponibilidad:** permitir que la información esté disponible cuando sea por personas autorizadas.
- Autenticación: el sistema debe ser capaz de verificar que usuario puede ingresar y cual no, por medio de la realización de una autenticación.
- **Control de acceso:** podrán acceder al sistema solo personal y usuario autenticado.¹⁷

5.3.6.2. Mecanismo de seguridad. Los mecanismos de seguridad son también llamadas herramientas de seguridad y son todos aquellos que permiten la protección de los bienes y servicios informáticos.

- **Preventivos:** son aquellos cuya finalidad consiste en prevenir la ocurrencia de un ataque informático. se concentran en el monitoreo de la información y de los bienes.
- **Detectores:** Son aquellos que tienen como objetivo detectar todo aquello que pueda ser una amenaza para los bienes.
- **Correctivos:** se encargan de reparar los errores cometidos o daños causados una vez que se ha cometido un ataque.¹⁸

5.3.7. NORMAS ISO/IEC 27000. La familia de las normas ISO/IEC 27000, se basa en marcos ya sea de referencia o de seguridad a nivel mundial que proporcionan un lineamiento y se fundamenta en la utilización de mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización.

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas. Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales serán el marco teórico que se tendrá en cuenta para efectos del presente trabajo:

¹⁷ <https://infosegur.wordpress.com/tag/integridad/>

¹⁸ Ibid., p.34

- **ISO/IEC 27000.** Esta norma proporciona una visión general de los sistemas de gestión de seguridad de la información y contiene los términos y definiciones que se utilizan en las diferentes normas de la 27000.
- **ISO/IEC 27001.** La última versión de esta norma fue publicada a finales del 2013, contiene los diferentes requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en las organizaciones independiente de su tipo, tamaño o naturaleza. Esta norma incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización.

Los dominios de la norma ISO/IEC 27001:2013¹⁹ corresponde a los diferentes capítulos que establecen los requerimientos que las organizaciones deben cumplir para el establecimiento de un Sistema de Gestión de Seguridad de la Información, los cuales se resumen a continuación:

Figura 5. Dominios ISO 27001:2013.

ISO 27001:2013 (14 dominios, 113 Controles)	
A.5	Política de seguridad.
A.6	Organización de la seguridad de la información
A.7	Seguridad de los RRHH.
A.8	Gestión de activos.
A.9	Control de accesos.
A.10	Criptografía.
A.11	Seguridad física y ambiental.
A.12	Seguridad en las operaciones.
A.13	Transferencia de información.
A.14	Adquisición de sistemas, desarrollo y mantenimiento.
A.15	Relación con proveedores.
A.16	Gestión de los incidentes de seguridad.
A.17	Continuidad del negocio.
A.18	Cumplimiento con requerimientos legales y contractuales.

Fuente. <http://www.iso.org>

¹⁹ http://www.iso.org/iso/catalogue_detail?csnumber=54534

ISO/IEC 27002. Guía de buenas prácticas en seguridad de la información que describe de forma detallada las acciones que se deben tener en cuenta para el establecimiento e implementación de los objetivos de control y controles descritos de una forma general en el Anexo A de la norma ISO 27001.

ISO/IEC 27003. Guía que contiene aspectos necesarios para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001, donde se describe el proceso desde la planeación hasta la puesta en marcha de planes de implementación²⁰

5.3.8. ¿Qué es una declaración de aplicabilidad? La Declaración de Aplicabilidad o SOA²¹ por las siglas en inglés (Statement of Applicability) 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 esto la organización debe seleccionar aquellos que debe implantar y mantener en su sistema²².

Según el Anexo A suele ser utilizado como una referencia para la implementación de medidas de protección de la información, y de esta manera poder comprobar que no se están dejando de lado medidas de seguridad necesarias que no habían sido consideradas dentro de una organización.

5.3.8.1. ¿En qué fase del proceso de gestión se sitúa el SOA? La Declaración de Aplicabilidad se desarrolla luego del tratamiento de riesgos, este tiene como objetivo la definición de las acciones a realizar para mitigar aquellos riesgos que han sido identificados y analizados. Las opciones de tratamiento de riesgos se pueden agrupar en:

- **Mitigar:** Consiste en implementar algún control que reduzca el riesgo.
- **Transferir:** Ocurre cuando se delega la acción de mitigación a un tercero.

²⁰ <http://www.iso27000.es/iso27000.html>

²¹ <http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf>

²² <http://docplayer.es/11036766-Diseno-de-un-sistema-de-gestion-de-seguridad-de-la-informacion-para-una-entidad-financiera-de-segundo-piso.htm>

- **Aceptar:** Se presenta cuando el impacto generado por un riesgo es suficientemente bajo para que la organización decida no tomar ninguna acción de mitigación o cuando el costo de la aplicación de un control supera el valor del activo.

Una vez que se han definido las opciones de tratamiento para los riesgos, la organización debe aplicar medidas de seguridad, es decir, decidir de qué manera serán mitigados los riesgos.

5.3.8.2. Características de una declaración de aplicabilidad SOA. El SOA puede encontrarse en el formato que más convenga a una organización; lo relevante es su contenido, que en general debe incluir los objetivos de control y controles seleccionados del estándar, las razones por las cuales han sido seleccionados y medidas de seguridad adicionales si es el caso.

También, debe indicar si los objetivos de control y controles se encuentran implementados y operando, los que hayan sido descartados, así como una justificación del porqué algunas medidas han sido excluidas (las que son innecesarias y la razón del porqué no son requeridas en una organización).

Los controles indicados en la Declaración de Aplicabilidad pueden ser seleccionados debido a distintas razones, por ejemplo, como resultado de una evaluación de riesgos, si se debe cumplir con algún requisito legal, obligaciones adquiridas por contratos o regulaciones, nuevos requisitos del negocio, mejores prácticas a utilizar, entre otras.

Posteriormente, la selección de controles de seguridad deriva en la creación de un plan de tratamiento de riesgos, principalmente para la definición de las actividades necesarias para la aplicación de los controles de seguridad, que hayan sido seleccionados y que no se encuentran implementados.

5.4. MARCO CONCEPTUAL

A medida que avanza el tiempo, los medios tecnológicos, han hecho que aparezcan nuevos ataques y nuevas formas de delito que han vuelto el internet objetivos principales de hacker para cualquier tipo de red y organización o personas que tengan equipos conectados a internet. Actualmente se ha ido desviando completamente y dando origen a nuevos personajes que usan los

medios informáticos y su conocimiento con ayuda de herramientas para delinquir y obtener beneficios económicos.

5.4.1. Definiciones

Vulnerabilidad: Son las debilidades de un sistema informático que pueda permitir el ingreso de amenazas que pueda causar daños y pérdida en una organización, Por lo tanto Las vulnerabilidades son fallas en los sistemas ya sean por una mala instalación o configuración, por la falta de capacitación del personal con los recursos del sistema, también por equipos de cómputo donde los programas y herramientas no son seguras para la información.

Amenaza: se considera un suceso de manera accidental o intencional de cualquier tipo que pueda causar algún daño en el sistema informático a una entidad u organización.

Impacto: es la consecuencia de una amenaza

Ataque: es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

Activo: Son aquellos recursos (hardware/software), que tiene una empresa. También son los elementos hardware, como los equipos de computos que tiene y que pone a disposición de sus usuarios para poder realizar el trabajo diario.

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información. Sistema de Gestión de Seguridad de la información, permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

5.5. MARCO LEGAL

En la actualidad las entidades de carácter público, invierten muy poco o nada en el aseguramiento tanto de sus recursos como de sus activos, incluyendo el más importante: La información. Al no implementar mecanismos de seguridad en las redes de computadores llevan no sólo a pérdidas sustanciales de dinero.

LEY 1273 DEL 5 ENERO DEL 2009 “protección de la información y de los datos” está establecida en la norma de la constitución política de Colombia²³

Estos son los aspectos que considera la ley para juzgar los delitos informáticos:

- **Acceso abusivo a un sistema informático.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad.
- **Obstaculización ilegítima de sistema informático o redes de telecomunicación.** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.
- **Interceptación de datos informáticos.** El que, sin orden judicial previa, intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.
- **Daño informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
- **Uso de software malicioso.** Quien produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación.
- **Violación de datos personales.** La persona que con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
- **Suplantación de sitios web para capturar datos personales.** Este delito es para quien diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

²³ <http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf>

6. MARCO METODOLOGICO

6.1. METODOLOGIA DE INVESTIGACIÓN

Diseño De Un Sistema De Gestión De Seguridad Informática Para La Alcaldía Municipal De La Jagua De Ibirico – Cesar Basado En La Norma ISO 27001:2013.

6.1.1. Metodología cuantitativa. Se manejó una metodología cuantitativa ya que se le asignó valores numéricos y declaraciones u observaciones, con el propósito de estudiar los métodos estadísticos posibles relaciones entre las variables.

6.1.2. Tipo de investigación. Teniendo en cuenta las características del proyecto, se utilizará el desarrollo del método investigación de tipo factible, este se basa en investigar elaborar y desarrollar y de esta manera solucionar problemas, requerimientos o necesidades de organizaciones²⁴.

Con base en la anterior definición, el presente trabajo corresponde al análisis y desarrollo de una propuesta para el diseño de un Sistema de Gestión de Seguridad de la Información para entidad de la alcaldía municipal de la jagua de ibirico cesar 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 es recogida de forma directa de la fuente, mediante encuestas, cuestionario, entrevista o reuniones.

6.2. METODOLOGÍA DE DESARROLLO

Objetivo 1. Describir mediante la Declaración de Aplicabilidad (SOA) la situación actual de la alcaldía municipal de la jagua de ibirico

²⁴ Manual de Tesis de Grado y Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Libertador, Pág.13.

Objetivo 2. Diseñar el análisis de riesgo mediante la metodología de Magerit de la alcaldía municipal de la jagua de ibirico

Objetivo 3. Identificar los controles existentes con que cuenta la entidad con la norma ISO 27001:2013.

Objetivo 4. Definir la política, alcance y objetivos del Sistema de Gestión de Seguridad de la información.

6.3. UNIVERSO Y MUESTRA

6.3.1. Universo o Población: el universo son activos y los procesos que realiza la alcaldía.

6.3.2. Muestra: Los riesgos y las amenazas que puedan encontrarse.

6.4. FUENTES DE INFORMACIÓN

6.4.1. Fuentes primarias. Son aquellas que brindan una demostración o certeza acerca del tema de estudio, este tipo de fuentes ofrecen una visión del suceso en específico, transmitiendo ideas nuevas, admitiendo apreciación de la sociedad.

- Los activos con que cuenta la alcaldía municipal de la jagua de ibirico.
- Diseño de un sistema de gestión de seguridad informática.

6.4.2. Fuentes Secundarias. Este tipo de fuentes abarcan información estructurada, formalizada, donde muestra resultados de estudios, o textos originales primarios, son utilizadas para ratificar hallazgos del estudio, extender el contenido de la información de una fuente primaria y para proyectar los estudios realizados.

Esta clase de fuente es creada normalmente por alguna persona que no posee contacto directo con el suceso o argumento.

- Internet
- Artículos
- Libros
- manuales consultados

Se utilizará estos medios para constituir los elementos teórico-prácticos necesarios para el desarrollo del proyecto.

7.RESULTADO A ENTREGAR

Como resultado se entregará un informe de las pruebas realizadas y las recomendaciones para definir el plan de mejoramiento de la seguridad informática y de la información en la alcaldía de la Jagua de Ibirico

7.1. La Declaración de Aplicabilidad o SOA (Statement of Applicability)

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:

A. Grupo de Controles que aplican:

A.1 Implementados (6 controles)

A.2 No implementados (36 controles)

A.3 Implementados parcialmente (52 controles)

A.4 Aplica en una posterior fase del ciclo del SGSI (24 controles)

A.5 Implementación a cargo de externo (1 controles)

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

Tabla 2. 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 3. 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 4. Declaración De Aplicabilidad

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 seguridad de la Información	Implementado parcialmente	Se está realizando un documento	Dentro de los pasos para la implementación de un SGSI es necesario definir 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	Aun 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	Aun 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 5. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
6.1.3	Asignación de responsabilidades	No implementado	Aun 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	Aun no se ha presentado la necesidad de nuevos servicios de procesamiento de información.
6.1.5	Se realizan acuerdos de confidencialidad	Implementado parcialmente	Aun no se han aplicado.	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 quien 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 6. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
6.2.1	Identificación de riesgos	No implementado	Aun no se ha documentado.	grupo externo tenga acceso a los medios de procesamiento de la información o la información de una organización, se debiera llevar a cabo una evaluación del riesgo para <u>identificar cualquier requerimiento de controles</u>
6.2.2	Aproximación a la seguridad al tratar con clientes	No implementado	Aun 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	Aun 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 Cítricos	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	Aun 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 las activos tecnológicos	Implementado parcialmente	Aun no se han aplicado.	El acuerdo debiera asegurar que no existan malos entendidos entre la organización y la otra parte.

Tabla 7. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
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	Aun 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 de la oficina de RH	Aun 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 de la oficina de RH	Aun 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 de la oficina de RH	Aun no se han definido los requerimientos de los perfiles del personal relacionado con el SGSI.

Tabla 8. (Continuación)

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	Implementado parcialmente	Aun 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	Aun 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.

Tabla 9. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
8.3.1	Responsabilidades en la terminación del contrato	Implementado parcialmente	Aun no se han aplicado.	Es necesario que se definan responsabilidades de confidencialidad incluso después de la terminación del contrato o cambio de trabajo.
8.3.2	Devolución de activos tecnológicos	Implementado parcialmente	Aun no se ha documentado.	El proceso de terminación debiera ser formalizado para incluir la devolución de todo el software, documentos corporativos y equipo entregado previamente.
8.3.3	Eliminación de permisos sobre los activos	Implementado parcialmente	Aun no se han aplicado.	A la terminación, se debieran reconsiderar los derechos de acceso de una persona a los activos asociados con los sistemas y servicios de información.
9.1	Áreas Restringidas	Para prevenir el acceso no autorizado físico, daños e interferencia a las instalaciones y la información de la organización.		
9.1.1	Perímetro de Seguridad Física	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de ubicación física relacionado con áreas seguras para los activos de información por parte del SGSI
9.1.2	Controles físicos de entrada	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de ubicación física relacionado con áreas seguras para los activos de información por parte del SGSI

Tabla 10. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de ubicación física relacionado con áreas seguras para los activos de información por parte del SGSI
9.1.4	Protección contra amenazas externas y ambientales	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de ubicación física relacionado con áreas seguras para los activos de información por parte del SGSI
9.1.5	Trabajo en áreas restringidas	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de ubicación física relacionado con áreas seguras para los activos de información por parte del SGSI
9.1.6	Acceso público, envíos y áreas de carga	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de ubicación física relacionado con áreas seguras para los activos de información por parte del SGSI
9.2	Seguridad de los Componentes Tecnológicos	Para evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las actividades de la organización.		

Tabla 11. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
9.2.1	Ubicación y protección de equipos tecnológicos	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de ubicación física relacionado con áreas seguras para los activos de información por parte del SGSI
9.2.2	Seguridad en el suministro de electricidad y servicios (utilities)	Implementado parcialmente	UPS y planta eléctrica.	Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; debieran ser adecuados para los sistemas que soportan.
9.2.3	Seguridad en el cableado	Aplica a una posterior fase del ciclo del SGSI	Debe estar a cargo de la administración	Aun no se han definido nuevos requerimientos de componentes tecnológicos relacionado con los activos de información por parte del SGSI
9.2.4	Mantenimiento	Implementado parcialmente	Aun no se han aplicado.	Hay definidos procedimientos para el mantenimiento preventivo, pero aún no han entrado en vigencia.
9.2.5	Seguridad de equipos fuera de las áreas seguras	No aplica	No aplica	Los equipos por fuera a las instalaciones seguras están en arriendo (outsourcing).
9.2.6	Destrucción y reutilización de equipos	No aplica	No aplica	No hay definido un procedimiento claro en la organización y no hay claridad de en quien recae esta función.

Tabla 12. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
9.2.6	Dstrucción y reutilización de equipos	No aplica	No aplica	No hay definido un procedimiento claro en la organización y no hay claridad de en quien recae esta función.
9.2.7	Extracción de activos informáticos	Implementado Parcialmente	Políticas de seguridad de la información y Manual de Procedimientos de la Seguridad de la Información	Se debe contemplar procedimientos que apoyen a un mejor control de la seguridad de la información. Por ejemplo si un equipo que contiene información crítica se desplaza a un servicio técnico o un tercero es necesario asegurar de que dicha información este protegida o no se pueda acceder.
10.1	Procedimientos Operacionales y Responsabilidades	Para garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.		
10.1.1	Documentación de procesos operativos	Implementado Parcialmente	Se realizó un documento	En la actualidad se cuenta con documentación formal de los procedimientos operativos realizados por los trabajadores necesarios para el correcto desempeño en las actividades.
10.1.2	Control de Cambios	Implementado Parcialmente	Se realizó un documento	El alcance de este control se incluyó a un procedimiento del equipo de desarrollo.
10.1.3	Segregación de funciones	Implementado Parcialmente	Se realizó un documento	Es necesario para reducir las oportunidades de modificación no autorizada o no intencionada de los activos de la información, así también el mal uso de los mismos. Actualmente se menciona en el Manual de Políticas la segregación de tareas en la organización.

Tabla 13. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
10.1.4	Separación de los ambientes de Desarrollo, prueba y producción	No implementado	Aun no se ha establecido.	Se debiera identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales y se debieran implementar los controles apropiados.
10.2	Administración de Servicios de terceros	Para implementar y mantener el nivel adecuado de seguridad de la información y la prestación de servicios en línea con los acuerdos de prestación de servicios de terceros.		
10.2.1	Entrega de servicios	Implementado Parcialmente	Aun no se ha documentado.	La entrega del servicio por un tercero debiera incluir los acuerdos de seguridad pactados, definiciones del servicio y aspectos de la gestión del servicio.
10.2.2	Monitoreo y revisión de servicios de terceros	No implementado	Aun no se ha documentado	No se realiza un monitoreo y revisión de los servicios de terceros en el tema de seguridad de la información, lo cual podría afectar a la Gestión adecuada de los problemas o incidentes de seguridad.
10.2.3	Administración de cambios a servicios de terceros	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	No se realiza la gestión de cambios para los servicios de terceros, lo cual puede afectar la criticidad de los sistemas y procesos de negocio involucrados.
10.3	Planeamiento y aceptación de sistemas	Para proteger la integridad del software y la información.		

Tabla 14. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
10.3.1	Administración de la capacidad	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Aun no se han definido nuevos requerimientos de la capacidad de la infraestructura tecnológica relacionado con los activos de información por parte del SGSI.
10.3.2	Aceptación de sistemas	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Aun no se han definido nuevos requerimientos de la capacidad de la infraestructura tecnológica relacionado con los activos de información por parte del SGSI.
10.4	Protección contra código malicioso y móvil	Para proteger la integridad del software y la información.		
10.4.1	Controles contra código malicioso	Implementado Parcialmente	Antivirus	El control frente al código malicioso se encuentra implementado, pero a la espera de procedimientos formales para salvaguardar la integridad y disponibilidad de la información.
10.4.2	Controles contra código móvil	No aplica	No aplica	Los controles frente a código móvil no se aplican puesto que el modelo de negocio del Servicio de la caja no permite el uso de código móvil.
10.5	Copias de seguridad	Para mantener la integridad y la disponibilidad de instalaciones de procesamiento de la información y de la información.		
10.5.1	Respaldo de la información.	Implementado Parcialmente	Aun no se ha documentado.	Actualmente se cuentan con procedimientos de respaldo de información es necesario formalizar y realizar una revisión si se están contemplando todos los activos que contengan información.

Tabla 15. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
10.6	Administración de la seguridad de la red	Para garantizar la protección de la información en las redes y la protección de la infraestructura de apoyo.		
10.6.1	Controles de la Red	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Actualmente no se cuentan definidas responsabilidades sobre la red, lo cual eleva la cantidad de amenazas a los sistemas de información.
10.6.2	Seguridad de los Servicios de Red	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Se debería implementar este control con la finalidad de no afectar la confidencialidad de la información transmitida a través de la red.
10.7	Manipulación de medios	Para evitar la divulgación no autorizada, modificación, eliminación o destrucción de bienes, y la interrupción de las actividades comerciales.		
10.7.1	Administración de medios removibles	No Implementado	Aun no se han aplicado.	Para evitar el robo de información, o transmisión de código malicioso que podría afectar las tres dimensiones de la información confidencialidad, integridad y disponibilidad, es necesario documentar y formalizar dicho control ya que en la práctica si se cumple.
10.7.2	Destrucción de medios	No Implementado	Aun no se han aplicado.	Actualmente no se cuentan con procedimientos formales para eliminar la información sensible de los equipos del Servicio de la caja.

Tabla 16. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
10.7.3	Procedimientos de manejo de la información	Implementado parcialmente	Aun no se han aplicado.	Se cuenta con acuerdo de confidencialidad. Es necesario también incluir otros procedimientos que no atiendan con la integridad y confidencialidad de la información.
10.7.4	Seguridad de la documentación de los sistemas	No Implementado	Aun no se han aplicado.	Este es un control que la caja debe implementar para una adecuada seguridad de la documentación de los sistemas, con procedimientos formales que permitan asegurar una buena manipulación de la información.
10.8	Intercambio de información	Para mantener la seguridad de la información y software intercambiado dentro de una organización y con cualquier entidad externa.		
10.8.1	Políticas y procedimientos del intercambio de información	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Se ha encontrado que no existen procedimientos formales para realizar el intercambio de información.
10.8.2	Acuerdos para el intercambio de información.	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	No existen acuerdos de intercambio en el Servicio de la caja esto podría afectar la confidencialidad de la información del negocio.
10.8.3	Medios físicos en movimiento	No Implementado	Aun no se han aplicado.	No se cuentan con procedimientos formales para el transporte de la información, permitiendo que la información pueda ser vulnerable a accesos no autorizados, mal uso de la información durante su transporte.

Tabla 17. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
10.8.4	Mensajería Electrónica	Implementación a cargo de externo	Aun no se han aplicado.	No se cuentan con procedimientos implementadas para el tratamiento de mensajes electrónicos, puede afectar accesos no autorizados a dichos mensajes, modificación del mismo o denegación de servicio.
10.8.5	Sistemas de información de negocios	No Implementado	Aun no se han aplicado.	No se cuenta con una adecuada protección de los sistemas de información del negocio, lo cual podría afectar la confidencialidad de la información del negocio. Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.
10.9	Servicios de Comercio Electrónico	Para detectar las actividades de procesamiento de información no autorizados.		
10.9.1	Comercio Electrónico	No aplica	No aplica	El modelo de negocio del Servicio no contempla el comercio electrónico.
10.9.2	Transacciones en Línea	No aplica	No aplica	El modelo de negocio del Servicio no contempla el comercio electrónico.
10.9.3	Información pública	No aplica	No aplica	La información que emplea el Servicio de la caja no es pública, sólo puede estar disponible para aquel solicitante que lo requiera, el incumplimiento de esta política podría comprometer la confidencialidad de la información

Tabla 18. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
10.10	Monitoreo	Los registros de auditoría de grabación de las actividades del usuario, excepciones y eventos de seguridad de información se producen y se conservarán durante un período acordado para ayudar en futuras investigaciones y la vigilancia del control de acceso.		
10.10.1	Auditoría de registros	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Existe una auditoria a los procesos del sistema, pero no se está contemplando una auditoría a la seguridad de la información, es necesario registrar un archivo de bitácora de auditorías, las cuales facilitarían realizar un adecuado monitoreo del control de accesos, identificando vulnerabilidades de la seguridad de la información.
10.10.2	Uso de sistemas de monitoreo	No Implementado	Aun no se han aplicado.	No se cuenta con procedimientos formales para el monitoreo del uso de los sistemas de información, el uso de este control asegura que los usuarios realicen actividades con previa autorización explícita, mitigando las amenazas a los sistemas de información.
10.10.3	Protección de registros de monitoreo	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Se debería brindar una protección de las bitácoras de los sistemas de información de la caja, con la finalidad de no causar un falso sentido de la seguridad.
10.10.4	Registros de monitoreo de administradores y operadores	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	Se deberían guardar las bitácoras del administrador y operador de los sistemas de la caja.

Tabla 19. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
10.10.5	Registro de fallas	No Implementado	Aun no se han aplicado.	No se guarda una bitácora de fallas de los sistemas, no permitiendo conocer el nivel de rendimiento actual de los sistemas, comprometiendo la continuidad del negocio.
10.10.6	Sincronía	No Implementado	Aun no se han aplicado.	Se debe revisar en todos los equipos del Servicio de caja cuentan con la sincronización del reloj.
11.1	Control de acceso a la información de acuerdo a las necesidades del negocio.	Para controlar el acceso a la información.		
11.1.1	Política de Control de Acceso	Implementado parcialmente	Políticas de seguridad de la información y Procedimientos de Seguridad de la Información	Existe una política de control de acceso que se encuentra administrada por la División de sistemas. Se pretende implementar procedimientos.
11.2	Administración de acceso de los usuarios	Para garantizar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.		
11.2.1	Registro de Usuarios	Implementado parcialmente	Se realizó un documento	Existe una política de control de acceso que se encuentra administrada por la División de sistemas. Se pretende implementar procedimientos.

Tabla 20. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
11.2.2	Administración de privilegios	Implementado parcialmente	Se realizó un documento	Existe una política de control de acceso que se encuentra administrada por la División de sistemas. Se pretende implementar procedimientos.
11.2.3	Administración de Contraseñas (passwords)	Implementado parcialmente	Se realizó un documento	Existe una política de control de acceso que se encuentra administrada por la División de sistemas. Se pretende implementar procedimientos.
11.2.4	Revisión de los permisos asignados a los usuarios	Implementado parcialmente	Se realizó un documento.	Existe una política de control de acceso que se encuentra administrada por la División de sistemas. Se pretende implementar procedimientos.
11.3	Responsabilidades de los usuarios	Para prevenir el acceso no autorizado de usuarios, y el compromiso o el robo de las instalaciones de procesamiento de la información y de la información.		
11.3.1	Uso de las contraseñas	Implementado parcialmente	Políticas de seguridad de la información.	Falta una mayor concienciación en el uso de las contraseñas.
11.3.2	Equipos desatendidos	No Implementado	Aun no se han aplicado.	Es necesaria una mayor concienciación sobre el tratamiento de los equipos desatendidos por los usuarios
11.3.3	Política de escritorios y pantallas limpias	No Implementado	Aun no se han aplicado.	Falta concienciación y control al respecto.

Tabla 21. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
11.4	Control de acceso a la red de datos			Para prevenir el acceso no autorizado a los servicios en red.
11.4.1	Políticas para el uso de los servicios de la red de datos	Implementado parcialmente	Políticas de seguridad de la información.	Actualmente la política sobre el uso de los servicios de red se encuentra administrada por el directorio activo de la Caja, y el Servicio tiene sus propias políticas.
11.4.2	Autenticación de usuarios para conexiones externas	Aplica a una posterior fase del ciclo del SGSI	Este control se va implementar en una siguiente fase del ciclo del SGSI.	La autenticación de los usuarios remotos se puede lograr utilizando, por ejemplo, una técnica basada en criptografía, dispositivos de hardware o un protocolo de desafío/respuesta.
11.4.3	Identificación de equipos en la red	Implementado parcialmente	Políticas de seguridad de la información.	Actualmente la política sobre la identificación de equipos en la red se encuentra administrada por el directorio activo de la caja, y el Servicio se limita a cumplir y respetar dicha política.
11.4.4	Diagnóstico remoto y protección de la configuración de puertos	Implementado	Firewall	Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyen el uso de un seguro y procedimientos de soporte para controlar el acceso físico al puerto.
11.4.5	Segregación en la red	Implementado parcialmente	Políticas de seguridad de la información.	La segregación de redes se encuentra administrada por la división de sistemas, el Servicio se limita a cumplirla con el fin de evitar intrusiones por parte de personal proveniente de otros proveedores o áreas de la caja.

Tabla 22. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
11.4.6	Control de conexión a la red	Implementado parcialmente	Políticas de seguridad de la información.	Los derechos de acceso a la red de los usuarios se debieran mantener y actualizar conforme lo requiera la política de control de acceso.
11.4.7	Control de enrutamiento de la red	No Implementado	Aun no se han aplicado.	Esto se aplica particularmente cuando las redes son compartidas con terceros (no-organización).
11.5	Control de acceso a los sistemas operativos	Para prevenir el acceso no autorizado a los sistemas operativos.		
11.5.1	Procedimientos para inicio de sesión de las estaciones de trabajo	No Implementado	Aun no se han aplicado.	El procedimiento de Log-on de seguridad en el sistema operativo no se encuentra implementado, todo equipo del directorio activo requiere log-on autorizado.
11.5.2	Identificación y autenticación de los usuarios.	No Implementado	Aun no se han aplicado.	La identificación y autenticación de usuarios debe encontrarse gestionada a través del directorio activo.
11.5.3	Sistema de administración de contraseñas.	Implementado parcialmente	Políticas de seguridad de la información.	La administración de las contraseñas se encuentra descrita en la política de seguridad de la información.

Tabla 23. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
11.5.4	Uso de las utilidades del sistema	Implementado parcialmente	Políticas de seguridad de la información.	No se ha implementado la restricción del uso de utilidades del sistema al no permitir instalar nuevo software en los equipos, así como otros utilitarios del Sistema Operativo. Se han limitado para todos los usuarios como política, falta formalizar y crear un procedimiento adecuado.
11.5.5	Time-out para las estaciones de trabajo.	No Implementado	Aun no se han aplicado.	Actualmente no se encuentra implementada la desconexión de terminales por tiempos muertos, en algunos equipos.
11.5.6	Limitación en los periodos de tiempo de conexión a servicios y aplicaciones	No Implementado	Aun no se han aplicado.	No existe un procedimiento formal para la limitación en el tiempo de conexión, el cual es importante para locales con acceso público o de alto tránsito de personal de otras organizaciones, puesto que podría comprometer la confidencialidad e integridad de la información.
11.6	Control de acceso a las aplicaciones	Para prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación.		
11.6.1	Restricción de acceso a los sistemas de información	Implementado	Administrador aplicaciones.	El control de acceso a las aplicaciones, caso particular la restricción del acceso de información se encuentra restringido por la División de sistemas, la aplicación y gestión de dicho control está a cargo de la misma.

Tabla 24. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
11.6.2	Aislamiento de sistemas sensibles	Implementado	Centro de datos	El aislamiento de sistemas sensibles se encuentra restringido por la División de sistemas, la aplicación y gestión de dicho control está a cargo de la misma.
11.7	Computación Móvil y Teletrabajo	Para garantizar la seguridad de la información cuando se utilizan las instalaciones de computación y teletrabajo móvil.		
11.7.1	Computación Móvil y comunicaciones	No aplica	No aplica	Actualmente el Servicio de red no debe contar con computadoras con comunicación inalámbrica u otro equipo móvil similar para realizar sus trabajos
11.7.2	Teletrabajo	No aplica	No aplica	Por política de la caja, todo trabajo debe ser realizado en las instalaciones de la organización, o en algún local previamente
12.1	Requerimientos de seguridad para los sistemas de	Para asegurar que la seguridad es una parte integral de los sistemas de información.		
12.1.1	Análisis y especificaciones de los requerimientos de seguridad	Implementado parcialmente	Políticas de seguridad de la información y Procedimientos de Seguridad de la Información.	Los requerimientos de seguridad para la seguridad de la información y los procesos para implementar la seguridad debieran ser integrados en las primeras etapas de los proyectos de sistemas de información.
12.2	Procesamiento correcto en aplicaciones	Para evitar errores, la pérdida, modificación o mal uso de la información en la aplicación no autorizada.		

Tabla 25. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
12.2.1	Validación de los datos de entrada	Implementado parcialmente	Aun no se han aplicado.	Se debieran realizar chequeos del input de las transacciones, la data fija (por ejemplo nombres y direcciones), y tablas de parámetros.
12.2.2	Control del procesamiento interno	Implementado parcialmente	Aun no se han aplicado.	El diseño e implementación de las aplicaciones debiera asegurar que se minimicen los riesgos de fallas en el procesamiento que lleven a la pérdida de la integridad de la información.
12.2.3	Integridad de los mensajes	Implementado parcialmente	Aun no se han aplicado.	Se debiera realizar una evaluación de los riesgos de seguridad para determinar si se requiera la integridad del mensaje y para identificar el método de implementación más apropiado.
12.2.4	Validación de los datos de salida	Implementado parcialmente	Aun no se han aplicado.	Los sistemas que han sido probados pueden producir output incorrecto en algunas circunstancias.
12.3	Controles Criptográficos	Para proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos.		
12.3.1	Política para el uso de controles criptográficos	No Implementado	Aun no se han aplicado.	Actualmente no se protege la información con controles criptográficos a nivel de aplicaciones
12.3.2	Administración de llaves	No Implementado	Aun no se han aplicado.	La administración de claves, vital para el correcto funcionamiento de dichos controles criptográficos con el fin de preservar la confidencialidad, integridad y disponibilidad de la información cifrada.

Tabla 26. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
12.4	Seguridad en los archivos del sistema (System Files)			Para garantizar la seguridad de los archivos del sistema
12.4.1	Control del software operacional (operativo)	Implementado parcialmente	Aun no se han aplicado.	Actualmente el control de la instalación de software en los equipos es responsabilidad de la División de sistemas al estar implementada la Política de Seguridad de la caja la cual no permite la instalación de software con un fin distinto a la productividad de los empleados.
12.4.2	Protección de los datos en sistemas de prueba	Implementado parcialmente	Aun no se han aplicado.	Las pruebas de los sistemas de información son realizadas por los proveedores, equipo de desarrollo y mantenimiento de sistemas de la división de sistemas.
12.4.3	Control de acceso a las librerías de código fuente	Implementado	Administrador aplicaciones.	Las restricciones en el control de acceso a los códigos fuentes de los sistemas de información son responsabilidad de la división de sistemas y sus proveedores.
12.5	Seguridad en el desarrollo y en los procesos de soporte técnico			Para mantener la seguridad de software de sistema de aplicación y la información.
12.5.1	Procedimientos para el control de cambios	Implementado parcialmente	Aun no se han aplicado.	La División de sistema es la responsable del correcto funcionamiento de los procedimientos de control de cambios.

Tabla 27. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
12.5.2	Revisión técnica de aplicaciones después de cambios al sistema operativo	Implementado parcialmente	Aun no se han aplicado.	Con el fin de evitar un impacto adverso en las operaciones y/o la seguridad de los sistemas de información, se debe realizar una revisión técnica de las aplicaciones.
12.5.3	Restricciones a cambios en paquetes de software	No Implementado	No se realiza.	Para evitar un posible impacto en las operaciones del Servicio de caja, se debe evitar el realizar cambios a los paquetes de software.
12.5.4	Fuga de información	No Implementado	No se realiza.	Con el fin de prevenir acceso no autorizado a la red y mal uso de los sistemas de información por parte del personal.
12.5.5	Desarrollo de software por parte de Outsourcing	Implementado	Por medio de documentación y pruebas	El desarrollo de software por parte de terceros es responsabilidad de la división de sistemas, este control debe ser implementado con el fin de preservar la seguridad de la información.
12.6	Administración Técnica de Vulnerabilidades	Para reducir los riesgos derivados de la explotación de las vulnerabilidades técnicas publicadas.		
12.6.1	Control técnico de vulnerabilidades	Implementado parcialmente	Aun no se han aplicado.	El cumplimiento e implementación de dicho control, mantiene actualizado los equipos de posibles vulnerabilidades que podrían comprometer la seguridad información.
13.1	Reporte de eventos de seguridad informática y de sus debilidades	Para garantizar la seguridad de la información de eventos y debilidades asociadas a los sistemas de información se comunican de una manera que permite acciones correctivas oportunas que deban tomarse.		

Tabla 28. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
13.1.1	Reporte de eventos de Seguridad de la información.	No Implementado	Aun no se ha documentado.	En la actualidad no se cuenta con un procedimiento ni formato para generar el reporte de incidentes de la seguridad de información conjuntamente con la respuesta ante estos incidentes y procedimientos a escala.
13.1.2	Reporte de debilidades de seguridad	No Implementado	Aun no se ha documentado.	No existe un reporte de las debilidades de la seguridad de la información, es necesario para la mejora de los controles de seguridad de la información.
13.2	Administración de incidentes de seguridad informática y de su <u>mejoramiento</u> .	Para garantizar un enfoque coherente y eficaz se aplica a la gestión de incidentes de seguridad de la información.		
13.2.1	Responsabilidades y procedimientos	No Implementado	Aun no se ha documentado.	Es necesario gestionar los incidentes de seguridad de la información para garantizar una rápida, efectiva y ordenada respuesta a los incidentes de seguridad de la información y asignar procedimientos y responsabilidades.
13.2.2	Aprendizaje a partir de los incidentes de seguridad	No Implementado	Aun no se ha documentado.	Se debiera utilizar la información obtenida de la evaluación de los incidentes en la seguridad de la información para identificar los incidentes recurrentes o de alto impacto.

Tabla 29. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
13.2.3	Recolección de evidencia	No Implementado	Aun no se ha documentado.	En este control se va a considerar la recolección de evidencias, con las herramientas existentes.
14.1	Consideraciones para la administración de la continuidad del negocio	Para contrarrestar las interrupciones a las actividades comerciales y proteger los procesos críticos de negocio de los efectos de los fallos principales de los sistemas de información o los desastres y asegurar su oportuna reanudación.		
14.1.1	Inclusión de seguridad de la información en el proceso de administración de la continuidad del negocio	Implementado parcialmente	Aun no se han aplicado.	Uno de los aspectos principales a considerar es concentrar los esfuerzos para realizar una oportuna recuperación de los procesos críticos del negocio.
14.1.2	Continuidad del negocio y análisis de impacto (BIA)	Implementado parcialmente	Aun no se han aplicado.	Con el fin de desarrollar una adecuada estrategia de continuidad de negocio es necesario partir de una evaluación de riesgos las cuales tiene que estar alineadas al SGSI.
14.1.3	Desarrollo e implementación de planes de continuidad	Implementado parcialmente	Aun no se han aplicado.	Es necesario desarrollar e implementar planes de continuidad para asegurar la disponibilidad de la información en el momento oportuno y nivel requerido. (Aplica solo para un plan de contingencia).

Tabla 30. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
14.1.4	Marco de planeación para la continuidad del negocio	Implementado parcialmente	Aun no se han aplicado.	Asegurar la consistencia de los planes de contingencia.
14.1.5	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio	Implementado parcialmente	Aun no se han aplicado.	Asegurar la efectividad y actualización del plan de contingencia
15.1	Cumplimiento con requerimientos legales	Para evitar el rebasamiento de cualquier ley, obligaciones legales, reglamentarias o contractuales, y de los requisitos de seguridad.		
15.1.1	Identificación de leyes aplicables	No Implementado	Aun no se ha documentado.	Asegurar que las normas que se den tengan una base legal para no afectar a la institución. Sólo se tomará en cuenta las normas que se refieran a la Seguridad de la Información.
15.1.2	Derechos de autor y propiedad intelectual	Implementado parcialmente	Aun no se han aplicado.	Cumplir con la legalidad y no afectar la propiedad intelectual.
15.1.3	Salvaguardar los registros de la organización	Implementado parcialmente	Aun no se han aplicado.	Evitar las pérdidas, falsificación, destrucción y el mal uso de los registros de la organización.

Tabla 31. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
15.1.4	Protección de los datos y privacidad de la información personal	No aplica		No existe una regulación sobre la protección de datos y privacidad de la información personal.
15.1.5	Prevención mal uso de los componentes tecnológicos	Implementado parcialmente	Políticas de seguridad de la información	Se requiere implantar medidas preventivas para evitar el mal uso de las instalaciones de procesamiento de información.
15.1.6	Regulación de controles criptográficos	No aplica		No existen regulaciones locales de los controles criptográficos.
15.2	Revisión de la política de seguridad y cumplimiento técnico.	Para garantizar el cumplimiento de los sistemas con las políticas y estándares de seguridad de la organización.		
15.2.1	Cumplimiento de los diferentes requerimientos y controles establecidos por la política de seguridad.	Implementado parcialmente	Revisión oficina de calidad.	Asegurar que las políticas de la seguridad de la organización estén cumpliendo las normas y estándares.
15.2.2	Chequeo del cumplimiento técnico	No Implementado	Aun no se han aplicado.	Asegurar que los controles de hardware y software estén implantados correctamente.

Tabla 32. (Continuación)

Control ISO	Requerimiento	Estado	Proceso de implantación	Razones para la selección
15.3	Consideraciones relacionadas con la auditoría interna	Para maximizar la eficacia y minimizar la interferencia a / desde el proceso de auditoría de sistemas de información.		
15.3.1	Controles para auditoría del sistema	No Implementado	Aun no se han aplicado.	Estar preparados para brindar los requerimientos solicitados en la auditoría para minimizar los riesgos o interrupciones en el proceso de negocio.
15.3.2	Protección de las herramientas para auditoría del sistema	No Implementado	Aun no se han aplicado.	Evitar que las herramientas de auditoría afecten la continuidad y seguridad del negocio.

Fuente. NTC-ISO/IEC 27001

7.2. Diseñar el análisis de riesgo mediante la metodología de Magerit

7.2.1. Inventario de activos: Con la revisión y aprobación de la gerencia “alcaldesa” para llevar a cabo este proyecto, se procede a realizar el análisis del proyecto SGSI (sistema de gestión de la seguridad de la información), a la Alcaldía de La Jagua de Ibirico – Cesar con el objetivo de garantizar la seguridad de los activos de la empresa.

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

Tabla 33. Activos con Magerit

Código	Nombre Grupo	Código Activo	Nombre Activo	Tipo Tecnologia
[host]	grandes equipos	[serv]	Servidores	Equipos Informáticos
[mobile]	informática móvil	[portatiles]	Computadores portátiles y otros dispositivos móviles	Equipos Informáticos
[pc]	informática personal	[secAcienda]	Secretaria De Hacienda	Equipos Informáticos
[pc]	informática personal	[SecEduc]	Secretaria De Educacion	Equipos Informáticos
[pc]	informática personal	[SecGov]	Secretaria De Gobierno.	Equipos Informáticos
[pc]	informática personal	[SecPLanea]	Secretaria De Planeacion.	Equipos Informáticos
[pc]	informática personal	[secEstruc]	Secretaria De Infraestructra.	Equipos Informáticos
[pc]	informática personal	[OfiJur]	Oficina Juridica	Equipos Informáticos

Tabla 5. (Continuación)

Código	Nombre Grupo	Código Activo	Nombre Activo	Tipo Tecnología
[pc]	informática personal	[thumano]	Oficna 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]	Contratacion	Equipos Informáticos
[pc]	informática personal	[gesSoc]	Gestion Social	Equipos Informáticos
[scan]	Scáneres	[E_platteryEscanner]	Equipos de plotter y escanners	Equipos Informáticos
[HW]	Equipos que son fácilmente transportados	[PC_portatiles]	EquiposPortatiles	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

Tabla 5. (Continuación)

Código	Nombre Grupo	Código Activo	Nombre Activo	Tipo Tecnología
[Intranet]	Intranet	[intranet]	Intranet	Redes De Comunicaciones
[LAN]	Red local	[c_hub]	Hub para soportar la red LAN	Redes De Comunicaciones
[LAN]	Red local	[c_switch]	Switch 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	[office]	Microsoft Office	Software
[office]	ofimática	[WEB1]	CUTEPDF	Software
[app]	Servidor de aplicaciones	[CONVENIO GOBERNACION DEL CESAR]	SIIAF AREA FINANCIERA (Módulos, Presupuesto Gastos, Presupuesto de Ingresos, Integración, Apropiación, Contabilidad, Egresos.	Software
[app]	Servidor de aplicaciones	[SICEP]	Contraloria G	Software
[app]	Servidor de aplicaciones	[SIDEF]	Contraloria G	Software

Tabla 5. (Continuación)

Código	Nombre Grupo	Código Activo	Nombre Activo	Tipo Tecnología
[app]	Servidor de aplicaciones	[Adquisicion]	Siipu Impuesto Predial	Software
[app]	Servidor de aplicaciones	[chip]	Chip Ministerio De Hacienda	Software
[app]	Servidor de aplicaciones	[PasivoCol]	Ministerio De Hacienda	Software
[dbms]	sistema de gestión de bases de datos	[oracle]	ORACLE MOTOR DE BASE DATOS	Software
[app]	Servidor de aplicaciones	[CONTRATO1]	SICAB CONTROL ENTRADA Y SALIDA FUNCIONARIOS	Software
[app]	Servidor de aplicaciones	[CONTRATO2]	SYS046 SALUD CIRCULAR 046	Software
[app]	Servidor de aplicaciones	[CONTRATO3]	SYSMARC MARCA DE GANADA	Software
[app]	Servidor de aplicaciones	[CONTRATO4]	SYSNOM NOMINA	Software
[app]	Servidor de aplicaciones	[CONTRALORIA 5]	SIRCC REPORTE INFORME A COTRALORALIA NACIONAL	Software
[app]	Servidor de aplicaciones	[CONTRATO5]	ZAFIRO INDUSTRIA Y COMERCIO	Software
[app]	Servidor de aplicaciones	[CONTRATO6]	SIAFF - ACTIVOS FIJOS ALMACE	Software

Tabla 5. (Continuación)

Código	Nombre Grupo	Código Activo	Nombre Activo	Tipo Tecnología
[sub]	desarrollo a medida	[contrato9]	VALBDUA	Software
[backup 1]	sistema de backup	[WEB.2]	APBAKUP	Software
[files]	Archivos	[predial]	Información de Contribuyentes	Datos/Información
[backup]	Copias de Respaldo	[A_Copias de Seguridad]	Archivo de Copias de seguridad de la información	Datos/Información
[passw ord]	Credenciales	[Pass_usuarios]	Contraseñas de acceso de usuarios del sistema	Datos/Información
[encryp t]	Claves de cifra	[CC_Aplicaciones_financiera]	Claves de cifra de Los bancos	Claves Criptográficas
[ext]	A usuarios externos	[S_U_Externo]	Servicios prestados a usuarios externos	Inventario De Servicios
[www]	World wide web	[S_Internet]	Servicio de internet al que pueden acceder los funcionarios.	Inventario De Servicios
[email]	Correoelectrónico	[S_correo]	Manejo de correos electrónicos	Inventario De Servicios
[file]	Almacenamiento de archivos	[S_A_Bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.	Inventario De Servicios

Tabla 5. (Continuación)

Código	Nombre Grupo	Código Activo	Nombre Activo	Tipo Tecnología
[cd]	DiscosDuros DD	[A_DD]	Almacenamientos en Disco Duro	Soportes De Información Almacenamiento Electrónico
[usb]	Memoria USB	[A_Memoria]	Almacenamiento en Memoria USB	Soportes De Información Almacenamiento Electrónico
[dvd]	DVR	[A_DVD]	Almacenamiento en DVD	Soportes De Información Almacenamiento Electrónico
[printed]	Material impreso	C_Documentaci ón_proyecto	Carpetas con la documentación de cada proyecto en ejecución	Soportes De Información Almacenamiento No Electrónico
		C_Reportes_fact uras	Carpetas de reportes y facturas impresos	Soportes De Información Almacenamiento No Electrónico
		C_Soportes- financieros	Carpetas de obligación financiera.	Soportes De Información Almacenamiento No Electrónico
[buildin g]	Edificio	[E_Edificio]	Instalacion física de la entidad	Instalaciones
[site]	[site] recinto	[S_cpconsejo]	Recinto del consejo	Instalaciones
[ui]	Usuariosinterno s	[U-Sistemas]	Personal de soporte TI	Personal
[adm]	Administradore s de sistemas	[A_sistemas]	Administrador de sistemas	Personal

Fuente: El autor.

7.2.2. 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 34. Identificación de amenazas en la Alcaldía de la Jagua de Ibirico.

AMENAZAS	ACTIVOS
[N.1] Fuego	[host] servidores
	[mobile] dispositivos móviles
	[pc] Equipo de computo de mesa
	[scan] Equipos de plotter y escanners
	[HW] Equipos Portatiles
	[print] Impresoras Lasser
	[print] Impresoras de inyección de tinta
[router] Enrutadores	
[N.2] Daños por agua	[host] servidores
	[pc] Equipo de computo de mesa
	[scan] Equipos de plotter y escanners
	[wifi] Ap para Red Inalámbrica
	[LAN] Red local Switch de 24 puertos
	[printed] Carpetas con la documentación de cada proyecto en ejecución
	[building] Instalacion física de la entidad
[N.7] Desastres naturales. Fenómeno sísmico.	[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
	[ui] Personal de soporte TI
	[adm] Administrador de sistemas
	[host] servidores
	[mobile] dispositivos móviles
	[pc] Equipo de computo de mesa
[scan] Equipos de plotter y escanners	

Tabla 6. (Continuación)

AMENAZAS	ACTIVOS
[I.5] Avería de origen físico o lógico.	[pc] Equipo de computo de mesa
	[print] Impresoras Lasser
	[router] Enrutadores
	[backup] sistema de backup
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.
[I.6] Corte del suministro eléctrico	[building] Instalacion física de la entidad
	[host] servidores
	[pc] Equipo de computo de mesa
	[scan] Equipos de plotter y escanners
	[HW] Equipos Portatiles
[I.7] Condiciones inadecuadas de temperatura o humedad	[app] Servidor de aplicaciones
	[host] servidores
	[pc] Equipo de computo de mesa
	[print] Impresoras Lasser
	[wifi] Ap para Red Inalámbrica
	[LAN] Red local Switch de 24 puertos
	[app] Servidor de aplicaciones
	[printed] Carpetas con la documentación de cada proyecto en ejecución
[I.8] Fallo de servicios de comunicaciones	[ui] Personal de soporte TI
	[adm] Administrador de sistemas
	[wifi] Ap para Red Inalámbrica
	[LAN] Red local Switch 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.

Tabla 6. (Continuación)

AMENAZAS	ACTIVOS
[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 computo de mesa
	[scan] Equipos de plotter y escanners
	[HW] Equipos Portatiles
	[print] Impresoras Lasser
	[print] Impresoras de inyección de tinta
	[os] sistema operativo
	[office] Microsoft Office
[E.2] Errores del administrador	[email] Manejo de correos electrónicos
	[printed] Carpetas con la documentación de cada proyecto en ejecución
	[host] servidores
	[router] Enrutadores
	[wifi] Ap para Red Inalámbrica
	[LAN] Red local Switch de 24 puertos
	[Intranet] intranet
[E.8] Difusión de software dañino	[os] sistema operativo
	[app] Servidor de aplicaciones
	[password] Contraseñas de acceso de usuarios del sistema
	[encrypt] Claves de cifra de Los bancos
	[host] servidores
	[pc] Equipo de computo de mesa
	[HW] Equipos Portatiles
[os] sistema operativo	
[dbms] ORACLE MOTOR DE BASE DATOS	
[www] Servicio de internet al que pueden acceder los funcionarios	
[email] Manejo de correos electrónicos	

Tabla 6. (Continuación)

AMENAZAS	ACTIVOS
[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
[E.24] Caída del sistema por agotamiento de recursos	[printed] Carpetas con la documentación de cada proyecto en ejecución
	[host] servidores
	[pc] Equipo de computo de mesa
	[HW] Equipos Portatiles
	[os] sistema operativo
	[app] Servidor de aplicaciones
	[dbms] ORACLE MOTOR DE BASE DATOS

Tabla 6. (Continuación)

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

Fuente. Libro Metodología Magerit Versión 3.

7.2.3. Valoración de amenazas. Se realiza una evaluación de amenazas basado en la frecuencia de materialización de la amenaza, las dimensiones de seguridad según MAGERIT y la escala de rango porcentual de impactos en los activos.

Tabla 35. Escala de Rango de frecuencia de amenazas.

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: Metodología Magerit Versión 3.

Tabla 36. Dimensiones de seguridad

Dimensiones de Seguridad	Identificación
Autenticidad	A
Confidencialidad	C
Integridad	I
Disponibilidad	D
Trazabilidad	T

Fuente: Metodología Magerit Versión 3.

Tabla 37. Escala de Rango porcentual de impactos en los activos

Impacto	Valor cuantitativo
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Metodología Magerit Versión 3.

De acuerdo a las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad.

En la siguiente tabla se puede observar los factores de amenaza de acuerdo a la clasificación de la metodología MAGERIT, tanto para factores naturales como no naturales. En la tabla se muestra cuáles son los activos que se ven afectados por cada uno de los factores de amenaza, así como la medición de la frecuencia o probabilidad de ocurrencia y el impacto que causaría de llegar a concretarse.

En la metodología MAGERIT se hace la medición en cada una de las características de la información, generalmente en las otras metodologías se hace la medición de tres características pilares de la seguridad de la información que son la confidencialidad, integridad y disponibilidad de la información o servicio, Magerit además considera las características de autenticidad y trazabilidad. En la medición del impacto hay que tener en cuenta el estándar Magerit donde se hace referencia a cuál de las características o criterios se califican, por ejemplo se observa que algunos activos solamente son afectados en su disponibilidad, sin embargo, otros pueden ser afectados en su confidencialidad, disponibilidad e integridad.

Por lo tanto para cada uno de los activos informáticos que han sido identificados, se debe aplicar la tabla de amenazas y su valoración correspondiente en probabilidad e impacto.

Tabla 38. Metodología Magerit.

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
[N.1] Fuego	[host] servidores	5				100%	
	[mobile] dispositivos móviles	5				100%	
	[pc] Equipo de cómputo de mesa	5			75%	5%	
	[scan] Equipos de plotter y escanners	5			75%		
	[HW] Equipos Portátiles	5			75%		
	[print] Impresoras Lasser	5			20%		
	[print] Impresoras de inyección de tinta	5	5%		20%		
[router] Enrutadores	5					100%	
[N.2] Daños por agua	[host] servidores	50		50%			
	[pc] Equipo de computo de mesa	10		50%		50%	
	[scan] Equipos de plotter y escanners	5			50%		
	[wifi] Ap para Red Inalámbrica	5			50%		
	[LAN] Red local Switch de 24 puertos	5		100%			
	[printed] Carpetas con la documentación de cada proyecto en ejecución	10		100%			
	[building] Instalacion física de la entidad	5		100%			
[N.7] Desastres naturales. Fenómeno sísmico.	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5					100%
	[usb] Almacenamientos en Disco Duro	5			50%		100%

Tabla 39. (Continuación)

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
[N.7] Desastres naturales. Fenómeno sísmico.	[printed] Carpetas con la documentación de cada proyecto en ejecución	50	5%			100%	
	[ui] Personal de soporte TI	5			50%	100%	
	[adm] Administrador de sistemas	5			50%		
	[host] servidores	5			50%		
	[mobile] dispositivos móviles	5		100%			
	[pc] Equipo de computo de mesa	10		100%			
	[scan] Equipos de plotter y escanners	10			20%		75%
[I.5] Avería de origen físico o lógico.	[pc] Equipo de computo de mesa	10					75%
	[print] Impresoras Lasser	10				20%	
	[router] Enrutadores	50			20%		
	[backup] sistema de backup	5		5%	75%		
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5					50%
	[building] Instalacion física de la entidad	10	5%		50%	50%	
[I.6] Corte del suministro eléctrico	[host] servidores	5		50%			
	[pc] Equipo de computo de mesa	5	100%		50%		
	[scan] Equipos de plotter y escanners	50		50%			
	[HW] Equipos Portatiles	10	100%				
	[app] Servidor de aplicaciones	5	5%				
[I.7] Condiciones inadecuadas de temperatura o humedad	[host] servidores	5			100%		
	[pc] Equipo de computo de mesa	50				20%	100%
	[print] Impresoras Lasser	5	5%			20%	

Tabla 40. (Continuación)

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
[N.7] Desastres naturales. Fenómeno sísmico.	[wifi] Ap para Red Inalámbrica	10		100%			
	[LAN] Red local Switch de 24 puertos	5			20%		
	[app] Servidor de aplicaciones	5			75%		
	[printed] Carpetas con la documentación de cada proyecto en ejecución	10	75%				
	[ui] Personal de soporte TI	5			50%		50%
	[adm] Administrador de sistemas	5	5%	50%			
[I.8] Fallo datos. de servicios de comunicaciones	[wifi] Ap para Red Inalámbrica	5		50%			
	[LAN] Red local Switch de 24 puertos	10		50%		50%	
	[Intranet] intranet	5				50%	
	[www] Servicio de internet al que pueden acceder los funcionarios	50		20%			
	[email] Manejo de correos electrónicos	10				20%	
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5		20%			5%
[I.10] Degradación de los soportes de almacenamiento de la información	[backup] sistema de backup Base de datos	5			50%		
	[backup] Archivo de Copias de seguridad de la información	10				5%	75%
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5	50%				

Tabla 41. (Continuación)

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
[E.1] Errores de los usuarios.	[pc] Equipo de computo de mesa	10		75%		20%	
	[scan] Equipos de plotter y escanners	50				20%	
	[HW] Equipos Portatiles	5					
	[print] Impresoras Lasser	5			20%		75%
	[print] Impresoras de inyección de tinta	5				5%	
	[os] sistema operativo	10		5%			
	[office] Microsoft Office	50	75%				
	[email] Manejo de correos electrónicos	5				20%	
[E.2] Errores del administrador	[printed] Carpetas con la documentación de cada proyecto en ejecución	5		50%			
	[host] servidores	10	20%				20%
	[router] Enrutadores	5				5%	
	[wifi] Ap para Red Inalámbrica	5			20%		
	[LAN] Red local Switch de 24 puertos	10					
	[Intranet] intranet	5		50%			
	[os] sistema operativo	5			75%		
	[app] Servidor de aplicaciones	50		5%			
	[password] Contraseñas de acceso de usuarios del sistema	5			50%		20%
[encrypt] Claves de cifra de Los bancos	10					75%	
[E.8] Difusión de software dañino	[host] servidores	5	20%				
	[pc] Equipo de computo de mesa	50			75%		
	[HW] Equipos Portatiles	5		20%			
	[os] sistema operativo	10		20%			50%
	[dbms] ORACLE MOTOR DE BASE DATOS	5					

Tabla 42. (Continuación)

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
	[www] Servicio de internet al que pueden acceder los funcionarios	5			20%		
	[email] Manejo de correos electrónicos	5	20%				
[E.15] Alteración accidental de la información	[office] Microsoft Office	10					20%
	[dbms] ORACLE MOTOR DE BASE DATOS	5		20%			
	[files] Información de Contribuyentes	5		20%	50%		
	[backup] Archivo de Copias de seguridad de la información	50		20%			
	[password] Contraseñas de acceso de usuarios del sistema	10		75%			
	[email] Manejo de correos electrónicos	5					5%
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5		50%			
	[usb] Almacenamientos en Disco Duro	5			50%	20%	
	[printed] Carpetas con la documentación de cada proyecto en ejecución	10			20%		
	[E.18] Destrucción de información	[office] Microsoft Office	5				
[dbms] ORACLE MOTOR DE BASE DATOS		5				50%	
[files] Información de		10				20%	

Tabla 430. (Continuación)

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
[E.18] Destrucción de información	Contribuyentes	50	5%			20%	
	[backup] Archivo de Copias de seguridad de la información	5			50%		
	[password] Contraseñas de acceso de usuarios del sistema	5		75%			
	[email] Manejo de correos electrónicos	5				5%	
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	10		20%	20%		
	[usb] Almacenamientos en Disco Duro	5		20%			
	[printed] Carpetas con la documentación de cada proyecto en ejecución	5		20%			
[E.24] Caída del sistema por agotamiento de recursos	[host] servidores	10				5%	
	[pc] Equipo de computo de mesa	5				50%	
	[HW] Equipos Portátiles	5				20%	
	[os] sistema operativo	10				20%	
	[app] Servidor de aplicaciones	50		50%			5%
	[dbms] ORACLE MOTOR DE BASE DATOS	5					75%
[E.25] Pérdida de equipos-Robo	[HW] Equipos Portátiles	5			20%		
	[usb] Almacenamientos en Disco Duro	10	50%				
	[printed] Carpetas con la documentación de cada proyecto en ejecución	5			20%		
	[files] Información de Contribuyentes	10	5%				

Tabla 44. (Continuación)

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
	[backup] Archivo de Copias de seguridad de la información	50			20%		50%
	[password] Contraseñas de acceso de usuarios del sistema	5					
	[pc] Equipo de computo de mesa	10		20%			
[A.5] Suplantación de la identidad del usuario	[HW] Equipos Portatiles	5			5%		
	[dbms] ORACLE MOTOR DE BASE DATOS	50			5%		50%
	[password] Contraseñas de acceso de usuarios del sistema	10					75%
[A.11] Acceso no autorizado	[host] servidores	5				50%	
	[adm] Administrador de sistemas	5		20%			
	[printed] Carpetas con la documentación de cada proyecto en ejecución	50					20%
	[backup] Archivo de Copias de seguridad de la información	10	75%				
A.24] Denegación de servicio	[host] servidores	5		20%			
	[app] Servidor de aplicaciones	5				75%	20%
	[www] Servicio de internet al que pueden acceder los funcionarios	50		20%			
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	10	75%				50%
[A.26] Ataque destructivo	[host] servidores	5		20%			
	[wifi] Ap para Red Inalámbrica	50				75%	
	[LAN] Red local Switch de 24 puertos	5			20%		75%

Tabla 45. (Continuación)

Relación de amenazas por activo identificando su frecuencia e impacto							
Impacto para cada dimensión %							
Amenaza	Activo	Frecuencia	[A]	[C]	[I]	[D]	[T]
	[dbms] ORACLE MOTOR DE BASE DATOS	10			20%		
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	10		20%			

Fuente: Metodología Magerit Versión 3.

7.2.4. Resultado plan de pruebas. 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 46. 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

Tabla 47. (Continuación)

Código	Vulnerabilidad	Riesgo
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 a los sistemas 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 exponga las posibles problemas

Fuente: Metodología Magerit Versión 3.

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

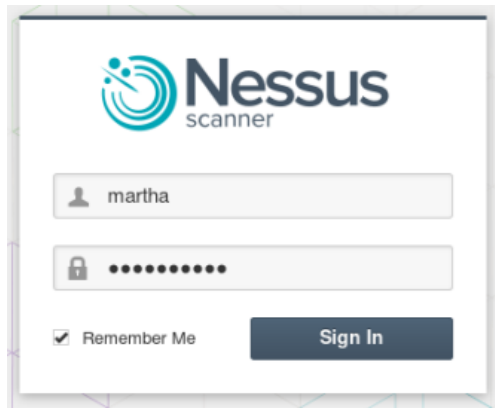
Figura 6. Página web de la Alcaldía de la Jagua de Ibirico.



Fuente. <http://www.lajaguadeibirico-cesar.gov.co/index.shtml>

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

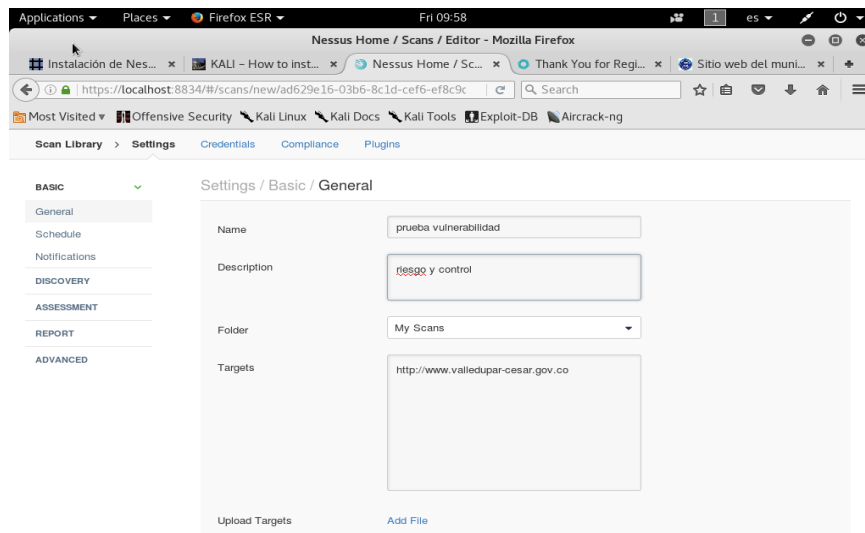
Figura 7. Instalación del scanner Nessus.



Fuente. Nessus maquina virtual

Para escáner el sitio <http://lajaguadeibirico-cesar.gov.co>

Figura 8. Pruebas de vulnerabilidad web



Fuente. Nessus maquina virtual

El análisis que se le realizó al sitio, arrojó 17 vulnerabilidades, solo una 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 9. 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			

Fuente. Nessus maquina virtual

Segunda Metodología: Se revisa el sitio web de la alcaldía de la Jagua de Ibirico <http://www.lajaguadeibirico-cesar.gov.co>, se observa que ofrece información y servicios; a continuación se muestra su página principal donde se observa la barra de menús, esta tiene seis (6) opciones principales:

- Nuestra alcaldía
- Trámites y servicios
- Planeación y ejecución
- Presupuesto y finanzas
- Participación
- Atención a la ciudadanía

En su menú principal se encuentra la opción de trámites y servicios.

En trámites ofrece:

- Incorporación y entrega de las áreas de cesión a favor del municipio
- Permiso de captación de recursos
- Impuesto predial unificado
- Renovación del reconocimiento deportivo a clubes deportivos, clubes promotores y clubes pertenecientes a entidades no deportivas
- Autorización para la operación de juegos de suerte y azar en la modalidad de promocionales
- Facilidades de pago para los deudores de obligaciones tributarias
- Esterilización canina y felina
- Impuesto sobre el servicio de alumbrado público

- Legalización urbanística de asentamientos humanos
- No disponible en línea
- Permiso para espectáculos públicos diferentes a las artes escénicas

En servicio ofrece:

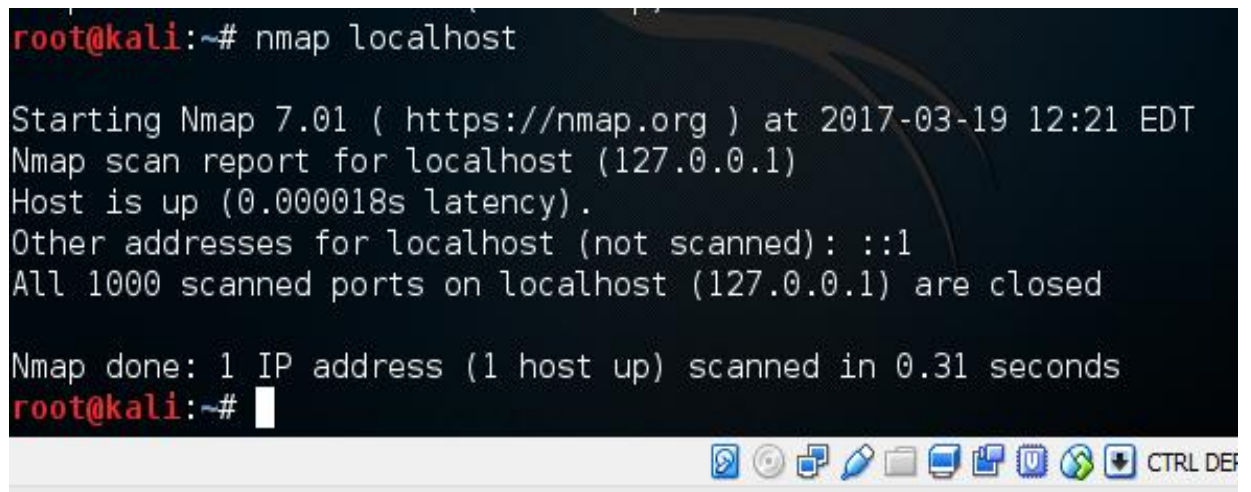
- Actualización de datos de identificación en la base de datos del sistema de identificación y clasificación de potenciales beneficiarios de programas sociales – SISBEN
- Retiro de personas de la base de datos del sistema de identificación y clasificación de potenciales beneficiarios de programas sociales - SISBEN
- Auxilio para gastos de sepelio
- Inclusión de personas en la base de datos del sistema de identificación y clasificación de potenciales beneficiarios de programas sociales - SISBEN
- Encuesta del sistema de identificación y clasificación de potenciales beneficiarios de programas sociales - SISBEN
- Sobretasa municipal o distrital a la gasolina motor
- Copia certificada de planos
- Certificado de residencia
- Certificado de paz y salvo
- Certificado de permiso de ocupación
- Radicación de documentos para adelantar actividades de construcción y enajenación de inmuebles destinados a vivienda
- Certificado de Estratificación Socioeconómica

Determinar mediante pruebas usando herramientas de software (Matriux, Kali Linux, otros) las vulnerabilidades, amenazas y riesgos de seguridad del sitio web de la alcaldía jagua de ibirico. Las pruebas se realizaran para fines educativos, por lo cual no se modificara 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:

Se realiza el escaneo de vulnerabilidades, se escanea los puerto del cliente host para verificar los servicios que se están ejecutando y cuales están abiertos. Primero realizamos un Nmap localhost para saber qué servicios están abierto y cerrados:

Figura 10. Ejecución de pruebas con Nmap.



```
root@kali:~# nmap localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-19 12:21 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000018s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are closed

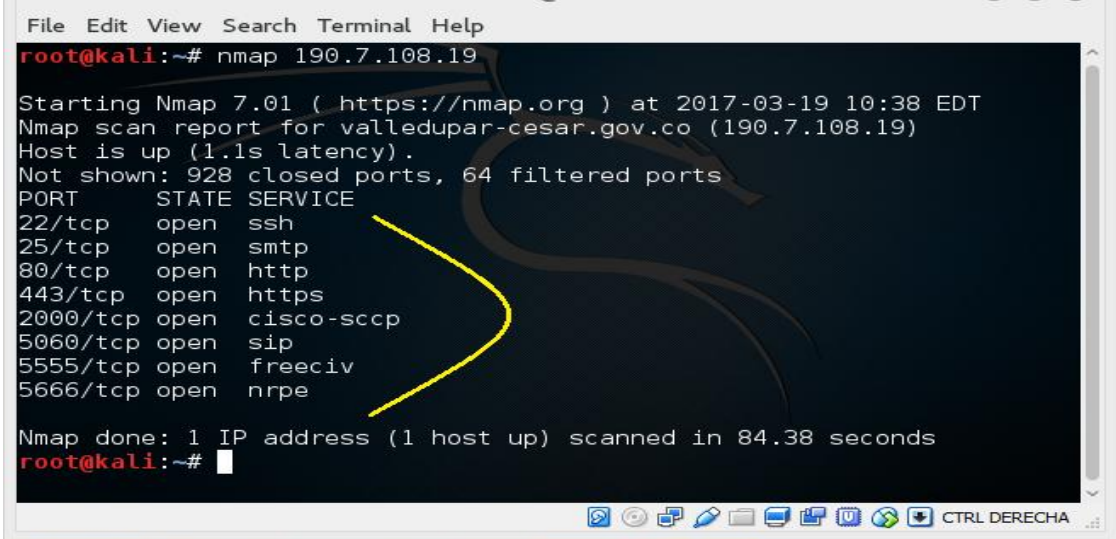
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@kali:~#
```

Fuente. Terminal Kali linux

Se observó que el sitio web de la alcaldía jagua de ibirico, tiene 928 puerto 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, 5555tcp abierto con el servicio freeciv y 5555tcp 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 -O 190.7.108.19 se observa que se está ejecutando en un Linux 2.6:

Figura 11. Resultados arrojadas Nmap



```
File Edit View Search Terminal Help
root@kali:~# nmap 190.7.108.19

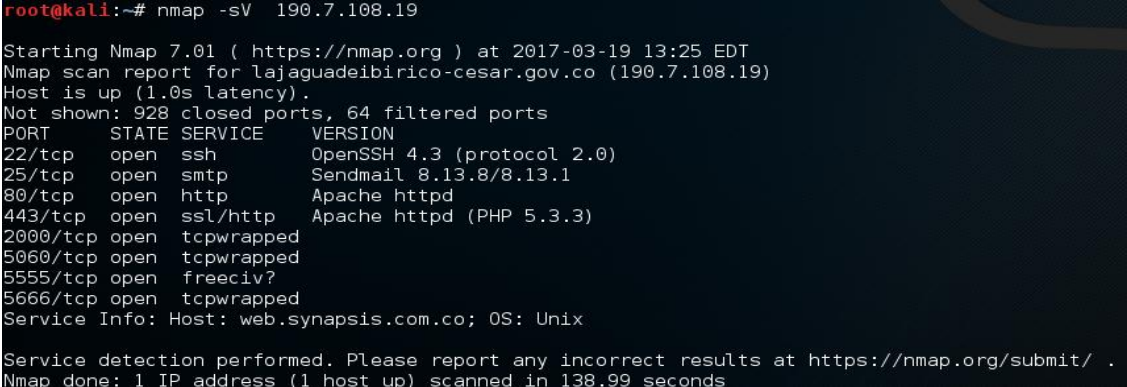
Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-19 10:38 EDT
Nmap scan report for valledupar-cesar.gov.co (190.7.108.19)
Host is up (1.1s latency).
Not shown: 928 closed ports, 64 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
5555/tcp  open  freeciv
5666/tcp  open  nrpe

Nmap done: 1 IP address (1 host up) scanned in 84.38 seconds
root@kali:~#
```

Fuente. Terminal Kali linux

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

Figura 12. Versión servicios Nmap.



```
root@kali:~# nmap -sV 190.7.108.19

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-19 13:25 EDT
Nmap scan report for lajaguadeibirico-cesar.gov.co (190.7.108.19)
Host is up (1.0s latency).
Not shown: 928 closed ports, 64 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.3 (protocol 2.0)
25/tcp    open  smtp         Sendmail 8.13.8/8.13.1
80/tcp    open  http         Apache httpd
443/tcp   open  ssl/http     Apache httpd (PHP 5.3.3)
2000/tcp  open  tcpwrapped
5060/tcp  open  tcpwrapped
5555/tcp  open  freeciv?
5666/tcp  open  tcpwrapped

Service Info: Host: web.synapsis.com.co; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.99 seconds
```

Fuente. Terminal Kali linux

Se realizó un escaneo solo a los puertos 80, 777, 3000 con el comando nmap –PO-p 80:777:3000 de la Ip 190.7.108.19 así:

Figura 13. Escaneos de puertos con Nmap

```
root@kali:~# nmap -PO -p 22,25,80,443 190.7.108.19
Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-19 13:56 EDT
Nmap scan report for lajaguadeibirico-cesar.gov.co (190.7.108.19)
Host is up (0.075s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@kali:~#
```

Fuente. Terminal Kali linux

7.2.5. Determinación del impacto. Para determinar el impacto se midió con las siguientes tablas:

Tabla 48. Nivel de degradación.

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 49. Probabilidad de Ocurrencia

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.

7.2.5.1. 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. $Riesgo = Impacto \times Frecuencia$; por ello se hace la siguiente valoración para la estimación del riesgo:

Tabla 50. Valoración del riesgo.

CLASE DE RIESGO	VALORACIÓN	VALORACIÓN
	CUALITATIVA	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 esta, tendremos que la matriz referente para la estimación del riesgo será la siguiente:

Tabla 51. Implementación de la valoración del riesgo en la Alcaldía

ESTIMACIÓN DEL RIESGO		VULNERABILIDAD (FRECUENCIA)				
		MUY POCO FRECUENTE	POCO FRECUENTE	NORMAL	FRECUENTE	MUY FRECUENTE
IMPACTO	MUY ALTO	5	10	15	20	25
	ALTO	4	8	12	16	20
	MODERADO	3	6	9	12	15
	BAJO	2	4	6	8	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 plasma en la siguiente tabla:

Tabla 52. Clase y estimación de riesgo

CLASE DE RIESGO Y ESTIMACION DEL RIESGO			
Amenaza	Activo	Clase Riesgo	IMPACTO
[N.1] Fuego	[host] servidores	8	6
	[mobile] dispositivos móviles	4	5
	[pc] Equipo de computo de mesa	4	5
	[scan] Equipos de plotter y escanners	8	5
	[HW] Equipos Portátiles	8	6
	[print] Impresoras Laser	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 computo de mesa	7	6
	[scan] Equipos de plotter y escanners	5	7
	[wifi] Ap para Red Inalámbrica	5	5
	[LAN] Red local Switch de 24 puertos	5	5

Tabla 53. (Continuación)

CLASE DE RIESGO Y ESTIMACION DEL RIESGO			
Amenaza	Activo	Clase Riesgo	IMPACTO
[N.7] Desastres naturales. Fenómeno sísmico.	[building] Instalacion física de la entidad	4	6
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	9	7
	[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 computo de mesa	8	8
	[scan] Equipos de plotter y escanners	8	
[I.5] Avería de origen físico o lógico.	[pc] Equipo de computo de mesa	8	8
	[print] Impresoras Lasser	9	
	[router] Enrutadores	9	10
	[backup] sistema de backup	5	
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5	
	[building] Instalacion física de la entidad	9	10
[I.6] Corte del suministro eléctrico	[host] servidores	7	
	[pc] Equipo de computo 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 computo de mesa	8	7
	[print] Impresoras Lasser	8	5
	[wifi] Ap para Red Inalámbrica	9	6
	[LAN] Red local Switch de 24 puertos	5	4
	[app] Servidor de aplicaciones	5	5

Tabla 54. (Continuación)

CLASE DE RIESGO Y ESTIMACION DEL RIESGO			
Amenaza	Activo	Clase Riesgo	IMPACTO
[I.8] Fallo de servicios de comunicaciones	[printed] Carpetas con la documentación de cada proyecto en ejecución	9	10
	[ui] Personal de soporte TI	5	9
	[adm] Administrador de sistemas	5	9
	[wifi] Ap para Red Inalámbrica	5	7
	[LAN] Red local Switch de 24 puertos	7	8
	[Intranet] intranet	7	8
	[www] Servicio de internet al que pueden acceder los funcionarios	5	5
	[email] Manejo de correos electrónicos	4	5
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	4	5
[I.10] Degradación de los soportes de almacenamiento de la información	[backup] sistema de backup Base de datos	5	5
	[backup] Archivo de Copias de seguridad de la información	6	7
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5	7
	[usb] Almacenamientos en Disco Duro	5	5
[E.1] Errores de los usuarios.	[pc] Equipo de computo de mesa	8	5
	[scan] Equipos de plotter y escanners	7	5
	[HW] Equipos Portátiles	5	7
	[print] Impresoras Lasser	5	7
	[print] Impresoras de inyección de tinta	5	5
	[os] sistema operativo	7	6
	[office] Microsoft Office	7	7
	[email] Manejo de correos electrónicos	5	6
	[printed] Carpetas con la documentación de cada proyecto en ejecución	9	4

Tabla 55. (Continuación)

CLASE DE RIESGO Y ESTIMACION DEL RIESGO			
Amenaza	Activo	Clase Riesgo	IMPACTO
[E.2] Errores del administrador	[host] servidores	8	6
	[router] Enrutadores	8	7
	[wifi] Ap para Red Inalámbrica	5	6
	[LAN] Red local Switch de 24 puertos	7	7
	[Intranet] intranet	6	6
	[os] sistema operativo	7	5
	[app] Servidor de aplicaciones	6	7
	[password] Contraseñas de acceso de usuarios del sistema	5	6
	[encrypt] Claves de cifra de Los bancos	7	5
[E.8] Difusión de software dañino	[host] servidores	5	4
	[pc] Equipo de computo de mesa	7	5
	[HW] Equipos Portatiles	7	5
	[os] sistema operativo	8	8
	[dbms] ORACLE MOTOR DE BASE DATOS	5	4
	[www] Servicio de internet al que pueden acceder los funcionarios	5	7
	[email] Manejo de correos electrónicos	5	8
[E.15] Alteración accidental de la información	[office] Microsoft Office	4	5
	[dbms] ORACLE MOTOR DE BASE DATOS	5	8
	[files] Información de Contribuyentes	5	5
	[backup] Archivo de Copias de seguridad de la información	8	5
	[password] Contraseñas de acceso de usuarios del sistema	4	5
	[email] Manejo de correos electrónicos	5	4
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	5	5
	[usb] Almacenamientos en Disco Duro	5	5
[E.18] Destrucción de información	[printed] Carpetas con la documentación de cada proyecto en ejecución	7	8
	[office] Microsoft Office	5	4
	[dbms] ORACLE MOTOR DE BASE DATOS	5	8

Tabla 56. (Continuación)

CLASE DE RIESGO Y ESTIMACION DEL RIESGO			
Amenaza	Activo	Clase Riesgo	IMPACTO
[E.24] Caída del sistema por agotamiento de recursos	[files] Información de Contribuyentes	7	8
	[backup] Archivo de Copias de seguridad de la información	5	7
	[password] Contraseñas de acceso de usuarios del sistema	8	7
	[email] Manejo de correos electrónicos	8	7
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	7	4
	[usb] Almacenamientos en Disco Duro	7	4
	[printed] Carpetas con la documentación de cada proyecto en ejecución	4	5
	[host] servidores	4	5
	[pc] Equipo de computo de mesa	5	7
	[HW] EquiposPortatiles	5	5
	[os] sistema operativo	7	5
	[app] Servidor de aplicaciones	8	5
	[dbms] ORACLE MOTOR DE BASE DATOS	5	7
[E.25] Pérdida de equipos-Robo	[HW] EquiposPortatiles	5	7
	[usb] Almacenamientos en Disco Duro	7	4
	[printed] Carpetas con la documentación de cada proyecto en ejecución	5	4
	[files] Información de Contribuyentes	10	5
	[backup] Archivo de Copias de seguridad de la información	6	5
	[password] Contraseñas de acceso de usuarios del sistema	5	7
[A.5] Suplantación de la identidad del usuario	[pc] Equipo de computo de mesa	10	8
	[HW] EquiposPortatiles	5	8
	[dbms] ORACLE MOTOR DE BASE DATOS	6	7
	[password] Contraseñas de acceso de usuarios del sistema	8	7

Tabla 57. (Continuación)

CLASE DE RIESGO Y ESTIMACION DEL RIESGO			
Amenaza	Activo	Clase Riesgo	IMPACTO
[A.11] Acceso no autorizado	[host] servidores	5	5
	[adm] Administrador de sistemas	5	6
	[printed] Carpetas con la documentación de cada proyecto en ejecución	6	5
	[backup] Archivo de Copias de seguridad de la información	6	6
A.24] Denegación de servicio	[host] servidores	5	4
	[app] Servidor de aplicaciones	5	6
	[www] Servicio de internet al que pueden acceder los funcionarios	6	5
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	7	5
[A.26] Ataque destructivo	[host] servidores	5	6
	[wifi] Ap para Red Inalámbrica	8	7
	[LAN] Red local Switch de 24 puertos	5	5
	[dbms] ORACLE MOTOR DE BASE DATOS	8	5
	[file] Servicio de almacenamiento de información en el servidor de bases de datos.	8	6

Fuente: El autor.

7.3. CONTROLES EXISTENTES CON QUE CUENTA LA ENTIDAD

Se procede a valorar la efectividad de los controles existentes puesto que al contar con una matriz de riesgo ya generada, lo que falta es determinar el nivel de desplazamiento que estos generan sobre el mapa.

Tabla 58. Evaluar controles

Aspectos A Evaluar	Opciones De Respuesta	Valor
Afecta impacto o probabilidad. Permite establecer el movimiento que genera sobre la matriz, si sobre el eje X (probabilidad) o sobre el eje Y (impacto).		
Categoría del control	Control Preventivo	20
	Control Detectivo	15
	Control Correctivo	5
Herramientas para ejercer el control	SI	15
	NO	0
Están definidos los responsables de la ejecución del control y del seguimiento	SI	15
	NO	0
La frecuencia de la ejecución del control y seguimiento es adecuada.	SI	20
	NO	0
El tiempo que lleva el control ha demostrado ser efectivo	SI	20
	NO	0
Está documentado los pasos para el manejo del control	SI	10
	NO	0

Fuente. Libro Metodología Magerit Versión 3.

Tabla 59. Valoración de controles

AMENAZAS	CONTROLES	Tipo de control (afecta impacto o probabilidad)	Categoría	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	Total Puntaje
[N.1] Fuego / [N.2] Daños por agua	Se cuenta con un Extintores por cada oficina y un solo botiquín.	Probabilidad	Preventivo	Si	No	Si	Si	No	75
	Se tiene brigadistas encargados de direccionar y prestar sus servicios de primeros auxilios.	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Simulacro de evacuación con lugar de encuentro	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[N.7] Desastres naturales. Fenómeno sísmico.	se tiene brigadistas encargados de direccionar y prestar sus servicios de primeros auxilios.	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Simulacro de evacuación con lugar de encuentro	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[I.5] Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[I.6] Corte del suministro eléctrico	planta eléctrica	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	estabilizadores equipo de cómputo jefes de oficina	Probabilidad	Detectivo	Si	Si	Si	Si	No	85

Tabla 60. (Continuación)

AMENAZAS	CONTROLES	Tipo de control (afecta impacto o probabilidad)	Categoría	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	Total Puntaje
[I.8] Fallo de servicios de comunicaciones	Se cuenta con dos diferentes canales de internet por si falla alguno de ellos	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Base de datos oracle ejecutada en línea	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[I.10] Degradación de los soportes de almacenamiento de la información	se cuenta con discos duros extraibles con copias de seguridad	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Servicio de almacenamiento de información en el servidor de bases de datos.	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[E.2] Errores del administrador	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[E.8] Difusión de software dañino	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	[email] Manejo de correos electrónicos	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[E.18] Destrucción de información	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	[backup] Archivo de Copias de seguridad de la información	Probabilidad	Preventivo	Si	Si	Si	Si	No	90

Tabla 61. (Continuación)

AMENAZAS	CONTROLES	Tipo de control (afecta impacto o probabilidad)	Categoría	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	Total Puntaje
[E.24] Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[E.25] Pérdida de equipos-Robo	Existe guardias de seguridad que revisan a los equipos que entran y salen de la entidad	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[A.5] Suplantación de la identidad del usuario	El acceso de los usuarios al los recursos tecnológicos se controla a través del directorio activo	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[A.11] Acceso no autorizado	Se cuenta con un sistema de control de acceso biométrico para ingresar a las áreas seguras y cámaras de vigilancia	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	Si	Si	Si	Si	No	90

Tabla 62. (Continuación)

AMENAZAS	CONTROLES	Tipo de control (afecta impacto o probabilidad)	Categoría	Existe una herramienta para ejercer el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada.	El tiempo que lleva el control ha demostrado ser efectivo	Está documentado los pasos para el manejo del control	Total Puntaje
	El acceso de los usuarios al los recursos tecnológicos se controla por el directorio activo	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
A.24] Divulgación de información de autenticación	Se tiene implementada la política de contraseña segura	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
[A.26] Ataque destructivo	Existe un plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	Si	Si	Si	Si	No	90
R7. Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	Probabilidad	Preventivo	Si	Si	Si	Si	No	90

Fuente. Libro Metodología Magerit Versión 3.

7.4. MANUAL DE POLÍTICA Y PROCEDIMIENTOS

Se realizó las políticas de seguridad informática para toda la entidad necesarias para un buen aseguramiento de los datos por parte de los funcionarios; del mismo modo se diseñan los procedimientos para el departamento de TI de la Alcaldía.

7.4.1. Políticas de seguridad de recursos humanos. La Alcaldía de la Jagua de Ibirico-Cesar, teniendo en cuenta la importancia que tiene el factor humano para el cumplimiento de los objetivos institucionales y que son los responsables del uso y administración de los activos de información, se compromete, a que la vinculación de nuevos funcionarios se realizara siguiendo un proceso formal de selección, acorde con la legislación vigente y las normas establecidas por la CNSC. Y de esta manera contar con personal idóneo para desempeñar las funciones para las cuales han sido vinculados a la organización.

Así mismo se requiere su compromiso y conocimiento con respecto a la seguridad de la información.

7.4.2. Normas relacionadas con la vinculación de nuevos Empleados. El personal de Recursos Humanos debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la Alcaldía de la Jagua de Ibirico-Cesar.

El personal de Recursos Humanos debe certificar que los empleados de la Alcaldía de la Jagua de Ibirico-Cesar firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

7.4.3. Personal provisto por terceras partes. El personal provisto por terceras partes que realicen labores en o para la Alcaldía de la Jagua de Ibirico-Cesar, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

7.4.4. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros. El personal de Recursos Humanos debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los empleados del instituto llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Recursos Humanos debe reportar las novedades de cada funcionario de la Alcaldía de la Jagua de Ibirico-Cesar, ya sea cambios de rol, vacaciones o retiros para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados.

7.4.5. Políticas de control de cambios de datos. Las modificaciones, actualización o borrado de datos institucionales de la Alcaldía de la Jagua de Ibirico-Cesar, deben ser realizados a través de la interfaz de usuario de los sistemas de información que procesan dichos datos, y según los roles de cada usuario. Las modificaciones realizadas fuera de la interfaz de usuario a los sistemas de información, se consideran una amenaza a la integridad de los mismos.

7.4.6. Normas relacionadas con el control de cambios de los datos. La modificación sobre datos deja un registro de auditoría, que es protegido de posibles modificaciones. En caso de no poder cumplir con la política anteriormente planteada se debe realizar la solicitud se por escrito, con visto bueno del dueño del activo y las modificaciones, solo pueden ser realizadas por el personal de soporte del ambiente de producción.

7.4.7. Inventario de activos. Los activos de información de la Alcaldía de la Jagua de Ibirico-Cesar, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que regulen el uso adecuado de la misma.

Los dueños de los procesos o quien haga sus veces deben identificar y elaborar un inventario de los activos de información aplicando el procedimiento establecido, el proceso de gestión documental y sus procedimientos asociados y designar una persona responsable de consolidar y administrar los activos de información.

El propietario del activo de información debe:

- Hacer un análisis de riesgos Anual, de los activos de información de su proceso.
- Tomar decisiones y acciones para eliminar, mitigar, transferir o aceptar los riesgos.
- Clasificar la información de acuerdo a la importancia de esta.
- Verificar anualmente o cada vez que sea necesario, el inventario de los activos de información con el fin de mantenerlos actualizados.
- Monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- La Coordinación de Archivo debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

7.4.8. Política de Clasificación y Manejo de la Información. La Alcaldía de la Jagua de Ibirico-Cesar debe establecer los niveles adecuados para la clasificación de la información de la organización teniendo en cuenta la sensibilidad de los mismos con el fin que sea una guía para que los dueños de los activos de información, la clasifiquen y cataloguen para determinar las acciones a tomar para la protección de la información. La institución debe proporcionar los recursos necesarios para la aplicación de controles que lleven a preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los empleados de la Alcaldía de la Jagua de Ibirico-Cesar y personal provisto por terceras partes que se encuentre autorizado y necesiten recurrir a su uso para el cumplimiento de las tareas asignadas.

El propietario del activo de información debe:

- Clasificar su información de acuerdo con la guías de clasificación de la Información establecida.
- Son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

- La información física y digital de la Alcaldía de la Jagua de Ibirico-Cesar debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- La Dirección de Tecnología junto con la Oficina de Riesgo deben definir los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activos.

7.4.9. Política de Gestión de copias de respaldo. Por medio de procedimientos previamente establecidos, la Alcaldía de la Jagua de Ibirico-Cesar certificara la generación de copias de respaldo y almacenamiento de su información, y proporcionara los recursos necesarios y mecanismos para la realización de estas actividades. Los propietarios de la información, con el apoyo del área de Tecnología, encargada de la generación de copias de respaldo, establecerán cuáles serán los lineamientos y estrategias a seguir y los tiempos que se guardara el respaldo y almacenamiento de la información.

Se determinara un mecanismo para guardar las copias generadas de información, bien sea fuera de las instalaciones de la organización o por medio de servicios en la nube dependiendo de la clasificación de la información (información sensible, critica, publica) se le dará el tratamiento alterno para el almacenamiento. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

7.4.10. Normas para la Gestión de copias de respaldo. Es responsabilidad de los usuarios de la plataforma tecnológica de la Alcaldía de la Jagua de Ibirico-Cesar identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

La Dirección de TI de Alcaldía de la Jagua de Ibirico-Cesar debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información.

El área de TI debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para validar su integridad y si se encuentran en condiciones óptimas para ser usadas en caso de ser requerido.

La dirección de TI debe designar personas idóneas que generen y adopten los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, asegurando su integridad y disponibilidad.

7.4.11. Política de Control de acceso a áreas seguras. Las áreas seguras y sus controles están definidos de acuerdo a los lineamientos establecidos en el documento de procedimientos de Control de acceso a áreas seguras. La organización proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. De igual manera se definirán controles para mitigar las amenazas físicas externas e internas a las que se esté expuesta la Alcaldía de la Jagua de Ibirico-Cesar, como se definió en el plan de tratamiento de riesgos se definirán los controles para cuidar las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

7.4.12. Normas Control de acceso a áreas seguras. Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones del instituto; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

Los ingresos y egresos de personal a las instalaciones de la Alcaldía de la Jagua de Ibirico-Cesar deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Dirección de TI autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

La Dirección de TI debe discontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

7.4.13. Políticas de Desarrollo de aplicaciones. Teniendo en cuenta que los sistemas de información son el soporte principal para el funcionamiento de los procesos misionales de la Alcaldía de la Jagua de Ibirico-Cesar, se busca brindar seguridad a los aplicativos institucionales desde el momento mismo del integral de las decisiones de arquitectura del software a construir.

Las áreas propietarias de sistemas de información, la Dirección de Tecnología y la Oficina de Riesgos incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

7.4.14. Normas de Desarrollo de aplicaciones. La Dirección de TI debe determinar cuáles serán las metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro del instituto formalmente asignada.

Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

7.4.15. Política De Seguridad De La Información. La presente política de Seguridad de la Información enmarcada en el SGSI, establece el sentido general de la alta Dirección y define el alcance, límite y principios de gestión y de acción con relación a la seguridad de la información.

7.4.16. Roles De Seguridad De La Información. Definir los roles de seguridad de la información de acuerdo a las funciones del colaborador de la alcaldía.

7.4.17. Políticas De Seguridad Y Privacidad De La Información. Las políticas enunciadas a continuación se rigen bajo la regulación actual del gobierno de Colombia, los límites y aplicabilidad de las mismas se rigen bajo el “numeral 3. Alcance” este documento.

7.4.18. Política De Teletrabajo. En caso de un colaborador requerir tener teletrabajo, se debe proteger la información a la que se tiene acceso, de los lugares en los que se realiza Teletrabajo y/o Acceso Remoto, para salvaguardar la confidencialidad y privacidad de la misma.

- Definir los tipos de usuarios que dispondrán de modalidad de teletrabajo y/o Acceso Remoto.
- Establecer un compromiso por parte del Teletrabajador con la seguridad de la información que se trate en el equipo de cómputo, sobre los riesgos derivados de la utilización de los equipos informáticos, riesgos de ciberseguridad y su prevención.
- Llevar un seguimiento de las conexiones remotas a los servicios de la alcaldía
- Verificar el acceso remoto este aprobada por la el líder de la dependencia y llevar un control de los usuarios que trabajan bajo esta modalidad.
- Verificar que sean cerradas todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción “desconectar” o “cerrar sesión”.

- Establecer medidas, en el sitio de teletrabajo, para evitar el acceso fortuito a información de la alcaldía por otros usuarios del equipo aparte del propio empleado: familiares o similar.

7.4.19. Política Para Dispositivos Móviles. Monitorear, proteger y supervisar la información que es almacenada en los dispositivos móviles, para mitigar los riesgos asociados al acceso y divulgación no autorizada a la información.

- Mantener un inventario actualizado de los medios removibles existentes, sus propietarios y la relación de la información contenida en cada uno de ellos.
- Instalar un software de antivirus
- la información que se guarda en medios extraíbles de almacenamiento de vigilarse para evitar la fuga de información.
- Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.), para mitigar el evento de fuga de información y propagación de virus en la red de la alcaldía
- Eliminar la información que se encuentre en la carpeta pública mínimo dos veces al mes.
- Implementar un método de bloqueo automático para los estados de inactividad.
- Establecer las configuraciones aceptables, para los dispositivos móviles institucionales y/o personales, de la alcaldía
- Realizar el intercambio de información entre dependencias de la alcaldía a través de las carpetas compartidas, pero bajo unas reglas específicas
- Hacer buen uso del acceso a redes inalámbricas en los equipos de cómputo asignados por la alcaldía y/o personales de acuerdo a sus funciones laborales.
- Evitar almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

- Evitar efectuar transferencias financieras, cualquier computador público o café internet.
- Evitar usar los dispositivos móviles de la alcaldía, donde no se pueda mitigar la pérdida

7.4.20. Política Gestión De Activos. Establecer los límites y procedimientos de los activos, analizar su administración y responsabilidades. Es importante definir los controles para salvaguardar la información creada, procesada, transmitida y/o almacenada de sus procesos, con el fin de minimizar impactos financieros, operativos en la alcaldía

- Identificar los activos de información en cada proceso de la alcaldía con el apoyo Del líder de información.
- Verificar el inventario de los activos de información.
- Garantizar que los activos de información cuenten con los niveles pertinentes de seguridad.
- Velar por que se suscriba un acuerdo de confidencialidad de carácter vinculante Alcaldía de La Jagua de Ibirico – Cesar y la persona que accederá a la información, toda vez, que la información que se intercambia y/o accede es de carácter reservado y/o confidencial, con el apoyo del proceso de Talento Humano y el proceso de Gestión Contractual.
- Definir las políticas de copias de respaldo de los activos de información.
- Establecer los controles de ingreso a oficinas, salas de telecomunicaciones, servidores y las áreas de trabajo que contengan información clasificada como reserva.
- Asegurar y gestionar la devolución del activo (equipos tecnológicos e información) que estaba bajo la responsabilidad del contratista o servidor público, antes de su desvinculación y/o cambio de contratación laboral, con la alcaldía.

- Establecer un acuerdo de confidencialidad de carácter vinculante entre la Alcaldía de La Jagua de Ibirico – Cesar y la persona que accederá a la información de la misma.
- Velar por que los colaboradores de la alcaldía, comprendan sus responsabilidades frente a la seguridad antes, durante y al cambiar y/o finalizar la contratación y/o relación laboral con la alcaldía.
- Ejecutar un borrado seguro a fin de evitar la recuperación de la información;
- Llevar a cabo la implementación de controles para los activos de información que involucran operaciones financieras en la alcaldía
- Coordinar la seguridad de las redes y procesamiento de información
- Restringir el acceso a correos personales, redes sociales y en general a otros sitios no asociados con las funciones del colaborador

7.4.21. Política De Control De Acceso. Implementar controles de acceso a los activos de información, con el fin de otorgar acceso solo por personas y medios autorizados, por tanto, la alcaldía, se debe determinar los mecanismos de protección y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos.

- Identificar, documentar y autorizar explícitamente que colaboradores, servidores públicos, contratistas y terceras partes, pueden acceder a los sistemas de información, recursos tecnológicos, áreas seguras entre otros.
- Autorizar los accesos a los sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y bajo la autorización de su jefe inmediato.
- Impartir controles de acceso, para restringir el ingreso a las áreas físicas e instalar cámaras de video que minimicen los riesgos.
- Emplear medidas de autenticación y control que ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones.
- Asegurar todas las áreas físicas

- Restringir el acceso a las áreas físicas e instalar cámaras de video, que cubran el menos el colaborador que utilice el equipo de cómputo.
- Proteger los servicios de procesamiento de información con los controles de acceso adecuados.

7.4.22. Política Sobre El Uso De Controles Criptográficos

- Salvaguardar la información a través del uso de herramientas criptografía, a fin de proteger la confidencialidad, la autenticidad y la integridad de la información.
- Estandarizar las herramientas y mecanismos de cifrado (simétricos y asimétricos) de la alcaldía las técnicas de cifrado deben estar alineadas a los requisitos legales del estado colombiano.
- Evitar la modificación, pérdida o destrucción de las claves necesarias para descifrar la información protegida, de acuerdo al procedimiento de recuperación de información cifrada ("key scrow").
- Garantizar la confidencialidad en el intercambio de las de las claves.

7.4.23. Política De Escritorio Y Pantalla Limpia. Mantener limpio el escritorio físico y la pantalla del computador, así como las instalaciones donde se procesa información de la alcaldía.

- Mantener el escritorio físico limpio y organizado
- Mantener la pantalla del equipo limpia, libre de iconos innecesarios
- Bloquear el equipo de cómputo cada vez que se retire de su puesto de trabajo

7.4.24. Políticas De Seguridad Para Protección De Activos Informáticos.

Los activos informáticos abarcan dos categorías, así:

Activos Informáticos Tangibles: Corresponden al hardware.

Activos Informáticos Intangibles: Corresponden al software, manuales y bases de datos.

7.4.25. Clasificación de la información de la Empresa o de Terceros manejada Internamente

Información Pública: A la cual tienen acceso todas las personas que trabajan o que se relacionan directa o indirectamente con la entidad. No implica control de acceso. Ejemplo: Publicada en la Página de Internet (WEBSITE), carteleras de la Empresa, Folletos, Informe de Gestión Corporativo Anual, etc.

Información Privada: Es aquella a la cual pueden acceder y usar el personal de empleados de la Empresa, pero no así personas externa o ajena a la misma.

Información Confidencial: Archivos o tablas cuyo acceso está permitido solo para algunas pocas áreas o usuarios de la Empresa o de sus contratistas (Ej. Revisor Fiscal, Asesor de Riesgos).

Información Secreta: Aquella a la que pueden acceder uno o pocos directivos de Alcaldía

7.4.26. Responsabilidad sobre los activos. Cada activo importante o valioso de información debe tener un propietario designado formalmente que es responsable de establecer la seguridad de dicho activo y garantizar que se mantenga su adecuada protección.

7.4.27. Mantenimiento del Inventario de Activos de Información. La División de Sistemas debe contar con un inventario formal, clasificado y actualizado de todos los activos de información. La clasificación de dichos activos debe realizarse en función de su importancia, criticidad, exposición a riesgos, integridad y disponibilidad para la Entidad.

7.4.28. Manejo de Información Financiera. La información financiera debe clasificarse como altamente confidencial y se deben tomar las medidas de seguridad necesarias (técnicas y administrativas) que protejan tal información de accesos no autorizados.

7.4.29. Etiquetado de información. Toda activo de información debe tener una etiqueta claramente visible a fin que los usuarios conozcan quien es el propietario y cuál es el nivel de clasificación designado.

7.4.30. Grabación periódica de datos por usuarios. A fin de prevenir daños o pérdida debido a malos funcionamientos del sistema o fallas de energía, los usuarios de sistemas de información que crean o modifican archivos de datos, deben grabar su trabajo de manera periódica usando las mejores prácticas.

7.5. POLITICAS DE SEGURIDAD PARA LA ADMINISTRACIÓN DEL HARDWARE Y DEL PROCESAMIENTO DE LA INFORMACIÓN

7.5.1. Especificación de los requisitos para los nuevos equipos. Las requisiciones de compras significativas de nuevos equipos deben contar con un Expediente Técnico que detalle la especificación de los requerimientos del usuario, los requisitos de Seguridad de la Información, la prioridad, el cumplimiento de estándares técnicos y funcionales, y la relación con los objetivos a corto y largo plazos de la Entidad.

7.5.2. Instalación de nuevos equipos. Todas las nuevas instalaciones de equipos, y sus respectivos requisitos de Seguridad de la Información, deben planificarse formalmente y notificarse a los interesados con la debida anticipación.

7.5.3. Prueba de equipos y sistemas. Todo equipo debe probarse exhaustivamente y pasar por un proceso de aceptación formal de usuarios antes de ser transferido al entorno de producción.

7.5.4. Gestión y uso de documentación de hardware. La documentación de hardware debe estar siempre actualizada y fácilmente accesible para el personal autorizado de soporte o mantenimiento

7.5.5. Desarrollo y Mantenimiento de Software Aplicativo. En todos los proyectos de desarrollo o mantenimiento de software aplicativo, sea por analistas y programadores internos o externos, el Jefe de la División de Sistemas debe garantizar la aplicación razonable de los siguientes estándares:

NTC 3585 - Sistemas de procesamiento de la información.

NTC 4243 - Tecnología de la información. Proceso del Ciclo de Vida del Software.

7.5.6. Compra de Software Aplicativo Comercial. Igualmente se deben aplicar los siguientes estándares para adquisición de software comercial, cuando sea necesario y razonable, de acuerdo con el criterio profesional del Jefe de la División de Sistemas:

NTC 3560 - Sistemas de procesamiento de la información.

NTC 5415-4 - Tecnología de la información. Evaluación del producto de software.

7.5.7. Políticas De Seguridad De Las Aplicaciones Del Sistema

7.5.7.1. Validación de los datos de entrada: Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la Entidad debe realizarse, de manera obligatoria, el control de datos de entrada, considerando, como mínimo, los procedimientos de consistencia de datos, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.

7.5.7.2. Control del proceso interno: Todo sistema en producción debe contemplar el control de los datos en proceso. Dichos controles deberán ser diseñados conjuntamente con el dueño del sistema. Como mínimo se debe considerar controles externos de integridad de datos así como momentos de ejecución de programas.

7.5.7.3. Validación de los datos de salida. Como parte del proceso de diseño, desarrollo y/o implementación de todo software en la Entidad debe existir, de manera obligatoria, un procedimiento para controlar los datos de salida, considerando, como mínimo, procedimientos de consistencia de datos de salida, correspondencia a las autorizaciones y privilegios de usuario, y procedimientos de manejo de errores.

7.5.7.4. Uso de los controles criptográficos. La Entidad debe evaluar constantemente, mediante un análisis de riesgos, qué información requiere ser protegida con medidas criptográficas.

7.5.7.5. Uso de técnicas de encriptación. Las técnicas de encriptación a ser usadas en la Entidad deben considerar las regulaciones y restricciones nacionales e internacionales. Antes de la transmisión, se deben coordinar los procedimientos que utilizarán el emisor y el receptor.

7.5.7.6. Firmas digitales. La conveniencia y viabilidad, así como los casos en los que se puede usar firmas digitales debe analizarse conjuntamente entre la parte

técnica y legal de la Entidad, teniendo en cuenta toda la legislación relativa que describe las condiciones en las que una firma digital tiene validez legal.

7.5.7.7. Seguridad de los archivos del sistema. La operación y administración de sistemas de la Entidad debe llevarse a cabo siguiendo procedimientos diseñados y documentados detalladamente (REFERENCIAR O ELABORAR) según las mejores prácticas debidamente aprobadas por los dueños de los sistemas.

7.5.8. Políticas De Control De Acceso Lógico A La Información De Los Usuarios.

7.5.8.1. Asignación de identificador de usuario a nuevos empleados: Se debe aplicar el procedimiento actual (referenciarlo) de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información de la Entidad.

7.5.8.2. Privilegios de acceso. La asignación de privilegios de acceso en los sistemas de la Entidad debe controlarse mediante un proceso formal de autorización, en el cual debe participar el usuario Jefe del área usuaria del sistema y éste debe corresponder con el perfil funcional del cargo.

7.5.8.3. Uso de contraseñas alfanuméricas de usuarios o de números: Las contraseñas otorgadas a los trabajadores son privadas y altamente confidenciales. La violación a dicha confidencialidad dará lugar a una acción disciplinaria.

7.5.8.4. Consideraciones para el manejo de clave de accesos: Debe evitarse el uso de contraseñas triviales o fáciles de adivinar, como nombres, números de la placas de vehículos, fechas del nacimiento, o similares; la contraseña no debe almacenarse en teclas de función programables, debe ser cambiada si llega a ser conocida por personas no autorizadas, entre otras.

El Sistema le solicitará automáticamente al usuario que cambie su clave de acceso cada 90 días.

Al escoger una clave de acceso, el usuario debe evitar asociaciones obvias, como nombres de familiares y/o mascotas, números telefónicos, fechas importantes, número de código de empleado, marca de su auto, dirección, etc.

Debe evitarse anotar la clave de acceso en medios visibles.

7.5.8.5. Control de acceso al sistema operativo: El acceso a comandos del sistema operativo debe restringirse para que solamente las personas administrativas de la división de sistemas que puedan ejecutar dichos comandos. Las funciones de administración de dichos sistemas deben requerir aprobación específica.

7.5.8.6. Aislamiento de sistemas sensibles o altamente confidenciales. Los controles de acceso para sistemas de información altamente confidenciales deben ser fijados en concordancia con la clasificación de los activos de información a ser protegidos.

7.5.8.7. Seguimiento de accesos y usos del sistema: Se debe advertir a todos los empleados que en caso de incidentes de seguridad, es necesario registrar y conservar evidencias o pistas para uso del Jefe División de Sistemas.

7.5.8.8. Monitoreo de accesos y uso del sistema: Todas las transacciones registradas con la clave de acceso serán de exclusiva responsabilidad de cada usuario en particular y podrán ser objeto de seguimiento al ser registradas automáticamente en los archivos LOG's.

7.5.8.9. Uso de equipos portátiles de cómputo: Las personas que usan computadoras portátiles fuera de la Entidad deben conocer los riesgos de Seguridad de Información referidos a equipos portátiles e implementar las protecciones apropiadas para reducir al mínimo dichos riesgos.

7.5.8.10. Difusión de las políticas a contratistas y trabajadores temporales: Se entregará formalmente un resumen de las Políticas de Seguridad de la Información a todo contratista y/o trabajador temporal antes del inicio de sus servicios.

7.5.8.11. Brechas de confidencialidad de terceros: Las violaciones de confidencialidad de terceros deben ser reportadas al Oficial de Seguridad de la Información tan pronto como sea posible.

7.5.9. Políticas Sobre Capacitación En Seguridad De La Información

7.5.9.1. Capacitación en Seguridad de la Información a trabajadores: Como primera medida fundamental en la administración de la seguridad informática, se debe priorizar la capacitación y actualización continuada al Jefe de la División de Sistemas, quien es responsable de su divulgación al interior de la Empresa.

La capacitación en Seguridad de la Información se debe impartir de manera individual, obligatoria y actualizada a todos los trabajadores, cuando sea necesario.

Se debe concientizar en temas de seguridad de la información al personal permanente de la Entidad mediante información actualizada sobre amenazas existentes y las medidas de seguridad apropiadas.

7.5.9.2. Capacitación en Seguridad de la Información a personal nuevo. El personal nuevo debe recibir capacitación básica en Seguridad de la Información como parte del proceso de inducción.

7.5.9.3. Capacitación en Seguridad de la Información al personal técnico. La capacitación del personal técnico en Seguridad de la Información deberá estar actualizada y acorde con la responsabilidad de configurar y mantener las protecciones requeridas por la Entidad.

7.5.9.4. Respuesta ante incidentes y malos funcionamientos de la seguridad.

Investigación de causas e impacto de incidentes. Los incidentes de Seguridad de la Información deben ser investigados apropiadamente por personal debidamente capacitado.

7.5.9.5. Reporte de incidentes de seguridad.

Los incidentes, sospechas de incidentes y brechas de seguridad de la información deben reportarse al Jefe División de Sistemas lo más rápidamente posible para agilizar las actividades de identificación de daños, reparación y recuperación, así como facilitar la recolección de evidencias.

8. RECURSOS NECESARIOS

Recursos necesarios para realizar el proyecto a mayor cabalidad.

Tabla 63. Recursos Humanos

CANTIDAD	RECURSOS HUMANOS
1	Ingeniero de sistemas encargado de la oficina de las tic
3	Personas encargadas de toda la información y procesos
1	Ingeniera de sistemas

Fuente Propia

Tabla 64. Recursos Tecnológicos

CANTIDAD	RECURSOS TECNOLÓGICOS
1	Equipo de computo
	Información de la alcaldía de la jagua de ibirico
	Internet

Fuente Propia

9. CRONOGRAMA DE ACTIVIDADES

Tabla 21. Cronograma de actividades

CRONOGRAMA DE ACTIVIDADES																	
FASES	Mes	FEBRERO				ABRIL				MAYO				JUNIO			
	Semanas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
FASE INICIALIZACION																	
Entrega propuesta																	
FASE PLANEACION																	
Describir mediante la Declaración de Aplicabilidad (SoA) la situación actual de la alcaldía municipal de la jagua de Ibirico																	
FASE EJECUCUION																	
Diseñar el análisis de riesgo mediante la metodología de Magerit de la alcaldía municipal de la jagua de Ibirico																	
Identificar los controles existentes con que cuenta la entidad con la norma ISO 27001:2013																	
FASE APLICACIÓN																	
Definir un manual de política y procedimientos a seguir en pro de mitigar posibles amenazas en los recursos informáticos de la alcaldía.																	

Fuente Propia

10. CONCLUSIONES

El diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013, es un herramienta que trae beneficios ya que le permite identificar los diferentes aspectos a la hora de utilizar un modelo de seguridad de la información.

La falta de controles que protejan la información, genera consecuencias graves para la alcaldía, esto afecta datos indispensables para la entidad, por lo que implementar controles adecuados y efectivos, le brinda una seguridad a la información. Es de vital importancia implementar mecanismo de control sobre el acceso de los dispositivos informáticos de la red de la entidad, con el objetivo de garantizar que solo pueden acceder los dispositivos autorizados.

Al realizar las tablas con la metodología MAGERIT se puedo observar los factores tanto naturales como no naturales de todos los activos con que cuenta la entidad, de igual manera se observo los activos que se ven afectados por cada uno de los factores de amenaza, así como la medición de la frecuencia o probabilidad de ocurrencia y el impacto que causa de llegar a concretarse, arrojando resultados no favorables para la integridad, confidencialidad de la información.

Al identificar controles existentes que emplea la alcaldía, en pro del beneficio de toda la entidad pública, como la de restringir la instalación de software por parte de los usuarios, el de revisar los equipos de computo que entran y salen, entre otras. Se observo que se cumple un 60 % por ciento de los controles que maneja la entidad.

Se realizo políticas y procedimientos de seguridad informática para la entidad para la protección de los datos por parte de los funcionarios y el departamento de TI de la Alcaldía. De esta manera es necesario establecer un plan anual de capacitación, formación y sensibilización en seguridad, con el objetivo de contar con sentido de pertenencia sobre la seguridad por parte de funcionarios y terceros que laboran para la entidad.

11. RECOMENDACIONES

La entidad requiere implementar una serie de controles con el objetivo de fortalecer su seguridad y poder dar cumplimiento a los requerimientos establecidos en la norma ISO 27001:2013.

Es necesario garantizar la debida ejecución de los controles y plan de acción que se pretenden llevar a cabo para mitigar las brechas encontradas, ya que la mayoría de estos planes de acción requiere un componente tecnológico.

Es preciso que la entidad evalúe la viabilidad de algunas políticas propuestas, debido a que su implementación demanda la adquisición de herramientas y/o soluciones tecnológicas, ya que la entidad pueda contar con un buen aseguramiento de los datos por parte de los funcionarios;

Realizar campañas de seguridad de la información, con el propósito de poder generar un sentido de pertenencia y apropiación en temas de seguridad en cada uno de los funcionarios de la entidad, y concientizar sobre los riesgos que pueden afectar la seguridad de la información.

BIBLIOGRAFIA

AMUTIO GÓMEZ, Miguel Ángel; CANDAU Javier., y MAÑAS José Antonio
MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los
Sistemas de Información. COLECCIÓN: Libro III - Guía de Técnicas. (Madrid),
2012.

BENCHIMOL, Daniel. Hacking COLECCIÓN: desde Cero. (Buenos Aires
Argentina), 2011.

CANCELADO GONZÁLEZ, Alberto. Administración de riesgos en tecnología
informática (España), 2003.

DERRIEN, Yann; Técnicas de la Auditoría Informática: La dirección de la misión
de la auditoría, (México D.F), 1995.

GÓMEZ FERNÁNDEZ, Luis y FERNÁNDEZ RIVERO Pedro. Cómo implantar un
SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de
Seguridad. (España), 2015.

ICONTEC, Norma Técnica NTC-ISO-IEC 27001, 2013. Tecnología De La
Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De
La Información (SGSI). Requisitos. (Bogota DC), 2006.

MINISTERIO DE COMUNICACIONES. Informe Final – Modelo De Seguridad De
La Información–Sistema Sansi – SGSI - Modelo De Seguridad De La Información
Para La Estrategia De Gobierno En Línea. (Bogotá), 2008.

MINTIC, Guía para la Implementación de Seguridad de la Información en una
MIPYME. (Bogotá), 2016.

MORENO, F. La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. 4ed. (Bogotá), 2009.

TORI, Carlos. Hacking ético. (Rosario Argentina), 2008.

ANEXO A

RESUMEN ANALITICO EDUCATIVO RAE

TÍTULO DEL DOCUMENTO	DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD INFORMATICA PARA LA ALCALDIA MUNICIPAL DE LA JAGUA DE IBIRICO – CESAR BASADO EN LA NORMA ISO 27001:2013
AUTOR	MARTHA LUCIA BRÍÑEZ BAUTISTA
AÑO DE LA PUBLICACIÓN	2017
DESCRIPCIÓN: Trabajo de grado La alcaldía no cuenta con sistema de información adecuado, lo que entorpece establecer el estado actual de seguridad, información de los funcionarios, procesos y tecnología, y de esta manera no se ve reflejado una planeación e identificación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.	
PALABRAS CLAVES	Seguridad de la Información, Norma NTC ISO 27001:2013, Metodología Magerit.
FORMULACIÓN DEL PROBLEMA: ¿Cómo Un Sistema de Gestión de Seguridad de la Información le proveerá a la alcaldía municipal de la jagua de Ibirico, mejorar la seguridad de la información de la entidad y la gestión de los riesgos asociados al uso de la información?	
2.1 OBJETIVO GENERAL Diseño de un sistema de gestión de seguridad informática de la alcaldía de La Jagua de Ibirico mediante la aplicación con la norma ISO 27001:2013	
2.2 OBJETIVOS ESPECÍFICOS <ul style="list-style-type: none">• Describir mediante la Declaración de Aplicabilidad (SOA) la situación actual de la alcaldía municipal de la jagua de Ibirico.• Diseñar el análisis de riesgo mediante la metodología de MAGERIT de la alcaldía municipal de la jagua de Ibirico.• Identificar los controles existentes con que cuenta la entidad con la norma ISO 27001:2013.• Definir un manual de política y procedimientos a seguir en pro de mitigar posibles	

amenazas en los recursos informáticos de la alcaldía.

CONTENIDO:

Las tecnologías de información y comunicación en conjunto con el internet han abierto sin números de posibilidades al acceso a la información, manejando un único objetivo y es el de salvaguardar la privacidad de la información obtenida a través de los sistemas, al igual que han ofrecido muchos beneficios ha estado expuesto a nuevos riesgos que abarcan la seguridad de la misma. ²⁵

En la actualidad las empresas u organizaciones de cualquier tipo deben tener en cuenta dentro de su plan la protección de la información, la creación de políticas y controles en busca de garantizar la información en el momento y a un futuro, puesto el de optar por sistemas seguros hará que tu entidad este a salvo de riesgos que se puedan volver en amenazas.

La seguridad de los sistemas informáticos así como de unas políticas bien fijadas en la gestión de información de datos y usuarios que sean precavidas a la hora del acceso en los entornos tecnológicos ya que muchas veces se ha comprobado que son los más atacados por hackers.

La aplicación de niveles de seguridad, es un factor diferenciador, y claro generador de confianza con valor incalculable para las empresas, puesto que hoy en día, los servidores web tienen que estar protegidos frente a cualquier tipo de amenazas y estar preparados ya que sus usuarios de una u otra forma se sentirán seguro de tener su información a salvo de posibles riesgos, que de una u otra manera se podrían presentar.

METODOLOGÍA: Esta investigación se realizó bajo los lineamientos de la metodología ISO 27001: 2013 y siguiendo los pasos básicos para la puesta en marcha de cualquier proyecto los cuales son: Análisis y observación de la empresa a auditar, planificación de la auditoria, ejecución de la auditoria e informe final. Para la consecución de las etapas anteriores se trabajó bajo los parámetros que disponen los servicios de auditoría y pruebas de seguridad informática los cuales se detallan en los siguientes pasos:

1. Describir mediante la Declaración de Aplicabilidad (SOA) la situación actual de la alcaldía municipal de la jagua de Ibirico.
2. Diseñar el análisis de riesgo mediante la metodología de MAGERIT de la alcaldía municipal de la jagua de Ibirico.
3. Identificar los controles existentes con que cuenta la entidad con la norma ISO 27001:2013.
4. Definir un manual de política y procedimientos a seguir en pro de mitigar posibles amenazas en los recursos informáticos de la alcaldía.

²⁵ <http://aprendeenlinea.udea.edu.co/lms/investigacion/mod/page/view.php?id=3118>

CONCLUSIONES: El diseño de un Sistema de Gestión de Seguridad de la Información basado en un modelo de mejoras prácticas y lineamientos de seguridad, como es la norma ISO/IEC 27001:2013, es un herramientas de gran ayuda que permite identificar los diferentes aspectos que se deben tener en cuenta cuando las organizaciones deciden establecer un modelo de seguridad de la información, ya que si los organizaciones logran cumplir al pie de la letra lo establecido está en la norma ISO/IEC 27001:2013, podar llegar a forjar en el tiempo un adecuado y sostenible Sistema de Gestión de Seguridad de la Información, aunque dicha labor depende del tamaño y naturaleza de la entidad y de la cultura de la misma en torno a la seguridad de la información.

Esta labor debe comenzar con el compromiso demostrable a la alcaldía municipal de la jagua de Ibirico y mostrar para donde va la seguridad de la información, labor que no es nada fácil cuando no se tiene concebida la seguridad de la información dentro de los objetivos estratégicos de la organización. El apoyo de la alta directiva, es indispensable para poder concebir un modelo de Seguridad de la Información que realmente apoye y apalanque la misión y visión de la organización, el cual es fundamental que se tenga antes de comenzar a diseñar un Sistema de Gestión de Seguridad de la Información, ya que si este no se logra conseguir, es casi seguro que cualquier iniciativa de seguridad que se pretender adelantar, no alcancen los resultados esperados y si por el contrario, genere el rechazo o el poco apoyo o interés por parte de la organización..

RECOMENDACIONES: Las recomendaciones finales que resaltamos de esta investigación después de haber evaluado todo el sistema y de haber encontrado todas estas fallas tanto en el sistema como en la empresa en general son las siguientes:

La entidad requiere implementar una serie de controles con el objetivo de fortalecer su seguridad y poder dar cumplimiento a los requerimientos establecidos en la norma ISO 27001:2013, por eso es fundamental que lleven a cabo los diferentes planes de acciones que se definieron en el presente trabajo de grado.

Es necesario que la Dirección de Tecnología de la entidad revise su capacidad con el objetivo de garantizar la debida implementación de los controles y planes de acciones que se requieren llevar a cabo para cerrar las brechas encontradas producto de los diagnósticos realizados, ya que la mayoría de estos planes de acción requiere un componente tecnológico.

Es necesario que la entidad evalúe la vialidad de algunos planes de acciones propuestos, debido a que su implementación demanda la adquisición de herramientas y/o soluciones tecnológicas que implica adelantar procesos de

contratación para su adquisición. Algunas de las soluciones tecnológicas que se proponen, pueden llegar a tener un costo elevado y/o su implementación puede demandar un tiempo considerable.

Realizar campañas de seguridad de la información, con el propósito de poder generar un sentido de pertenencia y apropiación en temas de seguridad en cada uno de los funcionarios de la entidad, y concientizar sobre los riesgos que pueden afectar la seguridad de la información.

1. **Bibliografía:** GÓMEZ FERNÁNDEZ, Luis y FERNÁNDEZ RIVERO Pedro. Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad (España), 2015.(online) disponible en: <http://www.aenor.es/aenor/normas/ediciones/fichae.asp?codigo=11248>
2. 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
3. BENCHIMOL, Daniel. Hacking desde Cero (Buenos Aires Argentina), 2011. (Online) disponible en: <https://upload.wikimedia.org/wikipedia/commons/b/b9/HakingCero.pdf>

Elaboró

Martha Lucia Briñez Bautista, 28/05/17