SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCÓ

LUIS CARLOS PALACIOS MOSQUERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATIVA
QUIBDÓ
2015

LUIS CARLOS PALACIOS MOSQUERA

TESIS DE GRADO PARA OPTAR POR EL TÍTULO:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR DE CURSO
WILSON CASTAÑO GALVIZ
MAGISTER EN INFORMÁTICA

DIRECTOR DE PROYECTO
MARTIN CAMILO CANCELADO RUIZ
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATIVA
QUIBDÓ
2015

Nota de Aceptación

_____

_____

_____

_____

_____

Firma del Presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

Dedicatoria.

Agradezco primordialmente a Dios por darme la inteligencia, sabiduría, paciencia, entendimiento y la capacidad por realizar este proyecto en vida.

A mis padres, hermanos, esposa e hijos por todo su apoyo, comprensión y sobre todo la paciencia de esperar todo este tiempo.

A mis amigos que entendieron y valoraron el tiempo que le dediqué a este proyecto, al tutor NILSON EMIR PALACIOS MOSQUERA del CEAD Quibdó, por ser un apoyo incondicional desde que ingrese a esta gloriosa institución.

Luis Carlos Palacios M.

Agradecimientos

Agradezco primordialmente a Dios por darme la inteligencia, sabiduría, paciencia, entendimiento y la capacidad por realizar este proyecto en vida.

A mis padres, hermanos, esposa e hijos por todo su apoyo, comprensión y sobre todo la paciencia de esperar todo este tiempo.

A la universidad y al cuerpo de tutores representados en cada una de las actividades propuestas durante la carrera, por brindarme la oportunidad de adquirir nuevos conocimientos y experiencias que contribuyeron a mi crecimiento como persona y como profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

1. INTRODUCCIÓN

Es de conocimiento que lo más importante en cuanto al manejo de la información de la empresa Aguas del Chocó PDA, es estar preparada para todos y cada uno de los eventos adversos que pueden llegar a sucederles, como impactar las actividades del negocio. Las organizaciones dependen de sus recursos, como bienes tangibles, empleados, sistemas y tecnologías de información, etc en caso de daños de alguno de estos componentes, pueden llegar a paralizarse y muchas veces se ven abocadas a comenzar de nuevo, es decir desde cero.

Para la empresa es de suma importancia, tener las políticas y objetivos de la seguridad de la información claro, en lugares públicos donde los empleados puedan tener acceso con facilidad, determinando puntos objetivos y fáciles de ejecutar.

Para la empresa Aguas del Chocó PDA. Es obligado el tema de la “Gestión de la Seguridad de la Información” y ha dejado de ser un tema relevante ocupando una posición muy importante ante la alta gerencia, es importante contar con varios factores que componen un SGSI, como la determinación de los criterios de evaluación, complementado con un análisis del riesgo bien documentado, un plan de tratamiento de riesgos de la actividad de la empresa en caso de que ocurran incidentes graves y la estrategia de la adopción de un plan de continuidad adicional, y unas buenas políticas de seguridad informática que ayude a prevenir o minimizar las pérdidas de información para la empresa, ya que constituye un ejercicio de responsabilidad ante sus clientes.

2. CAPITULO 1: EL PROBLEMA

2.1. Título

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCÓ.

2.1.1 Alternativa de grado:

Proyecto de Investigación

2.1.2 Tema u objeto de estudio:

El presente proyecto está inmerso en el tema de SGSI- Sistema de Gestión de Seguridad de la Información.

2.1.3 Línea de investigación:

Esta propuesta está inmersa en la cadena de formación de sistemas, principalmente en la línea de gestión de sistemas, que abarca las ciencias computacionales.

2.1.4 Formulación del problema:

¿De qué manera la empresa Aguas del Chocó, puede salvaguardar la información, sin que haya traumatismos de seguridad en la red de datos?

2.2. Justificación

El estudio propuesto, permitirá que la empresa Aguas del Chocó, disminuya sus niveles de riesgo, así como garantizará la permanente comunicación entre las 20 sedes de manera segura, permaneciendo en el tiempo y generando confianza con los usuarios.

Con el desarrollo del proyecto la empresa se posicionará, dentro del comercio electrónico, siendo una de las primeras en el Departamento del Chocó, que cuenta con este tipo de sistemas, permitiendo atraer usuarios de talla nacional.

Los empleados tanto internos como externos, estarán en la capacidad de seguir los lineamientos y requerimientos, que demanda el Sistema de Gestión de Seguridad de la Información de la Empresa Aguas del Chocó, logrando así la evolución y adaptación en los sistemas de gestión de la información.

2.3. Hipótesis

Una vez elaborado el SGSI de la empresa Aguas del Chocó, con un adecuado manejo de este recurso minimizará los niveles de riesgo a los que está expuesto, contribuyendo así al buen majo de la información asegurando que cada uno de los empleados apliquen los requerimientos planteados, igualmente este sistema permitirá la continuidad en el tiempo para prestar un buen servicio a los usuarios de manera que se respete y se cumpla con los criterios de seguridad.

2.4. Planteamiento del problema

Aguas del Chocó S.A ESP, es una empresa de sociedad por acciones de estamento público, creada para la ejecución del plan departamental de aguas, adscrita a la Gobernación del Chocó, así como un conjunto de estrategias de planeación y coordinación interinstitucional, formuladas y ejecutadas con el objeto de lograr la armonización integral de los recursos, y la implementación de esquemas eficientes y sostenibles en la prestación de los servicios públicos domiciliarios de agua potable y saneamiento en el departamento del Chocó.

El plan departamental de Aguas cuenta con una sede central situada en la capital del Departamento del Chocó - Quibdó, en la dirección Carrera 5ta No. 29 - 75 Barrio Cesar Conto, en un edificio de 5 pisos.

La empresa actualmente cuenta con un proyecto de regionalización denominado, plan de aseguramiento de la prestación de los servicios públicos domiciliarios de acueducto alcantarillado y aseo. Donde una vez se lleve a feliz término, se instalaran nuevas sedes en los 20 Municipios que están adscritos dentro del plan, con el fin de prestar los servicios de acueducto, alcantarillado y aseo, igualmente atenderán las peticiones, quejas, reclamos y sugerencias vía remota, desde los puntos de atención de servicio al cliente, así como la generación de facturas, lo cual demanda la necesidad estricta, de proteger la información de los usuarios.

Con la petición de diferentes consultas desde otros equipos hacia el servidor de aplicaciones de la empresa Aguas del Choco, se expone a riesgo de diferentes tipos de ataques, trayendo con ello graves problemas de seguridad a la red de datos, tanto interno como externo, llegando a un punto crítico de borrar, robar o alterar la información de la base de datos.

Este tipo de riesgo se debe a la necesidad de implementar políticas y normas de seguridad de la empresa Aguas del Choco.

Iniciar con la atención al usuario sin tomar medidas para mitigar estos tipos de riesgos, puede llegar a afectar seriamente la parte financiera de la empresa, generando consecuencias de liquidación de la empresa a corto tiempo.

2.5. Objetivos

2.5.1 General

Implementar un sistema de gestión de seguridad de la información en la empresa Aguas del Chocó que permita, disminuir los niveles de riesgos informáticos, aplicando la norma ISO 27001 y la metodología OCTAVE-S.

2.5.2 Específico:

- Definir procedimientos y mecanismos de protección que permitan la disminución de los riesgos informáticos en la empresa.
- Estandarizar el proceso del sistema de gestión de seguridad de la información de la empresa Aguas del Chocó mediante la comparación de las diferentes normas y metodologías nacionales e internacionales.
- Determinar el nivel de mejora en la seguridad informática en la empresa Aguas del Chocó mediante la socialización del SGSI.

.

3. CAPITULO 2 MARCO REFERENCIAL

3.1. Marco conceptual

- **PDA:** Plan departamental de aguas.

- **SGSI**: Sistema de gestión de seguridad de la información.

- **Método OCTAVE**: Este método se aplica a organizaciones de 300 ó más empleados, pero también se tiene que tener en cuenta la jerarquía de la organización. (riesgoscontrolinformatico.blogspot.es, 2014)[1]

- **Método OCTAVE-S:** Esto método surge gracias a la necesidad de organizaciones más pequeñas alrededor de 100 personas o menos. (riesgoscontrolinformatico.blogspot.es, 2014)

- **Método OCTAVE ALLEGRO:** Este variación del método es el formato más simplificado de método de Octave que se centra en los activos de la información. (riesgoscontrolinformatico.blogspot.es, 2014)

- **MAGERIT**: Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. (administracionelectronica.gob.es, 2012)

- **Hacker:** Es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas (Speedy, 2014).

- **Definición de zombie (informática):** En hacking, zombie es el nombre que recibe una computadora que se encuentra infectada con un programa deamon, que permite ser controlada por un pirata informático de forma remota, sin el consentimiento del dueño de la misma. El deamon abre puertos específicos en el sistema, los cuales permiten al hacker enviar comandos y así utilizar la computadora para su beneficio (adriinfo22, 01).

- **Spam:** Son los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico pero puede presentarse por programas de mensajería instantánea o por teléfono celular.

[1] RIESGOS INFORMÁTICO, Método elegido OCTAVE [Citado 20-Marzo-2014] Disponible en http://riesgoscontrolinformatico.blogspot.es/tags/metodo-elegido-octave/

- **Crack Informático:** Es un parche, creado sin conocer el código fuente del programa, cuya finalidad es la de modificar el comportamiento del software origina (segu-info, 2000).

- **Firewall:** Es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial (desarrolloweb, 2001).

- **Identificación:** Se refiere a las cosas como nombres de usuario y tarjetas de identificación. Es el medio por el cual un usuario del sistema identifica quiénes son. Este paso se realiza generalmente al iniciar sesión (Subinet, 2013).

- **Autorización** se produce después de que un usuario del sistema se autentica y luego es autorizado a utilizar el sistema.

- **El Atacante:** es la persona que crea los paquetes ICMP con la IP fuente falsa y lanza el ataque (Tarazona, 2013).

- **Intermediario:** la red amplificadora del paquete ICMP con su direccionamiento broadcast habilitado.

- **La Víctima:** su dirección IP ha sido suplantada para que las respuestas ICMP sean enviadas a ella. Se debe anotar que el intermediario también puede convertirse en víctima.

- **Disponibilidad:** De acuerdo con Chapela, durante la aplicación de las pruebas es necesario minimizar el peligro de interrupciones no programadas en servicios o procesos. Para esto, es necesario calendarizar las irrupciones de alto riesgo, desarrollar un plan de respaldo y conformar un equipo de respuesta capaz de actuar con rapidez. Además, debe determinarse con toda claridad qué probar y qué no. Tal es el caso de hardware y aplicaciones obsoletas, aplicaciones críticas, equipo sin respaldo –o carente de un plan de contingencia– y sistemas fáciles de colapsar cuando se examinan (ECURED).

- **Confidencialidad.** Para evitar que se pierda o fugue contenido valioso durante el desarrollo de las pruebas, debe establecerse claramente qué pueden copiar o leer quienes las ejecuten. Asimismo, conviene hacer un cambio completo de códigos de acceso al final de los ejercicios de penetración y establecer algunas prohibiciones, como: no copiar ni leer correo electrónico o información de bases de datos o archivos. Sobre este

punto, Rafael García, gerente regional de productos de Symantec para América Latina, detalla: "Los Pen Tests deben involucrar todas aquellas áreas que están más relacionadas con el core del negocio, por lo que la metodología a emplear y sus límites dependen siempre del giro de la empresa, el grado de profundidad de las pruebas y el análisis requerido. En este marco, debe privilegiarse la firma de acuerdos de secrecía en los contratos y dar prioridad a la honestidad de los consultores". (ECURED)[2]

- **Integridad y Responsabilidad:** Durante el desarrollo de las pruebas, las empresas deben reducir al mínimo la probabilidad de alteraciones en aplicaciones o datos. Por lo tanto, entre las prohibiciones a fijar a quienes las ejecutarán están: no instalar jamás puertas traseras (back doors), ni ocultar soluciones de acceso remoto (bots, troyanos, rootkits y demás); no borrar, alterar o inhabilitar registros y, desde luego, no apagar o modificar el comportamiento de las herramientas de detección establecidas. Un punto muy importante en todo esto es registrar quién hace qué, para evitar abuso de terceras partes en los Pen Tests, así como dejar claro que no deben eliminarse u ocultarse los rastros de las pruebas. Este proceso implica también autenticar a los consultores, con el propósito de identificarlos claramente en los sistemas evaluados. (ECURED)

- **Riesgo Político.** ¿Qué pasa si una falla no prevista en ciertos servicios críticos ocurre como resultado de las propias pruebas? Deben minimizarse las probabilidades de que se generen choques internos entre las diferentes áreas involucradas o confrontaciones con proveedores, y evitar factores que reduzcan el valor percibido o el profesionalismo de las pen test. “Dada la lucha de poder entre áreas que existe, en algunas empresas, — asegura García—si el departamento de sistemas es el encargado de contratar las pruebas debe sentirse respaldado previamente por la alta dirección, para que los resultados, sobre todo si no son del todo positivos, no se utilicen como arma de pugnas”. (ECURED)

- **Incumplimiento.** Diversas pruebas de penetración buscan dar cauce a requerimientos legales y regulaciones para evitar multas o sanciones a la hora de efectuarlas. Asimismo, los resultados de la revisión van de acuerdo con los lineamientos y estándares corporativos aplicables en cada caso (ISO 27001 / BS 7799, CoBIT, ITIL y demás). Danny Allan, analista de investigación de la empresa Watchfire, hace énfasis en la carga creciente que toma el cumplimiento de todo tipo de regulaciones. No sólo para

[2] ECURED, Prueba de penetración [Citado 08-Octubre-2012] Disponible en http://www.ecured.cu/index.php/Prueba_de_penetraci%C3%B3n#Fuente

cuestiones técnicas, sino también en temas que tienen que ver con rubros como: competencia, protección de datos, privacidad, terrorismo, operaciones de outsourcing, reputación y propiedad intelectual, entre otros. (ECURED)

- **Inguma:** es una herramienta para realizar de prueba de penetración escrita enteramente en python. El framework incluye los módulos para descubrir los hosts, información sobre ellos, sacar nombres de usuario y las contraseñas por fuerza bruta y por supuesto exploits para muchos productos.

- **DSniff:** Un juego de poderosas herramientas de auditoría y pruebas de penetración de redes. Este popular y bien diseñado set hecho por Dug Song incluye varias herramientas. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante -- por ej. debido al uso de switches {"layer-2 switches"}. sshmitm y webmitm implementan ataques del tipo monkey-in-the-middle activos hacia sesiones redirigidas de SSH y HTTPS abusando de relacione. (Stallman, 2003)

- **Protección:** Articulado por el Sistema Operativo. la protección se refiere a un mecanismo para controlar el acceso de los programas, procesos o usuarios a los recursos definidos por un sistema.” [Silbertschatz]. Es de orientación interna y establece mecanismos que representan el (como). (Arthur, 2012)

- **Cifrado:** Técnica que transforma un mensaje en otro ilegible. Aplicando técnicas que enmascaran los datos en un lenguaje no común para el sistema mediante la agregación de Bits de encriptación. En algunos casos se utilizan Claves, que son un patrón de cifrado y descifrado.

- **Vigilancia de Amenazas:** El sistema busca patrones de actividad sospechosa.

3.2. Marco teórico

3.2.1 Resumen Norma ISO/IEC 27000

Conjunto de Estándares y en fases de desarrollo por la organización (International Organization for Standardization) e IEC (International Elctroctechnical

Commission) que proporcionan un marco de gestión de la información utilizada por en cualquier organización sea pública o privada, grande o pequeña (ISO, 2007).

Su objetivo conduce a lograr la protección de la información, con dos propósitos certificación o las buenas prácticas de seguridad de la organización, en sus procesos internos y externos, Está sustentado en normas nacionales e internacionales, fuentes de derecho como complemento y apoyo a las legislaciones vigentes en cada país.

Para efectos del presente documento, se enfocará en tres de las nomas del conjunto
ISO 27000, así:

ISO 27001, publicada el 15 de octubre de 2005, pero con nuevas reformas en año 2013, contiene los requisitos del sistema de gestión de seguridad, abarca todo tipo de organización, y contiene los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información, dando opción a que se ajusten a las necesidades propias de cada organización, los controles proporcionan un marco de seguridad y los controles necesarios para proteger la información. Esta es la norma que se utiliza para certificación (ISO, 2007) Pag. 3.

Según la reorganización de las publicaciones ISO en la nueva estructura de Anexo SL que, junto a los cambios en los contenidos, ha desencadenado la actualización de las normas de la serie 27000. A continuación se muestra un diagrama de relación de la reorganización de las cláusulas principales de la versión 2005 a la publicada en 2013.

3.3. Marco Contextual

3.3.1 Nombre de la empresa

Aguas del Chocó S.A: es una empresa creada para la ejecución del plan departamental de aguas, adscrita a la Gobernación del Chocó. La empresa está dedicada a la gestión y construcción de proyectos del área en saneamientos básico, el cual abarca los pilares de acueducto, alcantarillado y aseo.

La empresa Aguas del Chocó como prestadores de servicios públicos, utiliza un software llamado INTEGRIN, para la generación de facturas, inscripción de suscritores o usuarios, peticiones, quejas, reclamos y todo lo concerniente al tema de atención al usuario desde todas las sedes que la integran.

3.3.2 Ubicación de la Empresa

El plan departamental de Aguas cuenta con una sede central situada en la capital del Departamento del Chocó, en la dirección Carrera 5ta No. 29 - 75 Barrio Cesar Conto, en un edificio de 5 pisos, el cual detallo a continuación.[1]

3.3.3 Misión

Promover e implementar políticas y estrategias innovadoras en lo institucional, comercial, financiero y técnico, para la eficiente prestación de los servicios públicos de agua potable y saneamiento básico en el departamento del Chocó (Aguas del Chocó, 2013).

La empresa velará por el cumplimiento de los principios establecidos en los planes departamentales de aguas, de tal manera que se alcance el proceso de transformación empresarial y/o fortalecimiento institucional en las empresas que prestan estos servicios públicos en los municipios que estén vinculados al plan.

3.3.4 Visión

Consolidarnos como una empresa eficiente y efectiva en la generación e implementación de las políticas de agua potable y saneamiento básico, que garanticen la prestación de servicios de alta calidad para satisfacer las necesidades de los clientes (Aguas del Chocó, 2013).

4. CAPITULO 3: MARCO METODOLÓGICO

4.1. Tipo de investigación

El tipo de investigación de este proyecto es *Cuantitativo* enmarcado dentro de la investigación:

Investigación evaluativa: Es el proceso que consiste en dar un juicio sobre una intervención, empleando métodos científicos. Mediante ella se evalúan los recursos, los servicios y objetivos de la intervención dirigidos a la solución de una situación problemática y las interrelaciones entre estos elementos, con el propósito de ayudar a la toma de decisiones.

La investigación se focaliza, a partir de la evaluación de los riesgos encontrados en la empresa Aguas del Chocó, se toma como punto de partida el diagnóstico realizado para poder determinar y manejar un buen plan de tratamiento del riesgo, determinando las características de evaluación para medir el impacto que causan los riesgos, seguidamente para mitigar ese impacto y minimizar el riesgo se debe generar unas buenas políticas de seguridad informática.

5. CAPITULO 4: ANÁLISIS DE RIESGO INFORMÁTICO AGUAS DEL CHOCÓ

5.1. Introducción

Aguas del Chocó no está exenta a las diferentes amenazas significativas que existen en su entorno, ante la posibilidad de ocurrencia de un incidente o desastre que afecte total o parcialmente su operación, debido a esto la empresa debe tener clara la necesidad de recuperar su operación en el menor tiempo posible, garantizando la continuidad de la prestación del servicio.

Una de las posibles consecuencias de una intrusión es la pérdida de datos el cual es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día con las copias de seguridad y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.

Otro de los problemas más graves es el robo de información sensible y confidencial, La divulgación de la información que posee la empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo más cercano a nosotros es el de las contraseñas de las cuentas de correo, por ello la seguridad informática es el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

Es aquí donde surge el concepto de análisis de riesgos informáticos que es un método sistemático de recopilar, evaluar, registrar, difundir y gestionar la información para formular recomendaciones orientadas a la adopción de medidas en respuesta a las vulnerabilidades o amenazas que se encuentran durante el análisis.

Los métodos y estándares de análisis de riesgos en general consideran cuatro etapas: la identificación de vulnerabilidades y amenazas, la evaluación del riesgo, la gestión del riesgo y la comunicación del riesgo. En la identificación del riesgo se especifican los acontecimientos adversos que son motivos de preocupación; En la evaluación del riesgo se tiene en cuenta la probabilidad real de que se materialice una amenaza aprovechando una vulnerabilidad; En la gestión del riesgo se identifican y aplican las mejores opciones que permitan reducir o eliminar la posibilidad de que se materialice las amenazas; y por último la comunicación del riesgo que consiste en el intercambio de información y opiniones que lleven a una mejor comprensión y adopción de decisiones. En la actualidad existen muchos estándares y metodologías de análisis de riesgos, pera la empresa Aguas del Chocó elegí la metodología OCTAVE sin desconocer que hay otras metodologías.

5.2. Objetivos

- Realizar el análisis de riesgos de la empresa Aguas del Chocó, con la metodología OCTAVE-S.

- Detectar los posibles riegos en el sistema informático de la empresa Aguas del Chocó.
- Dar recomendaciones que permitan mitigar las amenazas que se detecten con el análisis de riesgos realizado.

5.3. Metodología de Análisis de Riesgos Seleccionada.

La metodología de análisis de riesgos que seleccioné es OCTAVE-S porque es una metodología que fue desarrollado en respuesta a las necesidades de organizaciones más pequeñas alrededor de 100 personas o menos. Cumple con los mismos criterios que el método OCTAVE pero está adaptado a los limitados medios y restricciones únicas de las pequeñas organizaciones. Además OCTAVE-S utiliza un proceso simplificado pero produce el mismo tipo de resultados que OCTAVE y requiere un pequeño equipo de 3-5 personas que entienden la amplitud y profundidad de la empresa.

5.4. Fase Uno

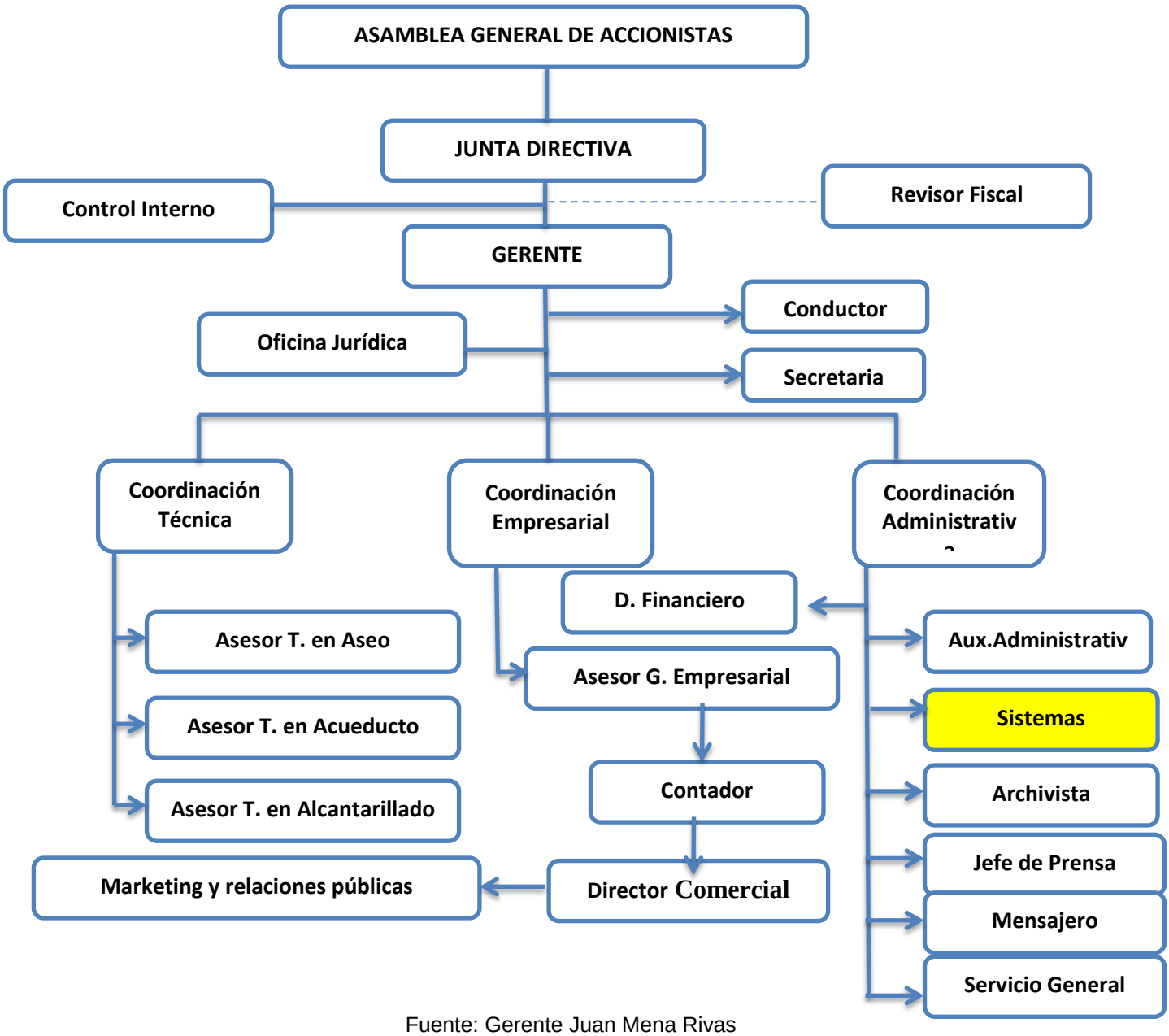
5.4.1 Identificación de La Empresa Aguas Del Chocó S.A.S

La organización es una empresa de capital público de tamaño medio, tiene 70 empleado de los cuales 20 son de planta y 50 son por prestación de servicios, su mayor accionista es la Gobernación del Chocó en cabeza del gobernador ya que cumple todas las funciones del plan departamental de aguas del chocó, la empresa ésta dedicada a la construcción de acueductos, alcantarillados y rellenos sanitarios, igualmente realiza el mantenimiento de los mismos en todo el Chocó.
Cabe recordar que por su tamaño la metodología OCTAVE-S se adapta con facilidad para aplicar el análisis de riesgo.

5.4.2 Organigrama Aguas del Chocó.

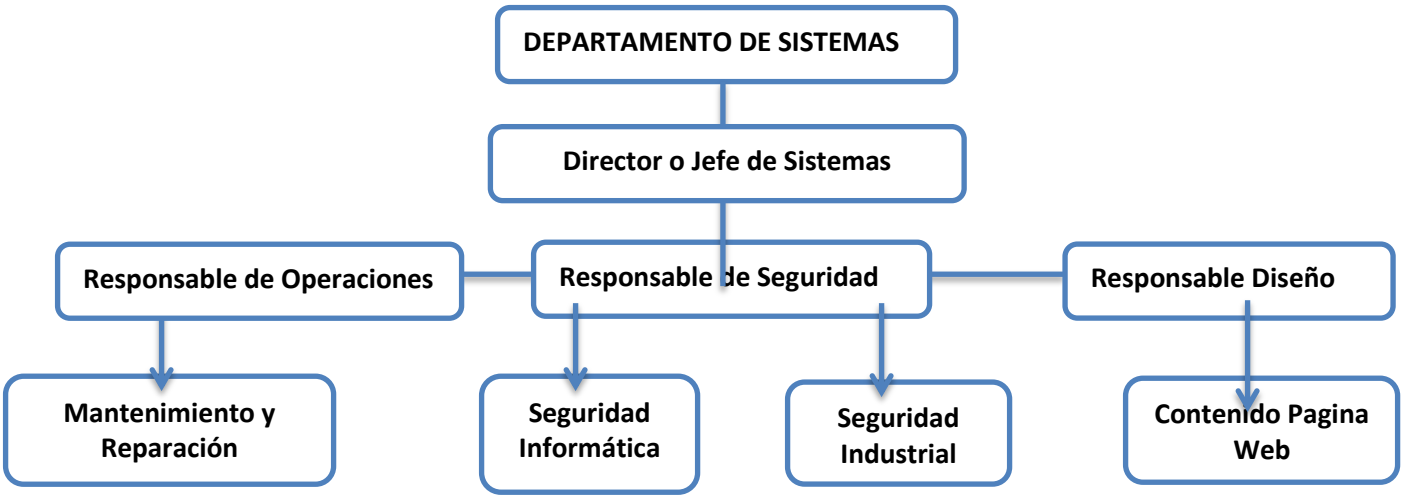
A fecha de la última actualización, la empresa se encuentra organizada del modo descrito en el siguiente diagrama.

Figura 1. Organigrama Aguas del Chocó



Fuente: Gerente Juan Mena Rivas

Figura 1. Organigrama Departamento de Sistemas



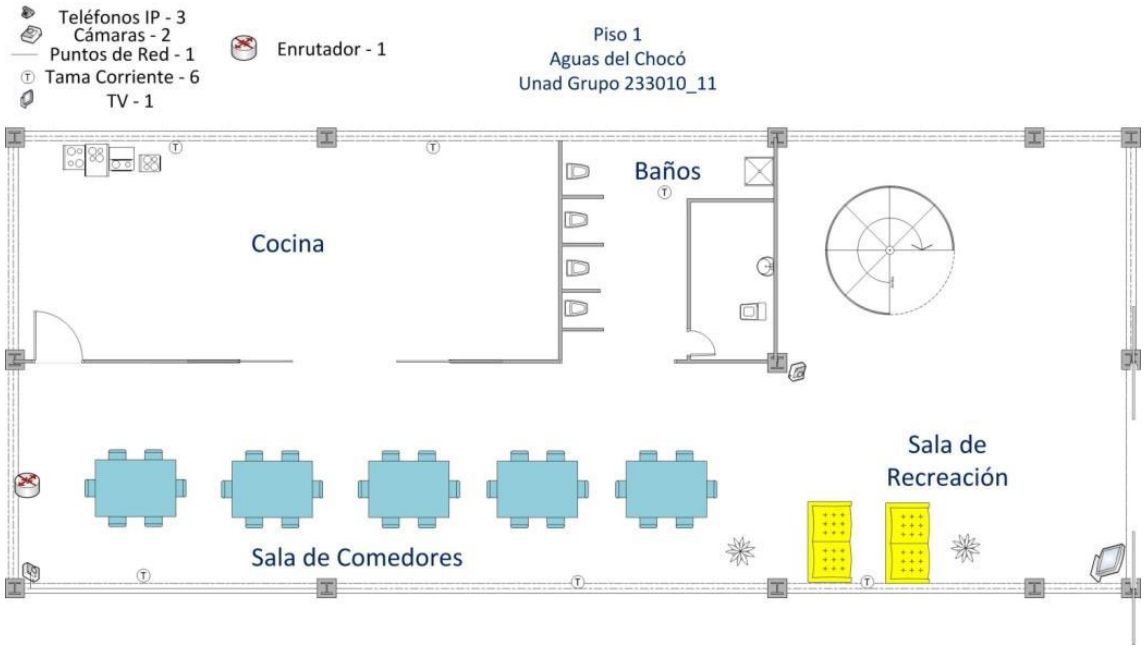
Fuente: Gerente Juan Mena Rivas

5.4.3 Descripción de la Infraestructura del edificio Aguas del Chocó.

5.4.3.1 Distribución de la Planta Primer Piso de la Empresa Aguas Del Chocó

En el primer piso funciona una cafetería y salón recreacional, éste nivel del edificio cuenta con los siguientes dispositivos y diseño.

Figura 2. Diagrama primer piso



Fuente: Levantamiento estructura física

La estructura de la red está formada por los siguientes puntos estratégicos que serían;

Tabla 1: Inventario primer piso

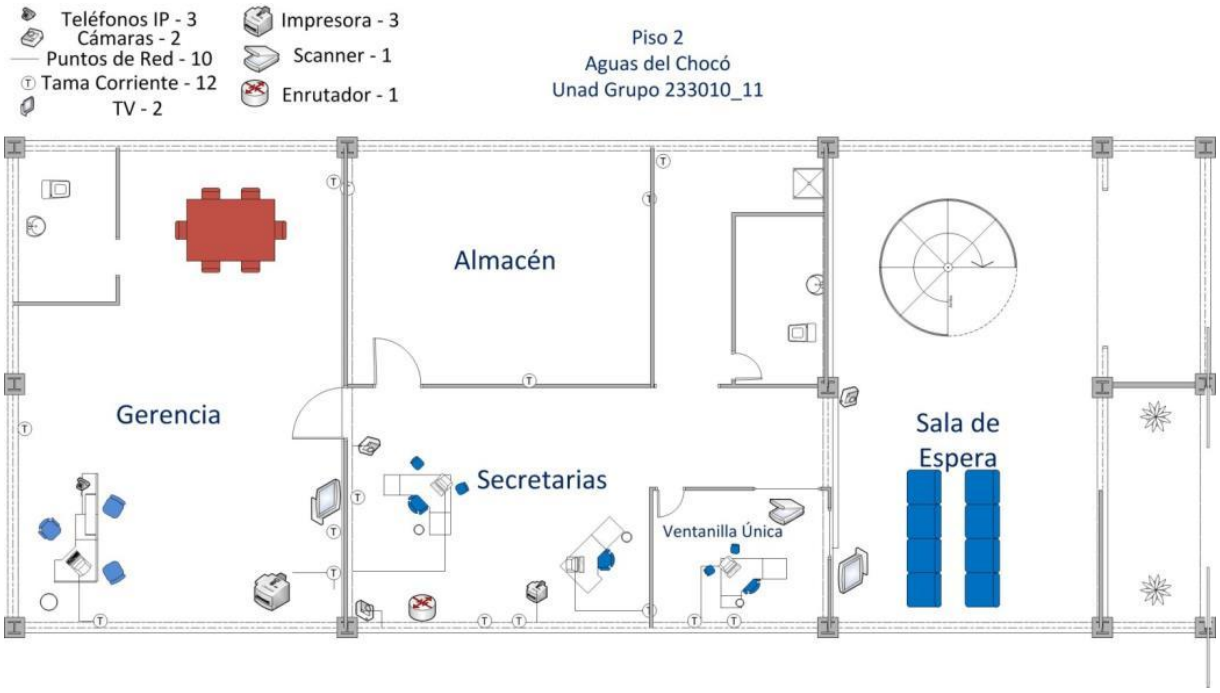
Televisión por Directv	1
Toma corriente doble regulado	6
Teléfono IP	1
Router	1

Fuente: Levantamiento de campo en el edificio.

5.4.3.2 Distribución de la Planta Segundo Piso de la Empresa Aguas del Chocó

En el segundo piso están las oficinas de Gerencia, Secretaria Privada, Almacén, Ventanilla Única y la Sala de Espera, éste nivel del edificio cuenta con los siguientes dispositivos y diseño.

Figura 3. Diagrama Segundo Piso



Fuente: Levantamiento estructura física

La estructura de la red está formada por los siguientes puntos estratégicos que serían;

Tabla 2: Inventario segundo piso

Gerencia		**Secretaria Privada**	
Puntos de red de datos	2	Puntos de red de datos	3
Televisión por Directv	1	Toma corriente doble regulado	3
Toma corriente doble regulado	2	Teléfono IP	1
Teléfono IP	1	Router inalámbrico	1
		Impresora de Red	1

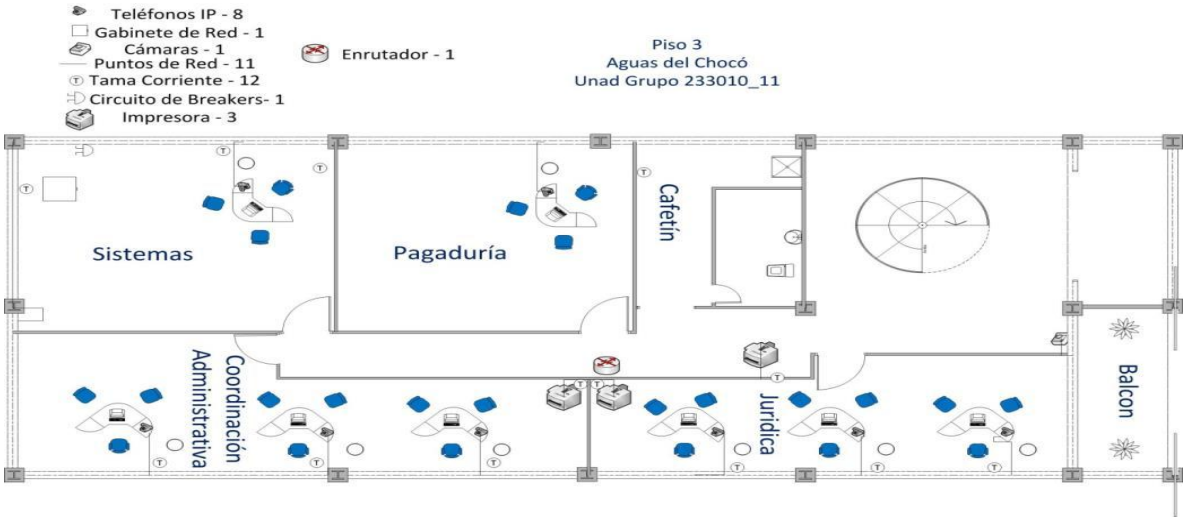
		Cámara de video	1
Almacén		**Ventanilla Única**	
Puntos de red de datos	3	Puntos de red de datos	1
Toma corriente doble regulado	3	Toma corriente doble regulado	2
Teléfono IP	2	Teléfono IP	1
		Scanner	1
Sala de Espera			
Televisión por Directv	1		
Cámara de video	1		

Fuente: Levantamiento de campo en el edificio.

5.4.3.3 Distribución de la Planta Tercer Piso Empresa Aguas del Chocó.

En el tercer piso están las oficinas de Jurídica, Pagaduría, Coordinación Administrativa y Sistemas, éste nivel del edificio cuenta con los siguientes dispositivos y diseño.

Figura 4: Diagrama tercer piso



Fuente: Levantamiento estructura física.

La estructura de la red está formada por los siguientes puntos estratégicos que serían.
Tabla 3: Inventario tercer piso

Jurídica		**Pagaduría**	
Puntos de red de datos	5	Puntos de red de datos	1
Toma corriente doble regulado	6	Toma corriente doble regulado	2
Teléfono IP	1	Teléfono IP	1
Coordinación administrativa		**Sistemas**	
Puntos de red de datos	5	Puntos de red de datos	1
Toma corriente doble regulado	4	Toma corriente doble regulado	2
Teléfono IP	2	Circuito caja breaker	2
		Teléfono IP	1
		Gabinete de red	1
Pasillo			
Router inalámbrico	1		
Impresora de Red	1		
Cámara de video	1		

Fuente: Levantamiento de campo en el edificio.

5.4.3.4 Distribución de la Planta Cuarto Piso de la Empresa Aguas Del Chocó.

En el cuarto piso están las oficinas de Gestión Empresarial, Área técnica y la Sala de Juntas, éste nivel del edificio cuenta con los siguientes dispositivos y diseño.

Figura 5: Diagrama cuarto piso

Fuente: Levantamiento estructura física

La estructura de la red está formada por los siguientes puntos estratégicos que serían.

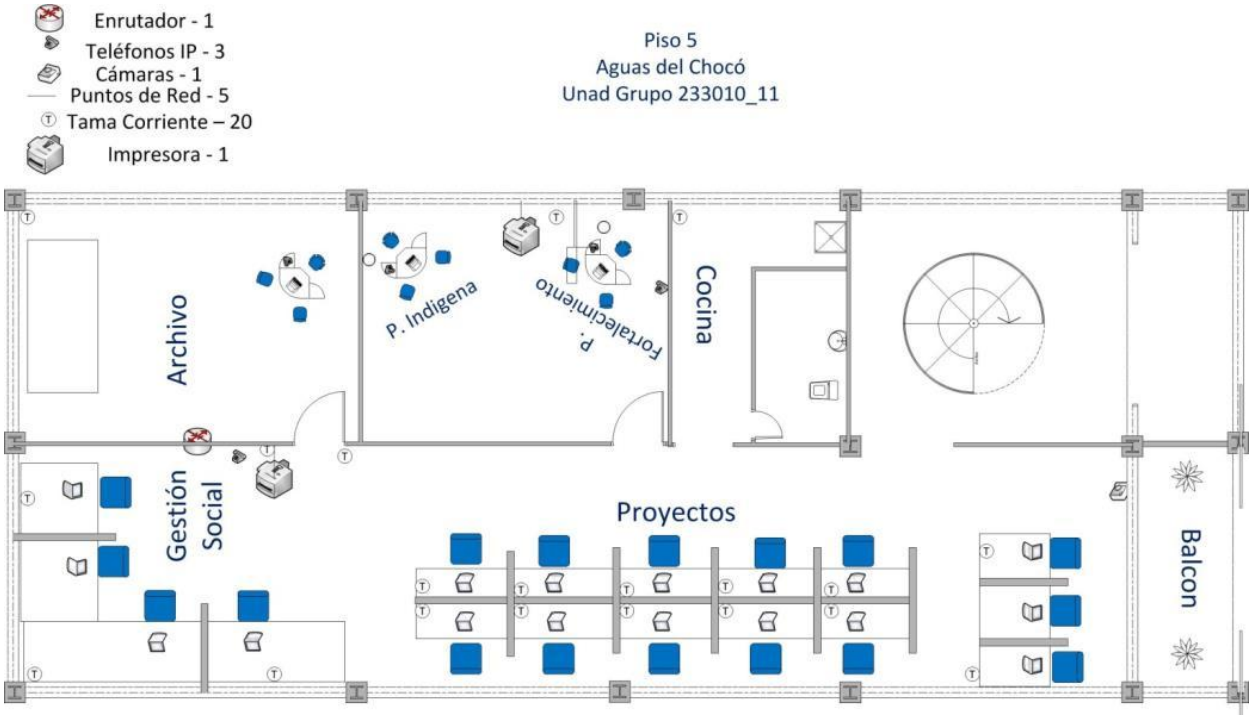
Tabla 4: Inventario tercer piso

Gestión Empresarial		**Área Técnica**	
Puntos de red de datos	4	Puntos de red de datos	10
Toma corriente doble regulado	3	Toma corriente doble regulado	8
Teléfono IP	1	Teléfono IP	1
		Impresora IP	
Sala de Juntas			
Puntos de red de datos	2		
Toma corriente doble regulado	4		
Video Bean	1		
Router	1		

Fuente: Levantamiento de campo en el edificio.

En el quinto piso están las oficinas de Archivo, Gestión Social, Coordinación Proyectos y área de proyectos, éste nivel del edificio cuenta con los siguientes dispositivos y diseño.

Figura 6. Diagrama Quinto piso



Fuente: Levantamiento estructura física

La estructura de la red está formada por los siguientes puntos estratégicos que serían.

Tabla 5: Inventario cuarto piso

Archivo		**Gestión Social**	
Puntos de red de datos	1	Puntos de red de datos	1
Toma corriente doble regulado	2	Toma corriente doble regulado	2
Teléfono IP	1	Teléfono IP	1
Coordinación de Proyectos		**Área de Proyectos**	

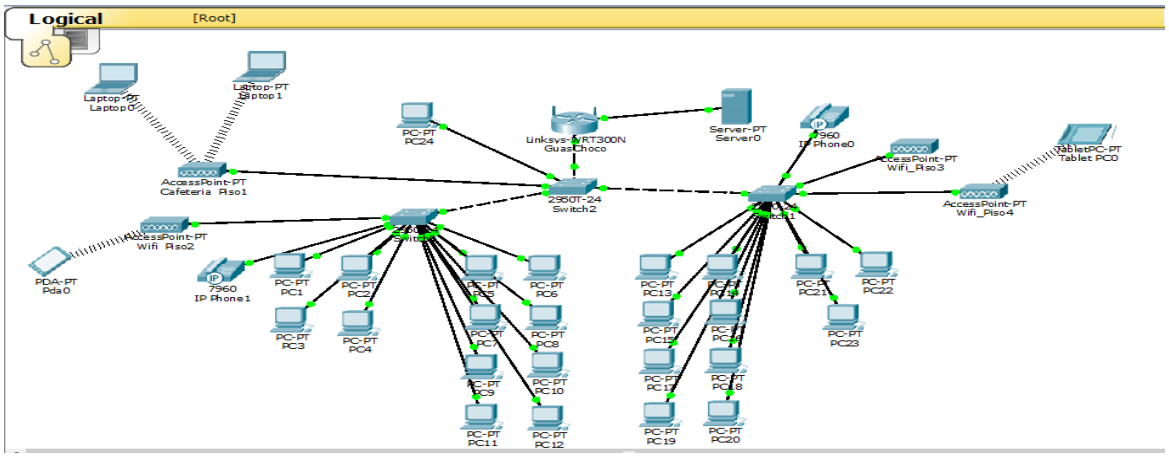
Puntos de red de datos	2	Puntos de red de datos	1
Toma corriente doble regulado	3	Toma corriente doble regulado	30
Teléfono IP	1	Impresora IP	2
		Teléfono IP	1
		Router	1

Fuente: Levantamiento de campo en el edificio.

5.4.3.5 Descripción Detallada Departamento de Tecnología de la Información:

Siendo más enfático, centralizamos en la oficina de sistemas ubicada en el tercer piso del edificio de Aguas del Chocó, teniendo en cuenta que esta oficina presta servicios de redes avanzadas, se centralizan los equipos que se encargan de manejar los procesos administrativos al interior de la organización, cuenta con un servidor de archivos principal, donde confluye mucha información de clientes y municipios, un servidor proxy que básicamente está administrando algunas conexiones y fue instalado con el objetivo de controlar el acceso a diferentes sitios web, por parte de los empleados, un servidor de bases de datos que administra información de usuarios, un servidor de telefonía IP, una impresora de red y equipos cliente que manejan los empleados del área.

Figura 7. El Edificio Cuenta Con el Siguiente Diagrama de Red



Fuente: Levantamiento estructura física

Todos los equipos esta ubicados en un gabinete, para su mayor manejo y comodidad, donde confluyen todos los equipos nombrados anteriormente,

mientras el que maneja la conexión desde el proxy tiene como único objetivo conectar las otras oficinas a la principal pero pasando por el servidor proxy.

Tabla 6: Resumen Recursos Informáticos

Red/Zona Desmilitarizada (DMZ)	
Cantidad	**Descripción del Activo**
1	SERVIDOR PROXY
1	SERVIDOR DE ARCHIVO
1	SERVIDOR DNS INTERNO + HOST IDS
1	SERVIDOR DE CORREO ELECTRONICO + HOST IDS
1	FIREWALL ZONA WI-FI
1	AP
RED INTERNA DE SERVICIOS	
1	SERVIDOR DE BASES DE DATOS
1	SERVIDOR DE APLICACIONES
1	SERVIDOR DE FICHEROS E IMPRESIÓN
1	NETWORK IDS
RED DE USUARIOS	
60	WORKSTATIONS

Fuente: Levantamiento de campo área de sistemas.

5.4.4 Determinación de los Criterios de Evaluación.

5.4.4.1 Criterios de Evaluación de Impacto.

Dentro del comité para desarrollar el análisis de riesgo de la empresa Aguas del Chocó se definieron los siguientes rangos de potencial impacto, (**alto, medio o bajo)**, a la seguridad de los datos en las áreas de confianza de usuarios, financiera, seguridad de las personas, productividad y multas o penalizaciones legales.

5.4.4.2 Confianza de Usuarios

Por el número de empleados y servicios que presta, se puede deducir que lleva buen tiempo en el mercado, con una aproximación en tiempo utilizando el antecedente del proyecto interno para la implantación de un Sistema de Gestión

de la Seguridad de la Información, que la empresa Aguas del Chocó, lleva más de un año en el mercado.

Por su tiempo se nota el reconocimiento por parte de las entidades financieras y de saneamiento básico, en materia de facturación y atención al usuario, y aún más se aumenta la confianza con el nuevo proyecto mencionado anteriormente, lo que le brinda plenas garantías para sostenerse en el tiempo sobre el mercado financiero y de saneamiento básico en materia de facturación y atención al usuario.

Por lo anterior y teniendo en cuenta que los servicios son prestados mediante plataformas web, por la responsabilidad que demanda ante los usuarios para realizar transacciones seguras se le puede considerar a esta área de posible y potencial alto impacto frente a la empresa Aguas del Chocó.

5.4.4.3 Financiera.

La empresa Aguas del Chocó, en su organigrama cuenta con las áreas de Director Comercial responsable de las Ventas, Marketing y relaciones públicas, y el Director Financiero, responsables de la Contabilidad y Compras, pesar de que no se describe la cuantía o no refleja un estado financiero no es relevante para el usuario en materia de garantías para la prestación de los servicios a satisfacción, por cuanto que su amplia trayectoria en el mercado genera plena confianza en los usuarios, por lo tanto se le considera a esta área de bajo potencial de impacto.

5.4.4.4 Seguridad de las Personas

El desarrollo del nuevo proyecto interno para la implantación de un Sistema de Gestión de la Seguridad de la Información, garantiza la preocupación del usuario frente al manejo de la confidencialidad e integridad de su información, el propio sistema se encarga de implementar todas las precauciones y consideraciones dentro de la empresa Aguas del Chocó, por lo anterior este no atenta directamente frente a la seguridad de las personas, por ello se considera de bajo impacto.

5.4.4.5 Productividad

Frente a la funcionalidad que demandan el servidor de aplicación de la empresa Aguas del Chocó, y por los servicios que presta se hace necesario la atención de un porcentaje de la planta de personal que garantice el buen funcionamiento, para que esté libre de toda clase de ficheros maliciosos y cualquier otro riesgo que atente contra la confidencialidad e integridad de los usuarios, de tal manera que brinde atención y vigilancia las 24 horas del día, de modo que internamente esté alejados de cualquier ataque se incurra en fallas de software o hardware, es allí donde se debe aplicar el plan de contingencia de la empresa utilizando los servidores de respaldo hasta que se solucione ese tipo de problemas, que puede ir desde la instalación de un sistema operativo hasta el cambio de una simple

tarjeta Lan, es por ello que el potencial impacto de una amenaza en esta área se considera de alto valor.

5.4.4.6 Multas o Penalizaciones Legales

De acuerdo a los datos suministrados por la empresa Aguas del Chocó, en materia de legalidad de software en su infraestructura, cuentan con licencia en regla y equipos configurados para descargar las actualizaciones desde la plataforma Windows Update de la organización de manera diaria, aunque no dejan muy claro las licencias de los servidores el tipo de sistemas operativos que manejan es de Windows, así como la carencia de descripción de cada una de sus características, se supone que por el diagrama de alto nivel con la arquitectura de los sistemas propio, y por el tipo de usuarios en materia de saneamiento básico que manejan no hay problemas de licenciamiento, por cuanto que estos son requisitos de contratación con entidades financieras y más con plataforma de interacción con millones de usuarios en la nube, al igual que no se evidencia ningún historial de demandas por los actores que interactúan en el sistemas, esta área se considera relativamente baja.

5.4.4.7 Criterios de Evaluación Activos de Información.

Respecto a los sistemas de información más relevantes:

- **El Sistema de Gestión de Proyectos** es básico puesto que es empleado para controlar todas las fases de los proyectos así como para el archivo de los productos resultantes (código fuente, documentación del proyecto como: diseños, planes de pruebas, material de documentación del producto, etc). Este sistema es crítico puesto que es donde reside el código fuente considerado el activo principal. Asimismo, no es únicamente un repositorio de ficheros sino que es un sistema para el control de los proyectos que incluye además del repositorio controlado de versiones de código fuente y el resto de documentación asociada, el sistema para planificar el proyecto y posteriormente realizar el control del progreso del mismo. La aplicación empleada también está basada en tecnología web y estructura de tres capas. Los servidores identificados en el diagrama actúan de servidor web y ejecutan la lógica del sistema mientras que toda la información es almacenada en el servidor de bases de datos corporativo.

- **Entorno para desarrollo simulado** para la prueba de las aplicaciones se dispone de un entorno para desarrollo simulado en los puestos de trabajo del desarrollador, y para las pruebas de integración se dispone de un entorno similar al de los clientes:

- **Servidores web** que ejecutan la capa de presentación e interactúan el resto de elementos del back-end.

- **Servidor de bases de datos** para el almacenamiento de datos de los diferentes estados de la aplicación y sus usuarios. Estos mismos servidores de bases de datos implementan otras bases de datos corporativas como son por ejemplo las del Sistema de aplicación INTEGRIN.

- **Servidor de aplicación** sirven de middleware entre la capa de presentación y el host. Estos elementos además sirven para simular todo el back-end que interacciona con la aplicación desarrollada, de modo que la organización no dispone de un host real.

5.4.4.8 Aspectos físicos de las TIC de la Organización

- **Plataformas Hardware que emplea virtualización y físicamente se ubica en el CPD** todos los sistemas corporativos mencionados anteriormente, así como el resto de infraestructura TIC de la empresa (otros servidores de ficheros para tareas de soporte administrativo, contable, dirección, recursos humanos, etc, servidor de correo) se encuentran implementados en plataformas Hardware que emplea virtualización y físicamente se ubica en el CPD de la organización o El CPD de la organización dispone de controles de acceso por tarjeta de proximidad y código PIN, equipos para el control de la temperatura y humedad, sistemas de extinción de incendios, dispositivos de suministro eléctrico ininterrumpido con capacidad para 15 minutos que a su vez se encuentra conectado a una línea de fuerza de emergencia facilitada por el proveedor del edificio que está alimentada por generadores eléctricos diesel.

5.4.5 Evaluación de las Prácticas de Seguridad Organizacional en la Empresa Aguas del Chocó.

5.4.5.1 Práctica Seguridad 1:

Avisos de seguridad y entrenamientos: En la Aguas del Chocó, se nota una buena infraestructura tecnológica, con buenos niveles de seguridad, sin embargo es indispensable capacitar al personal que labora en ella de manera constante.

La empresa no cuenta con mecanismos de información de alertar para informar al personal por cualquier medio sobre una posible penetración de un evento mal intencionado en la red.

Es importante tener en cuenta que la seguridad no solo depende de la tecnología a nivel software – hardware que maneje la empresa, sino que en su mayoría

depende del personal que labora en ella, con una sola persona que logren engañar con métodos utilizados para vulnerar la seguridad de la empresa, como lo es la ingeniería social, entre otros, la empresa podría estar en riesgo total hasta el punto de ir a la quiebra.

Por todo lo anterior es importante que todos los miembros de la organización sepan utilizar y manejas sus productos, así mismo conocer la ubicación del sitio en la web, en conclusión el no tener el personal en constante capacitación genera un alto riesgo para la empresa.

5.4.5.2 Práctica Seguridad 2:

Estrategia de seguridad: es gratificante que se esté implementando un sistema de gestión de la seguridad de la información en la empresa, pero es importante s auditarlo cada año, esto permite detectar posibles vulnerabilidades frente al manejo de la información que se le está dando, y así evitar prácticas inadecuadas que generen traumatismo para la empresa.

5.4.5.3 Práctica Seguridad 3:

Gestión de seguridad: como gestión la empresa Aguas del Chocó, está implemento este sistema de gestión de la seguridad de la información, la cual manifiestan que será un éxito total, sin embargo se debe implementar estrategias de acuerdo de confidencialidad a todos los empleados, así como inculcarle sentido de pertenencia por la empresa. Aun que se podría suponer tener todos los documentos que la acreditar para prestar el servicio, no cuenta con los certificados de calidad para prestar este tipo de servicios como los de la ISO 27001 Norma para asegurar la buena gestión de los activos de la información con el objetivo de garantizar la eficiencia de los procesos y la continuidad de la empresa. Al implementar los requisitos de ISO 27001 se reduce el riesgo en los sistemas de información, mediante la implementación de controles adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información (slideboom, 2007) .

5.4.5.4 Práctica Seguridad 4:

Políticas de seguridad y regulaciones: por lo general las políticas de seguridad de la información, así como sus regulaciones, están detalladas en el sistema de gestión de la seguridad de la información de la empresa, es importante resaltar que este debe ser publicado en un sitio web donde todos puedan tener acceso fácilmente.

5.4.5.5 Práctica Seguridad 5:

Gestión de la seguridad colaborativa: Como se evidencia en el diagrama de red y la información suministrada por la empresa, el servicio de internet es prestado por la empresa Telefónica, que cuenta con un servidor de acceso remoto telefónico, el cual se conectan los servidores de la red externa igualmente protegidos por un firewall externo, todo esto indica que el tráfico de red que se mueva en ese segmento es responsabilidad directa de la empresa, ya que el

aplicativo donde prestan los servicios esta implementada en un sistemas por capas de red aumentando al máximo los niveles de seguridad.
Igualmente la empresa cuenta con modem alternativo para la prestación del servicio de internet, garantizando el respaldo en caso que el otro falle.

5.4.5.6 Práctica Seguridad 6:

Planeación de contingencia: en la empresa no se evidencia un plan de contingencia o recuperación de desastre para garantizar el buen estado de los equipos y programas en la red, en caso de desastres naturales, terremoto, incendio, inundación, etc. Una vez pase un evento de esta naturaleza no existe un procedimiento para garantizar la continuidad en las operaciones y del servicio.

En conclusión no se evidencia una verdadera gestión de respaldos, lo que demuestra que la información de los usuarios no está muy bien protegida.

5.4.5.7 Practica Seguridad 7:

Control de acceso físico: se evidencia un buen control de seguridad a nivel físico dentro de la organización, detallando sistemas de vigilancia las 24 horas del día frente al registro de las personas que ingresan a cada una de sus áreas, igualmente existe un control de los dispositivos que entran y salen de la organización minimizando el riesgo por robo de información con equipos portátiles o pen driver.

5.4.5.8 Práctica Seguridad 8:

Auditoria y monitoreo de acceso físico: existe un director responsable de la seguridad de la empresa en cuanto a seguridad informática y seguridad física, pero no se evidencia las políticas y procedimiento que se desarrollan en ella para evitar una posible penetración de manera física.

5.4.5.9 Práctica Seguridad 9:

Gestión de sistemas y red: se evidencian actualizaciones de software de manera segura por medio de Update, al igual que la implementación de planes de seguridad, pero no hay evidencia de que tipos de herramientas a nivel de software se manejan para mitigar cualquier riesgo.

5.4.5.10 Practica Seguridad 10:

Monitoreo y auditoria de seguridad de la tecnología de la información: así se tenga buenas prácticas en el desarrollo y tráfico de la red, se debe contar con auditorias de monitoreo en la red, para garantizar la vigilancia permanente de los datos que la empresa está dedicada netamente a actividades de facturación y recaudo de nivel financiero, espacio atractivo para los ciberdelincuentes.

5.4.5.11 Práctica Seguridad 11:

Autenticación y autorización: es bueno contar con un buen firewall configurado tanto físico como software, pero se considera documentar los niveles de acceso a los usuarios, para este caso la autenticación se encuentra en otra instancia,

probablemente por cuestiones de seguridad no se recomienda suministrar esta información.

5.4.5.12 Práctica Seguridad 12:

Gestión de vulnerabilidad: es importante para garantizar un buen monitoreo del sistema la empresa, se debe contar con lista de chequeos para determinar cuando y donde hay que realizar una actualización o parches para mitigar un posible riesgo, por lo cual no se evidencia una buena gestión por parte de la organización.

5.4.5.13 Práctica Seguridad 13:

Encriptación: existen prácticas de autenticación en varios segmentos de la red, pero no hay evidencia de sistemas de encriptación para la protección de datos y contraseñas por parte de los usuarios tanto internos como externos, igualmente se puede suponer que la publicación hace parte de la reserva de la seguridad de la empresa.

5.4.5.14 Práctica Seguridad 14:

Arquitectura y diseño de seguridad: se evidencia la documentación y diseño de la red mostrando su diagrama estructural, pero se hace necesarios documentar la arquitectura y diseño de seguridad de la información, así como un flujograma de seguridad, igualmente se puede deducir que este documento hace parte de la reserva de la información.

5.4.5.15 Práctica Seguridad 15:

Gestión de incidentes legales: se evidencian la utilización de licencias de software de manera legal, pero igualmente no es claro quién es el responsable de las fallas de este tipo de adquisición para efectos de garantías y pólizas de seguros, tanto para eventos catastróficos y otras denominaciones.

5.4.6 Requerimientos Legales y Recomendaciones

Tras la falencias detectadas en el punto anterior, aplicando las 15 prácticas de seguridad de la metodología OCTAVE-S, frente a los activos identificados en la Aguas del Chocó, se generó la siguiente tabla de requerimientos legales y recomendaciones a seguir.

Tabla 7: Requerimientos Legales y Recomendaciones a Seguir

ACTIVOS DE INFORMACIÓN REQUERIMIENTOS LEGALES Y RECOMENDACIONES A SEGUIR	
RED/ZONA DESMILITARIZADA (DMZ)	
SERVIDOR DNS INTERNO + HOST IDS	Se debe proteger de cualquier ataque, en especial los de suplantación de identidad, de lo contrarios asumir las condiciones jurídicas que acarrean perjudicando a los miles de usuarios que interactúan en la plataforma, atentando contra la confidencialidad de los usuarios.
SERVIDOR DE CORREO ELECTRONICO + HOST IDS	Se debe proteger la identidad del usuario, para el caso se trata de servicios financieros, en especial facturación, por lo tanto se recomienda utilizar credenciales o certificados de autenticación, para garantizar y minimizar el riesgo de falsificación o suplantación de identidad.
NETWORK IDS	Estar en permanente actualización, en especial a los sistemas de detección de intrusos, ya que los ciberdelincuentes evolucionan en sus prácticas por penetrar estos activos que son tan atractivos.
FIREWALL ZONA WI-FI	Contar con las últimas actualizaciones tomadas directamente de la casa de los proveedores del equipo para evitar la inclusión de ficheros maliciosos, ya que esta es la parte más crítica

	y vulnerable por los medio de conexión.
AP	Tener bien sincronizados estos dispositivos, sobre todo en la implementación y configuración del firewall licenciado, así como aplicar las políticas de autenticación para ingreso al sistema, con el objetivo de blindar estos agujeros.
RED INTERNA DE SERVICIOS	
SERVIDOR DE BASES DE DATOS	Contar con las licencias actualizadas de todos los motores de bases de datos, sobretodo actualizaciones confiable para evitar la inyección de código malicioso u ataques masivos de fuerza bruta, ya que la vida de la empresa se encuentra en estos equipos.
SERVIDOR DE APLICACIONES	Tener seriamente desligado este equipo, conservando los niveles de la capa de red, para garantizar que no entre ni salga información de la base de datos si no se trata del personal con las verdaderas credenciales.
MAINFRAME	
SERVIDOR DE FICHEROS E IMPRESIÓN	Desligar este equipo de la red, aumentando los niveles de credenciales y privilegios de acceso ya que esta es la zona critica de la empresa, su mayor atractivo es el personal interno en especial los intrusos o visitantes

	mal intencionados.
RED DE USUARIOS	
WORKSTATIONS	Los equipos internos se deben mantener con los niveles de seguridad por si algún visitante mal intencionado intenta acceder físicamente de manera fraudulenta, al igual que la protección y vigilancia del robo de hardware.
SOFTWARES Y POLÍTICAS DE SEGURIDAD	
Licencias de Windows	Se recomienda delegar esta función especialmente al área de seguridad, para que examine rigurosamente el contenido de las adquisiciones y actualización, igualmente contar con el marco jurídico que cuente con plenas garantías de utilización.
Plan de gestión de la seguridad de la información.	Es obligación de la empresa actualizar permanentemente los planes de gestión de la información, así como designar un comité para su aplicación y evaluación, teniendo en cuenta que los métodos de robo cambian todos los días.

Fuente: Levantamiento de campo en el análisis de riesgo.

5.5. Fase Dos

5.5.1 Identificar Vulnerabilidades en la Infraestructura.

Para poder identificar las vulnerabilidades en la infraestructura computacional de la empresa Aguas del Chocó, fue necesario relacionar como lo indica la metodología OCTAVE-S, los componentes de la red con los activos críticos, así como la identificación de la importancia entre ellos.

Examinar la infraestructura computacional examinando las rutas de acceso.

De acuerdo a los estudios anteriores se puede determinar cómo los activos más importante de la empresa Aguas del Chocó, el servidor de aplicaciones y el servidor de bases de datos, por cuanto que allí están alojadas todas las aplicaciones con los servicios que ofrece la empresa, al igual que la información de los usuarios que se considera lo más sagrado, para un mayor análisis se identifican las rutas de acceso y los componentes claves de la red, relacionadas con el sistema, de acuerdo a diagrama de red, se puede concluir que los dos servidores están en un segmento de red denominado Zona desmilitarizada, se conectan mediante un Switch, pasando por un firewall, donde seguidamente toma el acceso a internet tanto por RDSI O ISP, el problema de esta estructura es que los dos servidores están ubicados en el mismo segmento de red, cuyos detalles se describen el siguiente paso de la metodología OCTAVE-S.

Específicamente el problema radica, que tanto el servidor de aplicaciones y el de bases de datos de la empresa, están en el mismo segmento de red, evidenciando un riesgo de descifrar o rastrear fácilmente, es decir con uno de los dos que se ubique, poniéndolo en contexto se podría saber dónde está el otro, porque se ubican en la misma zona desmilitarizada, este rastreo se puede realizar mediante algún método de ataque, puede ser el de inyección de código malicioso.

Aunque la empresa cumple con los lineamientos de la red por capa, la recomendación es que estos servidores estén separados, es decir en lugares diferentes, fuera de la infraestructura física de la empresa, con esto se consigue mitigar varios puntos de riesgo, que es la prevención de un posible evento catastrófico como terremoto, incendio, inundación etc., y la segregación de los puntos de acceso de los proveedores de internet, como es de conocimiento estos servicios cuentan con IPs dinámica o estática, la cual se apuntando hacia ese dirección se podría escanear todos los dispositivos conectados en ella.

Por ende para incrementar los niveles de seguridad es necesario que estén en diferentes puntos. Desde otra óptica del diagrama de red están los usuarios internos que implican un riesgo por el fácil acceso a los servidores y a la información, como alguien debe responder por un robo dentro de la empresa, se recomienda que los actores internos firmen acuerdos de confidencialidad, para no divulgar la información a nadie, garantizándole al usuario su total integridad, y por otro lado responsabilizando al actor interno las consecuencias jurídicas que acarrea la divulgación.

5.5.1.1 Responsabilidades como administrador de red

Cabe resaltar que es responsabilidad directa del administrador de la red todo lo concerniente u evento criminal que terceras personas ajenas a la empresa Aguas del Chocó realicen desde adentro.

Sin duda la seguridad de la empresa e incluso de las personas que laboran en ella está en manos del administrador, la mayoría de los usuarios que navegan en ella son inexpertos, es por ello que se sienten en confianza y acceden a todas sus cuentas electrónicas, como redes sociales y bancos que son los más comunes, siendo consciente de la inmensa responsabilidad es necesario ser un excelente administrador de la red, cuando se desconoce y se ignora la necesidad de tener una red segura, el caso es tan grave que pudiésemos ir a para a la cárcel inocentemente, es algo similar a ser director de una cárcel penitenciaria, es decir que si un recluso sale por algún lado del entorno físico sin que nadie absolutamente nadie lo detenga, la responsabilidad es netamente del director y debe pagar por ello siempre y cuando no se demuestre la causa por qué salió, poniendo en contexto a nivel de seguridad es responsabilidad del administrador de la red cuando un usuario mal intencionado se conecta a red y comete un delito informático, como todos sabemos los expertos en seguridad informática forense consiguen el rastro y ubican a la empresa la cual somos responsables.

Consiente de todas las herramientas utilizadas para hacer que un ataque sea exitoso, deben tener algunas precauciones, como una buena configuración de los dispositivos Wifi siendo el de mayor importancia el cifrado WPA2, monitorear constantemente quien se conecta y estar pendiente si el listado de direcciones IP es superior a las configuradas.

Otras precauciones que se deben tener, son los virus informáticos, hay que evitar al máximo una propagación de este, recordemos que es igual de peligroso que tener un intruso conectado a la red de la empresa, estos ficheros maliciosos los envían en todas las presentaciones, como correos electrónicos, memorias USB, páginas web atractivas utilizadas como señuelo, y el método más utilizadas en el momento ingeniería social, entre otros, la mayoría de los virus son creados para infectar maquinas con el objetivo de obtener, datos bancarios, datos personales, datos utilizados para estafar a las personas, email, redes sociales, o para obtener datos útiles para ser vendidos a empresas de publicidad o Data Brokers, entre otros dejando claro que se trata del cibercrimen.

5.6. Fase Tres

5.6.1 Informe de Evaluación del Riesgo

Después de identificar las vulnerabilidades como se describe en la fase dos, teniendo en cuenta que la empresa ya se encuentra en la implementación de un sistema de gestión de la seguridad de la información, por ello se ha diseñado un informe de evaluación del riesgo de la empresa Aguas del Chocó.

Tabla 8: Riesgos Encontrados

LISTA DE RIESGOS ENCONTRADOS				
CATEGORÍAS	**RIESGO**	**RIESGOS ENCONTRADOS**		**ÁREAS VULNERABLES**
		NIVEL DE IMPORTANCIA	**INSTRUMENTOS PARA MEDIR NIVEL**	
CONFIANZA DE USUARIOS	Fraude Suplantación de identidad	Alta	Monitorización	Director de operaciones
	Fallas de autenticación	Alta	Monitorización	Director de operaciones
	Fraude Suplantación de identidad	Alta	Monitorización	Director de operaciones
FINANCIERA	Falta de coordinación de la parte administrativa.	Bajo	Observación directa	Gerente
	Falta de asignación de responsabilidades de los eventos y actividades en la red	Bajo	Observación directa	Gerente
SEGURIDAD DE LAS PERSONAS	El personal encargado del área de seguridad no ejerce sus funciones	Bajo	Entrevista o descripción del caso	Responsable de la seguridad

LISTA DE RIESGOS ENCONTRADOS				
CATEGORÍAS	**RIESGO**	**RIESGOS ENCONTRADOS**		**ÁREAS VULNERABLES**
		NIVEL DE IMPORTANCIA	**INSTRUMENTOS PARA MEDIR NIVEL**	
	adecuadamente.			
	Las personas que interactúan en el sistema no aplican el sistema de gestión de la seguridad de la información.	Bajo	Entrevista o descripción del caso	Responsable de la seguridad
PRODUCTIVIDAD	Demora en el restablecimiento del sistemas	Alta	Monitorización	Director de operaciones
	Fallas de hardware	Alta	Monitorización	Director de operaciones
	Falla de software	Alta	Monitorización	Director de operaciones
MULTAS O PENALIZACIONES LEGALES	Realizar actualizaciones servidores no reconocidos	Bajo	Monitorización	Director de operaciones
	No pagar las licencias de los sistemas operativos con tiempo	Bajo	Monitorización	Director financiero

LISTA DE RIESGOS ENCONTRADOS				
CATEGORÍAS	**RIESGO**	**RIESGOS ENCONTRADOS**		**ÁREAS VULNERABLES**
		NIVEL DE IMPORTANCIA	**INSTRUMENTOS PARA MEDIR NIVEL**	
	Aplicar parches defectuosos	Bajo	Monitorización	Director de operaciones
	Instalación de ficheros maliciosos	Bajo	Monitorización	Director de operaciones

Fuente: Levantamiento de campo en el análisis de riesgo.

Tabla 9: Vulnerabilidades y Amenazas

LISTA DE VULNERABILIDADES Y AMENAZAS			
NO.	**VULNERABILIDADES DE SEGURIDAD**	**AMENAZAS DE SEGURIDAD**	**DESCRIPCIÓN DE LA AMENAZA**
1	Desconocimiento de los criterios de la seguridad informática de los Administrativos y Funcionarios.	Administrativos y funcionarios débiles y de fácil penetración por ingeniería social.	Alcance de la información por ingeniería social. Falta de estrategias de prevención y predicción de ataques.
2	Uso de dispositivos de almacenamientos externos para el transporte de información (Pen Drive, etc)	Rotación y propagación de virus con información y datos viciados.	Transporte de archivos, datos, y elementos informáticos dañinos para el

LISTA DE VULNERABILIDADES Y AMENAZAS			
NO.	**VULNERABILIDADES DE SEGURIDAD**	**AMENAZAS DE SEGURIDAD**	**DESCRIPCIÓN DE LA AMENAZA**
			sistema.
3	Falta de backup de Datos, Archivos e Información	Inexistencia en el almacenamiento de la información de respaldo.	La pérdida de información genera riesgos de seguridad.
4	Error en la configuración de las políticas de seguridad del Sistema.	Fragilidad y facilidad en la penetración en los sistemas de seguridad.	Los privilegios de las políticas de seguridad no se cumplen según los estructurados y permiten accesos inesperados.
5	Falla en el hardware de los equipos (Mantenimiento de Equipos)	El daño parcial o Total de los equipos permite la perdida de información,	La falta de mantenimiento preventivo y predictivo genera la reducción de la vida útil de los equipos.
6	Personal Administrativo o funcionarios en cuanto a la ingeniería social de hacker y/o Cracker.	Los funcionarios y Administrativos son vulnerables a razón de la información pertinente de la seguridad en la ingeniería social.	La filtración o falta de aplicación de políticas de seguridad que impidan el acceso a claves o contraseñas de los usuarios por falta de capacitación en prevención.
7	Control de Acceso al cuarto de comunicaciones de personal	El acceso a equipos y	El acceso o manejo de equipos

LISTA DE VULNERABILIDADES Y AMENAZAS			
NO.	**VULNERABILIDADES DE SEGURIDAD**	**AMENAZAS DE SEGURIDAD**	**DESCRIPCIÓN DE LA AMENAZA**
	no autorizado.	componentes de la red por personal no autorizado.	de la red sin el conocimiento indicado permiten la generación y debilidad en las redes.
8	Aplicación de políticas de seguridad a las contraseñas o Password de los Administrativos y funcionarios.	Las contraseñas y actualización periódica de las mismas no cumplen con las políticas de seguridad.	Fácil acceso e identificación de las contraseñas o Password.
9	Configuración no adecuada de los equipos de comunicación (Switch, Router, etc) Permisos de Router por defecto.	La falta de privilegios de seguridad en los equipos activos y de comunicación no permite establecer las políticas de seguridad. Cualquier miembro externo o interno puede acceder a la infraestructura computacional de la empresa. Robo de información.	La configuración inadecuada permite establecer rutas de vulnerabilidad de los sistemas.
10	Capacitación y actualización de	La falta de	El

LISTA DE VULNERABILIDADES Y AMENAZAS			
NO.	**VULNERABILIDADES DE SEGURIDAD**	**AMENAZAS DE SEGURIDAD**	**DESCRIPCIÓN DE LA AMENAZA**
	los Administrativos y Funcionarios en políticas de Seguridad Informática en el activo más importante de la empresa.	actualizaciones y capacitaciones de los funcionarios establecen criterios de inseguridad informática.	desconocimiento de la seguridad informática y sus políticas generan vulnerabilidades en el sistema generados por los funcionarios.
11	Debilidad en el diseño de protocolos utilizados en las redes y Políticas de seguridad baja.	La falta de protocolos, Normas y Estándares de seguridad.	Permeabilidad de las políticas de seguridad de la red.
12	Conectividad wifi de cualquier equipo externo a la red corporativa.	La falta de configuración para limitar el acceso a la red inalámbrica	Cualquier miembro externo o interno puede acceder a la infraestructura computacional de la empresa. Robo de información.

Fuente: Levantamiento de campo evaluación del análisis de riesgo arroja la Lista De Vulnerabilidades Y Amenazas.

Tabla 10: Valoración de Riesgos

VALORACION DE RIESGOS			
ESCALA PROBABILIDAD		**ESCALA IMPACTO**	
A	**ALTA**	**C**	**CATASTROFICO**
M	**MEDIA**	**M**	**MODERADO**
B	**BAJA**	**L**	**LEVE**

Fuente: Evaluación del riesgo conforme a la metodología. ISO 270001.

Tabla 11. Niveles de probabilidad e impacto

RIESGOS / VALORACION		PROBABILIDAD			IMPACTO		
		A	M	B	L	M	C
R1	Desconocimiento de los criterios de la seguridad informática de los Administrativos y Funcionarios.		X			X	
R2	Uso de dispositivos de almacenamientos externos para el transporte de información (Pen Drive, etc)	X					X
R3	Falta de backup de Datos, Archivos e Información		X		X		
R4	Error en la configuración de las políticas de seguridad del Sistema.		X			X	
R5	Falla en el hardware de los equipos (Mantenimiento de Equipos)	X			X		
R6	Personal Administrativo o funcionarios en cuanto a la ingeniería social de hacker y/o Cracker.			X		X	
R7	Control de Acceso al cuarto de comunicaciones de personal no autorizado.		X		X		
R8	Aplicación de políticas de seguridad a las contraseñas o Password de los Administrativos y funcionarios.		X			X	
R9	Configuración no adecuada de los equipos de comunicación (Switch, Router, etc)	X					X

	Permisos de Router por defecto.						
R10	Capacitación y actualización de los Administrativos y Funcionarios en políticas de Seguridad Informática en el activo más importante de la empresa.		**X**				**X**
R11	Debilidad en el diseño de protocolos utilizados en las redes y Políticas de seguridad baja.		**X**		**X**		
R12	Conectividad Wifi de cualquier equipo externo a la red corporativa.		**X**				**X**

Fuente: Valoración del riesgo conforme a la metodología. ISO 270001.

Tabla 12: Matriz Clasificación de Riesgos

MATRIZ CLASIFICACIÓN DE RIESGOS			
	LEVE	**MODERADO**	**CATASTROFICO**
ALTO	R5		R9, R2
MEDIO	R3, R7, R11	R8, R1, R4	R10, R12
BAJO		R6	

Fuente: Matriz conforme a la metodología. ISO 270001.

6. CAPITULO 5: ESQUEMA DOCUMENTAL DEL SGSI DE LA AGUAS DEL CHOCÓ.

6.1. Introducción

Es de conocimiento que lo más importante de la empresa Aguas del Chocó, es estar preparada para todos y cada uno de los eventos adversos que pueden llegar a sucederles, pues pueden llegar a impactar las actividades del negocio, estas organizaciones dependen de sus recursos, del personal, poseen bienes tangibles, sistemas y tecnologías de información, etc y si alguno de estos componentes es dañado o deja de estar accesible, pueden llegar a paralizarse y muchas veces se ven abocadas a comenzar de nuevo desde cero.

Para la empresa es de suma importancia, tener las políticas y objetivos de la seguridad de la información claro, en lugares públicos donde los empleados puedan tener acceso con facilidad, determinando puntos objetivos y fáciles de ejecutar.

Teniendo en cuenta la importancia que genera, contar con una certificación ISO 27001, la empresa debe contar con las declaraciones de aplicabilidad bien documentadas.

Para la empresa Aguas del Chocó, es obligado el tema de la “Gestión de la Seguridad de la Información” y ha dejado de ser un tema relevante ocupando una posición muy importante ante la alta gerencia, es por este motivo que es importante contar con un PLAN DE TRATAMIENTO DE RIESGOS de la actividad del Negocio en caso de que ocurran incidentes graves y la estrategia de la adopción de un plan de continuidad adicional a prevenir o minimizar las pérdidas para el negocio constituye un ejercicio de responsabilidad ante los clientes.

Para desarrollar un buen tratamiento de los 12 riesgos detectados en el análisis de riesgos para la empresa Aguas del Chocó, se implementó el **Plan de Tratamiento de Riesgos,** mediante un formato que identifica desde su estructura organizacional el impacto de cada riesgo, se toma una valoración y seguimiento, así como su respectivo monitoreo y aplicación de mitigación por parte del responsable de cada área.

6.2. Objetivo

6.2.1 General

Identificar las diferentes formas de tratar los riesgos, evaluando las amaneas y vulnerabilidades para lograr un buen análisis de riesgo de cada uno de los activos del sistema de gestión de la información de la empresa Aguas del Chocó, de manera que permita aplicar los controles de mitigación de riesgo llevándolos a su mínima expresión.

6.2.2 Objetivos Específicos

- Mitigar el riesgo aplicando controles que lleven el activo a un nivel aceptable estipulado por la gerencia de la empresa.
- Amortizar el posible impacto en el momento que ocurra un riesgo, detectando eventos no deseables, relacionados y recuperándose de ello.
- Documentar y revisar los controles de mitigación del riesgo emanados por la norma ISO 270001.

6.3. Política y Objetivos de la Seguridad de la Información

El presente documento tiene como finalidad la implementación de las Políticas de Seguridad Informática (PSI) para la empresa Aguas del Chocó.

Para la ejecución de esta Política de Seguridad de la información, se ha tenido en cuenta el análisis de riesgos que se realizó a la empresa anteriormente en el capítulo 5 con el propósito de poder detectar las vulnerabilidades y amenazas que puedan materializarse y producir daños en los activos informáticos.

6.3.1 Objetivo

Dotar de la información necesaria en el más amplio nivel de detalle a los usuarios, contratistas, empleados y directivos de Aguas del Chocó, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red institucional, así como la información que es procesada y almacenada en estos.

6.3.2 Alcance

La Política de Seguridad de la Información de Aguas del Chocó, se crea en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información.

La presente política debe ser conocida y cumplida por todo el personal de la empresa sin distingo de rango ni tipo de contratación en todo el ámbito de la Institución, a sus recursos y a la totalidad de los procesos, internos y externos.

De acuerdo a lo anterior, la información que genera y gestiona la institución constituye un activo estratégico clave para asegurar la continuidad del negocio, por lo que la Seguridad de la Información es una herramienta para garantizar su integridad, disponibilidad y confidencialidad.

Entre las Políticas de Seguridad tenemos:

6.3.3 Tratamiento Total de la Seguridad:

Para la empresa Aguas del Chocó, un tratamiento total incluye aspectos de la seguridad de los computadores distintos a los de la seguridad de los Sistemas Operativos, como pueden ser:

La seguridad externa, haciendo referencia al aspecto físico, debe garantizar el control de intrusos o personal ajeno a la empresa, así como también la preparación ante desastres como incendios e inundaciones.

Concedido el acceso físico, el S.O debe identificar al usuario antes de permitirle el acceso a los recursos (Seguridad de la interfaz del usuario).

La seguridad interna, hace énfasis a los controles incorporados tanto del hardware, como del S.O para asegurar la confiabilidad, operabilidad y la integridad de los programas y datos.

6.3.4 Seguridad Externa y Seguridad Operacional

6.3.4.1 Seguridad Externa

Consiste básicamente en la Seguridad Física, la cual incluye la Protección contra desastres e intrusos; para lo cual se hace necesario algunos mecanismos de detección como: Detectores de humo, Sensores de calor, Detectores de movimiento, entre otros.

6.3.4.2 Seguridad Operacional

Consiste en las diferentes políticas y procedimientos implementados por el Departamento de Sistemas y Telecomunicaciones de la empresa, para la instalación computacional.

6.3.5 Red Interna

Dentro de las Políticas de uso y administración de la Red interna de la empresa Aguas del Chocó. se encuentran:

La disposición de un directorio compartido, de uso exclusivo para los empleados de la empresa, solo con fines de uso laboral (compartir y almacenar información pertinente a sus tareas), no para almacenar cosas personales.

Se realizarán copias de seguridad una vez por semana (Sábados), a la información guardada en la Red Interna por los empleados de la empresa y del Sistema de Gestión de Proyectos; estas copias se realizarán en un medio de almacenamiento externo, con el fin de proteger la información y tener respaldo de los datos.

6.3.6 Disposición y Manejo de los Equipos de Cómputo

Para la empresa Aguas del Chocó, es de vital importancia esta Política de Seguridad, la cual hace referencia a:

Al gabinete de Telecomunicación o Área de Sistemas, ubicada en el Centro de Cableado Principal en donde se encuentran los Servidores, debe permanecer cerrada con el acceso restringido por controles de acceso por personal autorizado; cualquier persona que ingrese, deberá registrarse en la bitácora con su nombre, firma y motivo de la visita. De igual forma, dicha área debe permanecer con el Aire acondicionado en correcto funcionamientos, control de incendios, su respectivo respaldo eléctrico mediante UPS y a una temperatura adecuada para los Servidores.

6.3.7 Cuentas de Usuarios

Es la cuenta que constituye la principal vía de acceso a los sistemas de información que posee la empresa; estas cuentas aíslan al usuario del entorno, impidiendo que pueda dañar al sistema u otros usuarios, y permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros. Procedimiento para la creación de cuentas nuevas:

- La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por escrito y ser debidamente autorizada por el Director del Departamento de Sistemas y Telecomunicaciones.
- Cuando un usuario recibe una cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad informática y acepta sus responsabilidades con relación al uso de esa cuenta.

6.3.8 Protección por Contraseña

- El usuario es responsable exclusivo de mantener a salvo su contraseña.
- La longitud mínima de caracteres permisibles en una contraseña se establece de 8 caracteres, los cuales tendrán una combinación alfanumérica y también puede usar signos.
- La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres.
- Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guardada en un lugar seguro.
- El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

6.3.9 Sistemas Supervivientes

Para el Departamento de Sistemas de la empresa Aguas del Chocó, el diseño de sistemas de alta seguridad debe asegurar:

- Su operación de manera continua y confiable.
- Su disponibilidad.

6.3.10 Internet

Dentro de las Políticas de uso y administración del Internet y con base a que esta es una herramienta cuyo uso autoriza la empresa en forma extraordinaria, puesto que contiene ciertos peligros, debido a que los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas. El Departamento de Sistemas de la empresa Aguas del Chocó, ha estipulado que se debe aplicar una política que procure la seguridad y el monitoreo constante de este servicio.

6.3.11 Correo Electrónico

Generalidades frete al uso del correo:

- Utilizar el correo electrónico corporativo, como una herramienta de trabajo y no como casillero personal, para lo cual existe el correo personal.
- No enviar archivos de gran tamaño a compañeros de oficina. Para eso existe la Intranet o Directorios compartidos dentro de la Red Interna.
- No facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.

- Si se recibe un correo de origen desconocido, consultar inmediatamente con el Departamento de Sistemas sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc).

6.3.12 Penetración al Sistema Operativo

En vista de que para el Departamento de Sistemas y Telecomunicaciones, la penetración al Sistema Operativo puede consistir en cambiar el bit de estado de la máquina, del estado problema al estado supervisor; el intruso podrá así ejecutar instrucciones privilegiadas para obtener acceso a los recursos protegidos por el S.O.

6.3.13 Generalidades

Cada uno de los Departamentos que hacen parte de la empresa Aguas del Chocó, deberá de emitir al Director del Departamento de Sistemas y Telecomunicaciones, los riesgos, inconvenientes, vulnerabilidades, y demás aspectos que consideren relevantes para las actividades críticas que realicen, con el fin de poder elaborar un esquema de Seguridad y Planes de Contingencia para los Sistemas Operativos, por parte del Departamento de Soporte Tecnológico e Informático de la empresa.

6.3.14 Sanciones

Cualquier violación a las Políticas y Normas de Seguridad para los Sistemas Operativos con que cuenta la Planes de Contingencia para los Sistemas Operativos, por parte del Departamento de Soporte Tecnológico e Informático de la empresa, y que se han establecido en este documento; deberá ser sancionada de acuerdo al reglamento interno, emitido por la Dirección del Departamento de Sistemas de la empresa, avalada por la JUNTA DIRECTIVA DE SOCIOS y la GERENCIA.

Las sanciones se pueden ver reflejadas, desde un llamado de atención, acta de descargos, o hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

6.3.15 Recomendaciones

Se tendrá que conformar y convocar un COMITÉ DE SEGURIDAD INFORMATICA a nivel de la alta gerencia, la cual estará al tanto de cada uno de los riesgos, problemáticas, inconvenientes, vulnerabilidades, y demás aspectos que se consideren relevantes para la Seguridad e Integridad de los Sistemas de la Empresa. Para el óptimo funcionamiento del Departamento de Sistemas y Telecomunicaciones, se recomienda conformar tres procesos específicos, los cuales velarán por el óptimo funcionamiento de la infraestructura tecnológica de la entidad. Estos procesos estarán distribuidos de la siguiente manera:

- Proceso de soporte y mantenimiento.
- Proceso de administración de redes.

- Proceso de Informática, investigación y desarrollo

Se recomienda implementar planes de contingencia para todos los procesos concernientes a la Seguridad informática y continuidad del negocio.

7. CAPÍTULO 6: DECLARACIÓN DE APLICABILIDAD EN EL SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACION DE LA EMPRESA AGUAS DEL CHOCÓ.

La declaración de aplicabilidad ó en ingles SOA(Statement of Applicability) es un documento que relaciona los controles que se utilizan en el momento de implementar el sistema de gestión de seguridad de la información en una organización . Estos controles se encuentran consignados en el anexo A de la norma ISO 27001:2013 para que las organizaciones u empresa interesadas en obtener la certificación seleccionen aquellos que más se adecuen según sus características específicas como: el tipo de actividad que desarrolla, el tamaño y el sector para que posteriormente se puedan implantar.

La elección de los controles forma parte del Plan de Tratamiento de riesgos. Este plan consiste en definir de una forma clara y concisa cómo se van a implementar los controles, quién será el responsable de ello, cuándo tendrá lugar y cuánto costará. En definitiva, este documento recoge un plan de actuación necesario para coordinar todas las actividades que se desarrollarán en el proyecto de certificación de ISO 27001.

Es un documento que lista los objetivos y controles que se van a implementar en una Organización, así como las justificaciones de aquellos controles que no van a ser implementados. Para conseguir este listado único, se requiere de una identificación de riesgos, definición de controles, identificación de requisitos legales, regulatorios, contractuales, etc, y claro está, de revisar las necesidades de la Organización.

Esta identificación se conoce como un análisis de brecha o gap analysis, el cual identifica la diferencia entre lo que debería tenerse implementado en la organización y lo que se tiene realmente disponible.

7.1. Formato de Declaración de Aplicabilidad.

Cada compañía es independiente a la hora de crear su formato teniendo en cuenta su Sistema de Gestión de Seguridad de la Información, pero hay ciertos parámetros que se deben cumplir. Estos parámetros son:

- Número del control del anexo A de la norma.
- Una explicación en la que se diga si el control es aplicable o no.
- Procedimientos o especificaciones que implantan el control.

Tabla 13: Declaración de Aplicabilidad

	DECLARACION DE APLICABILIDAD				
CONTROLES		IMPLEMENTADO			RAZONES PARA IMPLANTARLO O MEJORARLO
NUMERO DE CONTROL ISO/ ECI 27001:2013	REQUERIMIENTOS	SI	NO	NO APLICA	
5. POLÍTICAS DE SEGURIDAD					
5.1 Directrices de la Dirección en seguridad de la información					
5.1.1 Conjunto de políticas para la seguridad de la información.	La Dirección debería conocer aprobar y publicar un documento de la política de seguridad de la Información y comunicar la política a todos los empleados y las partes externas relevantes.		X		Desconocimiento de los criterios de la seguridad informática delos Administrativos y Funcionarios.
5.1.2 Revisión de las políticas para la seguridad de la información.	La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.	X			Los privilegios de las políticas de seguridad no se cumplen según los estructurados y Permiten accesos inesperados.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN					
6.1 Organización interna.					
6.1.1 Asignación de	Se deberían definir claramente todas las		X		Las responsabilidade

responsabilidades para la seguridad de la información.	responsabilidades para la seguridad de la información.				s son conocidas a nivel informal en la organización.
6.1.2 Segregación de tareas.	Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.		X		Los roles están segregados informalmente. Solo las funciones más importantes de los cargos del área de sistemas se encuentran documentados en el manual de funciones.
6.1.3 Contacto con las autoridades.	Se deberían mantener los contactos apropiados con las autoridades pertinentes.	X			Existe un proceso de gestión legal y cumplimiento normativo en donde se establecen los procedimientos para gestionar las relaciones con las autoridades reguladoras.
6.1.5 Seguridad de la información en la gestión de proyectos.	Se debería manejar protocolos de seguridad en el manejo de información sobre los nuevos proyectos que	X			Existen protocolos pero debería mejorarse pues a veces no está

	se están desarrollando, probando y produciendo. así como para el archivo de los productos resultantes (código fuente, documentación del proyecto como: diseños, planes de pruebas, material de documentación del producto, etc)				claro a quien se le debe permiso para acceder a la información de los nuevos proyectos, lo que podría ocasionar que la competencia pueda acceder a información sumamente importante para el negocio.
6.2 Dispositivos para movilidad y teletrabajo.					
6.2.1 Política de uso de dispositivos para movilidad.	Se debería establecer medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.		X		No se tiene en cuenta políticas para el manejo de aplicaciones de informática móvil.
6.2.2 Teletrabajo.	Se debería desarrollar e implantar una política, planes operacionales y procedimientos para las actividades de teletrabajo.			X	Todavía no se ha implementado el teletrabajo en la empresa.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.					
7.1 Antes de la contratación.					
7.1.1 Investigación de antecedentes.	Se deberían realizar revisiones de verificación de antecedentes de los	X			Se investigan los antecedentes para los

	candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.				candidatos a cargos en la empresa, dependiendo el cargo y la información a la que tendrá acceso.
7.1.2 Términos y condiciones de contratación.	Como parte de su compromiso con la empresa, los empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	X			La empresa diseñó un documento de confidencialidad que debe ser firmado por los funcionarios, empleados, contratistas y terceros.
7.2 Durante la contratación.					
7.2.1 Responsabilidades de gestión.	La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la		X		La dirección reconoce a la seguridad con un factor decisivo en el negocio, pero le falta mejorar su gestión para que haya una

	organización.				adecuada sinergia en la empresa.
7.2.2 Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.		X		Se realiza capacitación sobre temas de seguridad esporádicamente, pero no se hace de manera constante y completa.
7.2.3 Proceso disciplinario.	Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.		X		No se especifican de forma clara las sanciones previstas por incumplimiento de la Política de Seguridad de la Información.
7.3 Cese o cambio de puesto de trabajo.					
7.3.1 Cese o cambio de puesto de trabajo.	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas.	X			Se informa al área de sistemas el retiro de los funcionarios Los jefes de área son los responsables de

					ejecutar la finalización de un empleo frente a funcionarios que estén a su cargo. El área de recursos humanos y administrativos está encargada de los trámites administrativos de la finalización del contrato.
8. GESTIÓN DE ACTIVOS.					
8.1 Responsabilidad sobre los activos.					
8.1.3 Uso aceptable de los activos.	Todos los empleados y contratistas deberían hacer buen uso de los activos de la empresa para el logro de los objetivos propuestos por la empresa.		X		El personal hace uso de los recursos informáticos como internet para entrar a su correo personal y hacer actividades diferentes al trabajo que se les fue asignado.
8.1.4 Devolución de activos.	Todos los empleados, contratistas y terceros deberían devolver todos los activos de la	X			Al finalizar un contrato con la compañía, el área de

	organización que estén en su posesión a la finalización de su empleo, contrato o acuerdo.				recursos humanos y administrativos es responsable de verificar que todos los activos de la organización que estén en posesión empleados, contratistas y terceros sean devueltos.
9. CONTROL DE ACCESOS.					
9.1 Requisitos de negocio para el control de accesos.					
9.1.1 Política de control de accesos.	Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.	X			La plataforma de red de la compañía cuenta con un firewall que bloquea los accesos no autorizados en la red
9.1.2 Control de acceso a las redes y servicios asociados.	En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la política de		X		Los empleados pueden ingresar de forma remota a la red interna de la empresa lo que puede causar problemas que pueden comprometer la disponibilidad y

	control de accesos y necesidad de uso de las aplicaciones de negocio. Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio.				confidencialidad de la información
10. CIFRADO.					
10.1 Controles criptográficos.					
10.1.1 Política de uso de los controles criptográficos.	Deberían implantarse controles criptográficos como firmas y certificados digitales para que la confidencialidad e integridad de la información se mantengan		X		Existen prácticas de autenticación en varios segmentos de la red, pero no hay evidencia de sistemas de encriptación para la protección de datos y contraseñas por parte de los usuarios tanto internos como externos.
11. SEGURIDAD FÍSICA Y AMBIENTAL.					

11.1 Áreas seguras.					
11.1.1 Perímetro de seguridad física.	Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.		X		Aunque los servidores y dispositivos se encuentran aislados ,no se manejan dispositivos de seguridad física como tarjetas de control de entrada que impidan el ingreso de personas no autorizadas a zonas restringidas
11.1.2 Controles físicos de entrada.	Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.	X			se evidencia un buen control de seguridad a nivel físico dentro de la organización, detallando sistemas de vigilancia las 24 horas del día frente al registro de las personas que ingresan a cada una de sus áreas, igualmente existe un control de los

					dispositivos que entran y salen de la organización minimizando el riesgo por robo de información con equipos portátiles o pen driver
11.1.3 Seguridad de oficinas, despachos y recursos.	Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.	X			Existe personal encargado de la seguridad y protección de las instalaciones Sumado a eso se cuenta con cámaras de video que vigilan constantemente las puertas de ingreso a cada oficina.
11.1.4 Protección contra las amenazas externas y ambientales.	Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	X			La empresa cuenta con un programa de brigadas de acción en caso de emergencia. Implementos de seguridad.

					ambiental y física a. Extintores b. Sistema de aire acondicionado c. Red regulada de voltaje d. Detector de humo y/o incendio
11.2 Seguridad de los equipos.					
11.2.1 Emplazamiento y protección de equipos.	El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.	X			Se define el procedimiento seguro para realizar la instalación de equipos.
11.2.2 Instalaciones de suministro.	Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.	X			El edificio cuenta con dos plantas de energía accionadas automáticamente en caso de Interrupción eléctrica. La compañía cuenta con una

					UPS que funciona en caso de presentarse una falta de Energía.
11.2.3 Seguridad del cableado.	Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.		X		El cableado de las instalaciones de la empresa tiene algunas deficienciencias porque no cumple con las normas de cableado aceptas internacionalmente.
11.2.4 Mantenimiento de los equipos.	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.		X		El mantenimiento a los equipos se hace de forma deficiente.
11.2.5 Salida de activos fuera de las dependencias de la empresa.	Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos.			X	No aplica debido a que la compañía no cuenta con equipos fuera de sus instalaciones.
11.2.6 Seguridad de los equipos y activos fuera de	Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la			X	No aplica debido a que la compañía no cuenta con

las instalaciones.	organización considerando los diversos riesgos a los que están expuestos.				equipos fuera de sus instalaciones
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación	X			Se realiza el control de dispositivos usb conectados al equipo.
12. SEGURIDAD EN LA OPERATIVA.					
12.1 Responsabilidades y procedimientos de operación.					
12.1.1 Documentación de procedimientos de operación.	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.	**X**			En la intranet de la compañía se encuentran publicados los procedimientos de la compañía, así como instructivos de usuario para operaciones específicas.
12.1.2 Gestión de cambios.	Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información.	**X**			Los cambios son realizados por el personal debidamente autorizado

12.1.3 Gestión de capacidades.					
12.1.4 Separación de entornos de desarrollo, prueba y producción.	Se debería separar cada uno de los entornos de la empresa para evitar perdida de información y errores de operación.	X			Los desarrolladores son el únicos que están autorizados a acceder a los entornos de desarrollo y las personas encargadas de pruebas y producción poseen su propio ambiente con recursos informáticos asignados a cada uno
12.2 Protección contra código malicioso.					
12.2.1 Controles contra el código malicioso.	Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.	X			Los equipos de la compañía se encuentran protegidos por software de detección y reparación de virus y mensualmente se publican las estadísticas de virus como forma de concienciación.

					La empresa cuenta con un programa de bloqueo de código móvil y de ejecutables en las estaciones de trabajo
12.3 Copias de seguridad.					
12.3.1 Copias de seguridad de la información.	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.	X			Se realizan copias de seguridad en soportes
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.					
16.1 Gestión de incidentes de seguridad de la información y mejoras.					
16.1.1 Responsabilidades y procedimientos.	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.		X		Existe un procedimiento informal de registro de fallos Procedimientos de Manejo de Incidentes es estipula que se establecerán funciones y procedimientos

					de manejo de incidentes
16.1.2 Notificación de los eventos de seguridad de la información.	Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados.		X		No existe la comunicación de eventos de riesgo operativo se comunican en el contexto establecido por el sistema de administración del riesgo operativo
16.1.3 Notificación de puntos débiles de la seguridad.	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.		X		No existe una comunicación de debilidades en Materia de Seguridad
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.					
17.1 Continuidad de la seguridad de la información.					
17.1.1 Planificación de la continuidad de la seguridad de la información.	La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.		X		La empresa no cuenta con los requisitos establecidos para garantizar la continuidad del servicio en situación de

					desastre.
17.1.2 Implantación de la continuidad de la seguridad de la información.	La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.		X		La empresa no ha establecido los lineamientos para iniciar un mantenimiento al momento de un desastre natural.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.		X		La empresa no cuenta con controles de revisión de dispositivos al momento de un desastre.
17.2 Redundancias.					
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	Debería haber instalaciones adecuadas para el procesamiento de la información en la empresa.	X			Para el almacenamiento de datos de los diferentes estados de la aplicación y sus usuarios. Estos mismos servidores de bases de datos

					implementan otras bases de datos corporativas como son por ejemplo las del Sistema de Gestión de Proyectos.
18. CUMPLIMIENTO.					
18.1 Cumplimiento de los requisitos legales y contractuales.					
18.1.1 Identificación de la legislación aplicable.	Todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la organización para cumplir con estos requisitos, deberían ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información y la Organización.	X			Las leyes y normatividad aplicables a la seguridad de la información que rigen sobre la empresa se encuentran documentadas
18.1.2 Derechos de propiedad intelectual (DPI).	Se deberían implantar procedimientos adecuados que garanticen el cumplimento de la legislación, regulaciones y requisitos contractuales para el		X		Los derechos de propiedad intelectual no son contemplados en los acuerdos de servicios la empresa no

	uso de material con posibles derechos de propiedad intelectual asociados y para el uso de productos software propietario.				cuenta con un software que permita detectar el uso de software no autorizado en la empresa.
18.1.3 Protección de los registros de la organización.	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio.	X			Existe un área de archivo en donde se custodian los registros importantes de la compañía, por otra parte las garantías de contratos se encuentran debidamente custodiadas en un gabinete metálico especial.
18.1.4 Protección de datos y privacidad de la información personal.	Se debería garantizar la protección y privacidad de los datos y según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales	X			existe una definición de la responsabilidad del manejo de los datos de carácter personal
18.1.5 Regulación de los controles criptográficos.	Se deberían utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes.	X			Se conocen y cumplen parcialmente los requisitos emitidos por la Superintendencia Financiera

					sobre los controles cifrados.
18.2 Revisiones de la seguridad de la información.					
18.2.1 Revisión independiente de la seguridad de la información.	Se debe realizar revisión periódica (mensual) de la seguridad de la información.		X		La empresa no cuenta con mecanismos de información de alertar para informar al personal por cualquier medio sobre una posible penetración de un evento mal intencionado relacionado con el manejo de la información
18.2.2 Cumplimiento de las políticas y normas de seguridad.	Los directivos se deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad	X			Existen procedimientos informales del revisión del cumplimiento de normas por parte del personal
18.2.3 Comprobación del cumplimiento.	Se debería comprobar regularmente la conformidad de los sistemas de información con los estándares de		X		El sistema de gestión de la seguridad de la información en la empresa, está

	Implantación de la seguridad.				en estado de implementación pero aún no ha sido terminado, la cual permite detectar posibles vulnerabilidades frente al manejo de la información que se le está dando, y así evitar prácticas inadecuadas que generen traumatismo para la empresa.

Fuente: Aplicación del anexo(A) de Metodología. ISO 270001 para Declaración De Aplicabilidad.

7.2. Plan de Tratamiento de Riesgos

Para el tratamiento del riesgo es necesario evaluar con las opciones específicas de las dos tablas siguientes.

Tabla 14: Tratamiento del riesgo

Tratamiento del riesgo:
Evitar
Implementado
Reducir
En implementación

Fuente: Metodología. ISO 270001 para Tratamiento del Riesgo.

Tabla 15: Valoración del Riesgo

Valoración del Riesgo			
PROBABILIDAD	**IMPACTO**	**EVALUACIÓN**	**VALORACIÓN**
[1] Baja	[5] Leve	Aceptable	Aceptable
[2] Media	[10] Moderado	Tolerable	Tolerable
[3] Alta	[20] Catastrófico	Moderado	Moderado
		Importante	Importante
		Inaceptable	Inaceptable

Fuente: Metodología. ISO 270001 para la Valoración del Riesgo.

Tabla 16: Tratamiento del Riesgo R1

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 1

Macroproceso: **Responsable Seguridad**

Proceso: Responsable de sistemas de información

Riesgo: Desconocimiento de los criterios de la seguridad informática de los Administrativos y Funcionarios.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[2] Media**	**[10] Moderado**	**Moderado**	**Moderado**	Tratamiento del riesgo:	**Evitar**

Acción:

Evitar el acceso a redes sociales, correos personales, paginas no autorizadas

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R1	Restringir el acceso a páginas no autorizadas dentro de la empresa.	Departamento de seguridad informática.	26/03/2015	31/05/2015	01/06/2015	Responsable Seguridad	Administrativos y funcionarios débiles y de fácil penetración por ingeniería social.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 1), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 17: Tratamiento del Riesgo R2

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 2 de 2

Macroproceso: **Director Operaciones**

Proceso: Director de Sistemas de información

Riesgo: Uso de dispositivos de almacenamientos externos para el transporte de información (Pen Drive, etc)

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[3] Alta**	**[20] Catastrófico**	**Inaceptable**	**Inaceptable**	Tratamiento del riesgo:	**Evitar**

Acción:

Deshabilitar los puestos de

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R2	Uso de dispositivos de almacenamientos externos para el transporte de información (Pen Drive, etc)	Sistemas de información	26/03/2015	31/05/2015	01/06/2015	Director Operaciones	Rotación y propagación de virus con información y datos viciados.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 2), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 18: Tratamiento del Riesgo R3

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 3

Macroproceso: **Responsable Seguridad**

Proceso: Departamento seguridad industrial

Riesgo: Falta de backup de Datos, Archivos e Información

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[2] Media**	**[5] Leve**	**Tolerable**	**Tolerable**	Tratamiento del riesgo:	**Asumir**

Acción:

Diseñar mecanismos de respaldo por fuera de la sede principal.

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R3	Falta de backup de Datos, Archivos e Información	Departamento seguridad industrial	26/03/2015	31/05/2015	01/06/2015	Responsable Seguridad	Inexistencia en el almacenamiento de la información de respaldo, en los momentos catastróficos.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 3), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 19: Tratamiento del Riesgo R4

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 4

Macroproceso: **Director Operaciones**

Proceso: Responsable Sistemas de información

Riesgo: Error en la configuración de las políticas de seguridad del Sistema.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN	
Calificación del Riesgo:	**[2] Media**	**[10] Moderado**	**Moderado**	**Moderado**	Tratamiento del riesgo: **Asumir**

Acción:

Cumplir con los lineamientos que rige el sistema de gestión de seguridad de la información.

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R4	Penetración en los sistemas de seguridad.	Sistemas de información	26/03/2015	31/05/2015	01/06/2015	Director Operaciones	Error en la configuración de las políticas de seguridad del Sistema.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 4), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 20: Tratamiento del Riesgo R5

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 5

Macroproceso: **Responsable de sistemas de información**

Proceso: Departamento de tecnología e información

Riesgo: Falla en el hardware de los equipos (Mantenimiento de Equipos)

Calificación del Riesgo:	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN	Tratamiento del riesgo:	
	[3] Alta	**[5] Leve**	**Tolerable**	**Tolerable**		**Reducir**

Acción: Realizar los mantenimientos preventivos y correctivos de los equipos para reducir la probabilidad de algún daño.

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R5	El daño parcial o Total de los equipos permite la perdida de información,	Departamento de tecnología e información	26/03/2015	31/05/2015	01/06/2015	Responsable de sistemas de información	Falla en el hardware de los equipos (Mantenimiento de Equipos)	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 5), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 21: Tratamiento del Riesgo R6

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 6

Macroproceso: **Responsable Seguridad**

Proceso: Departamento de seguridad informática

Riesgo: Personal Administrativo o funcionarios en cuanto a la ingeniería social de hacker y/o Cracker.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[1] Baja**	**[10] Moderado**	**Tolerable**	**Tolerable**	Tratamiento del riesgo:	**Evitar**

Acción:

Evitar el acceso a redes sociales, correos personales, paginas no autorizadas

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R6	restringir el acceso a páginas no autorizadas dentro de la empresa	Departamento de seguridad informática	26/03/2015	31/05/2015	01/06/2015	Seguridad	Los funcionarios y Administrativos son vulnerables a razón de la información pertinente de la seguridad en la ingeniería social.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 6), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 22: Tratamiento del Riesgo R7

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 7

Macroproceso: **Responsable Seguridad**

Proceso: Departamento Seguridad Industrial

Riesgo: Control de Acceso al cuarto de comunicaciones de personal no autorizado.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[2] Media**	**[5] Leve**	**Aceptable**	**Aceptable**	Tratamiento del riesgo:	**Compartir**

Acción:

Señalizar el área restringida para evitar posibles inconvenientes

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R7	Implementar sistemas biométricos de acceso para evitar el acceso a personal no autorizado.	Departamento Seguridad Industrial	26/03/2015	31/05/2015	01/06/2015	Seguridad	El acceso a equipos y componentes de la red por personal no autorizado.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 7), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 23: Tratamiento del Riesgo R8

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 8

Macroproceso: **Responsable Seguridad**

Proceso: Departamento Seguridad Informática

Riesgo: Aplicación de políticas de seguridad a las contraseñas o Password de los Administrativos y funcionarios.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[2] Media**	**[10] Moderado**	**Moderado**	**Moderado**	Tratamiento del riesgo:	**Asumir**

Acción:

Cumplir con los parámetros establecidos en las políticas de seguridad de la empresa

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R8	Implementar contraseñas que cumplan con los criterios de seguridad mínimo de caracteres 8 máximo 12.	Departamento Seguridad Informática	26/03/2015	31/05/2015	01/06/2015	Seguridad	Las contraseñas y actualización periódica de las mismas no cumplen con las políticas de seguridad.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 8), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 24: Tratamiento del Riesgo R9

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100 VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 9

Macroproceso: **Responsable Seguridad**

Proceso: Departamento Seguridad Informática

Riesgo: Configuración no adecuada de los equipos de comunicación (Switch, Router, etc)
Permisos de Router por defecto.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[3] Alta**	**[20] Catastrófico**	**Inaceptable**	**Inaceptable**	Tratamiento del riesgo:	**Evitar**

Acción:

Seguir las instrucciones de configuración, plasmadas en las políticas de seguridad de la empresa.

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R9	Aplicar la configuración con los niveles de seguridad necesarios para evitar este tipo de incidentes.	Departamento Seguridad Informática	26/03/2015	31/05/2015	01/06/2015	Seguridad	La falta de privilegios de seguridad en los equipos activos y de comunicación no permite establecer las políticas de seguridad. Cualquier miembro externo o interno puede acceder a la infraestructura computacional de la empresa. Robo de información.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 9), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 25: Tratamiento del Riesgo R10

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 10

Macroproceso: **Director de operaciones**

Proceso: Departamento Sistemas de información

Riesgo: Capacitación y actualización de los Administrativos y Funcionarios en políticas de Seguridad Informática en el activo más importante de la empresa.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[2] Media**	**[10] Moderado**	**Moderado**	**Moderado**	Tratamiento del riesgo:	**Compartir**

Acción:

Actualizar periódicamente y hacer cumplir el sistema de gestión de seguridad de la información de la empresa.

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R10	Publicar las políticas de seguridad donde todos los funcionarios puedan acceder con facilidad.	Sistemas de información	26/03/2015	31/05/2015	01/06/2015	Director de operaciones.	La falta de actualizaciones y capacitaciones de los funcionarios establecen criterios de inseguridad informática.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 10), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 26: Tratamiento del Riesgo R11

	PLAN DE TRATAMIENTO DE RIESGOS	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 11

Macroproceso: **Director de operaciones**

Proceso: Departamento Sistemas de información

Riesgo: Debilidad en el diseño de protocolos utilizados en las redes y Políticas de seguridad baja.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[2] Media**	**[10] Moderado**	**Moderado**	**Moderado**	Tratamiento del riesgo:	**Compartir**

Acción:

Actualizar periódicamente y hacer cumplir el sistema de gestión de seguridad de la información de la empresa.

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R11	Implementar mecanismos criptográficos para el manejo de la información.	Sistemas de información	26/03/2015	31/05/2015	01/06/2015	Director de operaciones.	La falta de protocolos, Normas y Estándares de seguridad.	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 11), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

Tabla 27: Tratamiento del Riesgo R12

Empresa Aguas del Chocó	**PLAN DE TRATAMIENTO DE RIESGOS**	COD: 100
		VERSION: 1.0
	FORMATO DE TRATAMIENTO DE RIESGOS	Página 1 de 12

Macroproceso: **Responsable de Seguridad.**

Proceso: Departamento seguridad informática

Riesgo: Conectividad wifi de cualquier equipo externo a la red corporativa.

	PROBABILIDAD	IMPACTO	EVALUACIÓN	VALORACIÓN		
Calificación del Riesgo:	**[2] Media**	**[20] Catastrófico**	**Importante**	**Importante**	Tratamiento del riesgo:	**Evitar**

Acción:

Implementar la configuración adecuada utilizando los niveles más altos de seguridad plasmados en las políticas de seguridad.

Plan de Tratamiento del Riesgo

Nº	Actividades	Responsable	Fecha de Inicio	Fecha de Cierre	Fecha de Seguimiento	Responsable del seguimiento	Hallazgos	Estado de la actividad
R12	Restringir el acceso a los equipos no autorizados, utilizando un segundo nivel de seguridad.	Departamento seguridad informática	26/03/2015	31/05/2015	01/06/2015	Seguridad.	La falta de configuración para limitar el acceso a la red inalámbrica	**Sin implementar**

Política de tratamiento del Riesgo

Observaciones

Fecha: 26/03/2015

Aprobado: Luis Carlos Palacios Mosquera
Equipo de Gestión

Fuente: Tabla (8) Lista de Riesgos Encontrados Tabla (9) lista de Vulnerabilidades y Amaneas (Items 12), Tabla (13) de Tratamiento del Riesgo, Tabla (14) de Valoración del Riesgo.

8. CAPÍTULO 7: POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Las siguientes políticas de seguridad son aplicables a los clientes y proveedores, que tengan alguna relación con la empresa **Aguas del Chocó.** bien sea de tipo legal, contractual o de cualquier otra índole y que en razón de ésta, tengan acceso a aplicativos, centros de cómputo, redes u otros aspectos regulados en este documento.

8.1. Política de Acceso Portátiles Sede Empresa Aguas del Chocó

Todo portátil que ingrese por la portería, deberá ser registrado en los formatos definidos por el Departamento de Seguridad Informática de la empresa Aguas del Chocó, y podrá ser revisado por el personal de sistemas. Tecnología Información, con el fin de determinar si los equipos cumplen con los requisitos mínimos establecidos por esta área.

Estos requisitos son:

1. Programa antimalware, actualizado.
2. Actualización del sistema operativo con los últimos parches liberados por el fabricante.
3. Tener activado el protector de pantalla protegido con contraseña.
4. Tener deshabilitado la conexión compartida de Internet en todas las interfaces.
5. Tener habilitado el firewall de Windows.

8.2. Requerimientos De Seguridad – Conexión Con Clientes.

8.2.1 Introducción

Con el fin de minimizar los riesgos que se puedan presentar al entregar información sensitiva de la empresa Aguas del Chocó a un Cliente o Proveedor, para que sea el quien la administre, la haga disponible para la empresa, y la proteja, se hace necesario contar con fuertes elementos de seguridad físicos, lógicos y procedimentales por parte de éstos.

8.2.2 Seguridad de la Red de Conexión con la Empresa Aguas del Chocó.

El proveedor, deberá presentar un diagrama detallado y completo de su arquitectura de red, en el cual se especifique también la relación con otras redes, en especial las de otros clientes.

Firewall: El firewall podrá ser cualquier hardware o software que se encuentre catalogado como firewall, más no como equipo de comunicaciones con

capacidades de firewalling deberá tener, como mínimo, capacidad para VPNs , e integración con detector de intrusos, o posibilidad para instalar un detector de intrusos.

8.2.3 Acceso a Través de Enlace Dedicado Privado.

El proveedor deberá garantizar que su red de conexión con otros clientes (incluyendo a la empresa Aguas del Chocó.) se encuentra separada de la zona desmilitarizada de Internet (DMZ).

El cliente, proveedor o tercero deberá garantizar que el enlace dedicado de la empresa Aguas del Chocó, llegará a una zona específicamente dispuesta para ello.

El proveedor deberá garantizar la independencia del tráfico de los diferentes clientes que acceden a la red de los primeros por este medio. Para ello, el proveedor deberá ofrecer adicionalmente a la empresa Aguas del Chocó, esquemas de conexión que incluyan VPNs.

8.2.4 Acceso Via VPN – Internet

El proveedor, podrá ofrecer adicionalmente a la empresa Aguas del Chocó. esquemas de conexión que incluyan VPNs vía Internet. Para esto, el proveedor deberá garantizar que la red VPN se encuentre separada de la zona desmilitarizada de Internet (DMZ), así como garantizar la independencia del tráfico VPN de los diferentes clientes que se conecten por este medio.

8.2.5 Seguridad en las Redes lan del Cliente Y Computadores de Usuario Final.

La versión de software del proveedor que se ejecutarán en las estaciones de usuario final deben ser compatibles con todas las actualizaciones de seguridad emitidas por parte de Microsoft y su programa de actualizaciones de definiciones mensual para corrección de vulnerabilidades detectadas a sus sistemas operativos y todos sus componentes como son: Internet Explorer, MDAC, SQL, etc.

La versión de Software del cliente o proveedor que se ejecutarán en las estaciones de usuario final deben ser compatibles con versiones de Antivirus conocidas, en particular con la instalada en la actualidad.

8.2.6 Usuarios, Contraseñas y Roles

El cliente o proveedor deberá cumplir las políticas de seguridad para el manejo de contraseñas establecido por la empresa Aguas del Chocó.

El cliente o proveedor deberá tener y presentar la información relacionada con sus políticas de seguridad con respecto al manejo de contraseñas.

El cliente o proveedor deberá proporcionar información sobre la forma en la cual se realiza la identificación, autenticación y autorización de los usuarios en la red de este.

El cliente o proveedor deberá tener y presentar la información sobre la forma en la cual se administra la creación, modificación o eliminación de las cuentas de los usuarios en la red de cada uno de estos.

8.3. Verificación de la Seguridad

8.3.1 Verificación Durante la Etapa de Análisis y Evaluación de Propuestas

La empresa Aguas del Chocó, podrá verificar a su discreción y sin previo aviso, el cumplimiento por parte del cliente o proveedor de los requerimientos anteriormente establecidos.

8.3.2 Acceso a Recursos y Aplicaciones de la Empresa Aguas del Chocó.

La empresa Aguas del Chocó, utilizará servicios de acceso remoto para la conexión del cliente o proveedor, a las aplicaciones y recursos requeridos, este será el único medio permitido por la empresa para el acceso a las aplicaciones.

La empresa se reserva el derecho a cambiar a su discreción la forma de acceso a las aplicaciones para esto, y si encuentra que la red del cliente o proveedor se puede ver afectada en un alto grado, se avisará a este con una anticipación no mínima a treinta (30) días calendario sobre las modificaciones a las que haya lugar.

8.4. Prohibiciones a los Clientes o Proveedores

Se encuentra prohibido a todos los clientes o proveedores que guarden alguna relación con la empresa Aguas del Chocó, las siguientes conductas:

- La descarga de programas, fotos, música, videos y demás tipo de información digital vía Internet, al igual que del tráfico de información vía Messenger o mensajería instantánea, a excepción de los medios autorizados por la empresa.

- Instalar en los equipos cualquier Software no autorizado, sin importar su modo de distribución, ya sea electrónica o físicamente.

- Compartir carpetas, transferir archivos por la red ya sea por Email o cualquier otro transporte, con fines diferentes a los laborales, ya sea para diversión, intrusión o cualquier otro tipo de interés.

- Dañar física o lógicamente los equipos o la infraestructura informática.

- Conectar, desconectar, desmantelar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización expresa del Gestor de seguridad de empresa.

- Instalar dispositivos o tarjetas de acceso remoto, módems, RDSI, routers o cualquier otro dispositivo de comunicaciones en los equipos e infraestructura tecnológica destinados para la prestación del servicio.

- Usar cuentas de equipos sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta.

- Realizar cualquier acto que interfiera en el correcto funcionamiento de los equipos informáticos o de la infraestructura tecnológica para la prestación del servicio, estaciones de trabajo de escritorio o portátiles, equipos terminales de telefonía o terminales de comunicaciones alámbricas o inalámbricas, equipos periféricos, red de comunicaciones, canal de comunicaciones de voz, datos o Internet.

- Instalar o ejecutar programas que perjudiquen la estabilidad de los equipos, su sistema operativo o sus programas internos o aplicaciones de las empresas. Esto incluye los programas conocidos como virus informáticos, cualquier tipo de ensayo o experimento, hardware, software, spammers, spimmers, troyanos, keyloggers, entre otros.

- Uso del servicio de manera tal que constituya una molestia, abuso, amenaza o que de cualquier forma atente contra la integridad del equipo e infraestructura tecnológica.

- Tratar de evitar o alterar los procesos o procedimientos de medida del tiempo, utilización del ancho de banda o cualquier otro método utilizado para documentar el uso de los productos y servicios.

- Extraer información física o electrónica que viole los derechos de autor y/o la confidencialidad de la empresa Aguas del Chocó. sus clientes o sus proveedores.

- Intentar sobrepasar protecciones de datos o sistemas de seguridad informática.

- Trasmitir cualquier información con fines personales diferentes a los a la relación contractual o de cualquier otra índole con la empresa, o con fines políticos o religiosos, campañas de SPAM, SPIM, ventas de artículos, entre otros.

- Uso de equipos portátiles propios, para acceso a los recursos tecnológicos de la empresa, sin previa autorización.

8.5. Otorgamiento de Permisos

Para la obtención de permisos para la instalación de programas, software, dispositivos entre otras herramientas informáticas especiales que se requieran para el cumplimiento de los objetivos relacionados con su vínculo como cliente o proveedor de la empresa Aguas del Chocó, deberá contar con documento escrito debidamente firmado por el Gestor de Seguridad Informática.

9. CAPÍTULO 8: PLAN DE CONTINUIDAD DE LA EMPRESA AGUAS DEL CHOCÓ.

9.1. Introducción

Un Plan de Continuidad del Negocio, es una concepción gerencial más que técnica, ya que se basa en el entendimiento de los procesos críticos de la empresa Aguas del Chocó, de los elementos que soportan su operación y el riesgo que representa la paralización parcial o total de los mismos en términos de pérdidas financieras u oportunidades de negocio.

Como vemos en la actualidad es importante para la empresa estar preparada para todos y cada uno de los eventos adversos que pueden llegar a sucederles, ya que pueden llegar a impactar las actividades del negocio. Las organizaciones dependen de sus recursos, del personal, poseen bienes tangibles, empleados, sistemas y tecnologías de información, etc y si alguno de estos componentes es dañado o deja de estar accesible, pueden llegar a paralizarse y muchas veces se ven abocadas a comenzar de nuevo desde cero.

Para este tipo de empresa es como una póliza de garantía contar con la implementación "**Sistemas de Gestión de Seguridad de la Información**" y ha dejado de ser un tema relevante ocupando una posición muy importante ante la alta gerencia, es importante contar con un plan alternativo que asegure la continuidad de la actividad del Negocio en caso de que ocurran incidentes graves y la estrategia de la adopción de un plan de continuidad adicional a prevenir o minimizar las pérdidas para el negocio se constituye un ejercicio de responsabilidad ante sus clientes.

Para una mejor orientación se trabajará con la Guía de Desarrollo de un Plan de Continuidad de Negocio (Jiménez, 2007)

9.2. Objetivos

9.2.1 General

Elaborar un plan de Continuidad de negocio para la empresa Aguas del Chocó

9.2.2 Específicos

- Diseñar un formato de chequeo que permita realizar la auditoría externa del SGSI con la metodología MAGERIT.
- Aplicar la normativa ISO/IEC 27001 y 27002.
- Conocer las estrategias que se puedan implementar para el aseguramiento de la continuidad del negocio en la empresa Aguas del Chocó.

9.3. Organización de los Equipos

9.3.1 Comité de Crisis

Su objetivo es el de reducir al máximo el riesgo y la incertidumbre en la dirección de la situación, debe tomar las decisiones “clave” durante los incidentes, además de hacer de enlace con la dirección de la empresa Aguas del Chocó, manteniéndoles informados de la situación regularmente.

Tabla 28: Comité de Crisis

Responsable del Comité:	JHON JAIRO MURILLO ALBORNOZ Seguridad Industrial Teléfono Móvil: 3104500281 Teléfono Casa: 6713524
Miembros del Comité:	YUSLEIDY CUESTA SAUCEDO Responsable de Seguridad Teléfono Móvil: 3218591714 Teléfono Casa:6722169
	HORIANA DEL MAR MOSQUERA GARCIA Responsable Diseño Teléfono Móvil: 3104500281 Teléfono Casa: 6715622

Fuente: Miembros del Comité de Crisis

9.3.1.1 Funciones

Análisis de la situación.

- Tomar la decisión de activar o no el Plan de Continuidad
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación
- Iniciar el proceso de notificación a los empleados

Lugar de Reunión: Oficina Director de Operaciones, Interior de la Aguas del Chocó

9.3.2 Equipo de Recuperación

Su función es restablecer la infraestructura necesaria para la recuperación. Esto incluye el servidor, PC’s, comunicaciones de voz y datos y cualquier otro elemento requerido para llevar a cabo la restauración de un servicio.

La empresa Aguas del Chocó por su tamaño a la fecha cuenta con personal calificado en las áreas de Seguridad Informática, Operaciones, y Mantenimiento - Reparación, quienes serán los encargados de llevar a cabo todo el proceso de recuperación, para lo cual deberá desarrollar las siguientes actividades:

Los profesionales que hagan parte de las dependencias antes mencionadas, deberán desplazarse hasta la Oficina de Seguridad Informática para recibir instrucciones. De acuerdo al orden de criticidad los sistemas a poner en marcha son: los Firewall, Servidores, Mainframe, Network IDS, Work stations y por últimos la WIFI.

Como alternativa de restablecimiento rápido se recomienda recurrir al servidor de respaldo para asegurar las últimas copias generadas.

Si se trata de daños catastróficos, acordar los puntos de reunión vía telefónica en oficinas externas o casa de algunas personas responsables.

Tabla 29: Equipo de Recuperación

Integrantes del equipo:	LUIS CARLOS PALACIOS MOSQUERA Depto. Seguridad Informática Teléfono Móvil: 3122099207 Teléfono Casa: 6713526 JORGE ARBOLEDA LOZANO Mantenimiento y Reparación Teléfono Móvil: 3128150585 Teléfono Casa: 6714320 FABIOLA VALENCIA CÓRDOBA Responsable de Operaciones Teléfono Móvil: 3207410210 Teléfono Casa: 6721872

Fuente: Miembros del Equipo de Recuperación de la empresa Aguas del Chocó

9.4. Fase de Alerta

En esta fase vamos a definir los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos.

9.4.1 Notificación

Cualquier empleado que haya detectado una situación de contingencia o un incidente (fuego, inundación, virus, etc.), debe dar aviso con el máximo posible de detalle de manera inmediata al Jefe o superior jerárquico, éste a su vez da aviso a la persona de contacto del Comité de Crisis (Seguridad Industrial); una vez que el miembro del Comité de Crisis es informado del incidente, procederá a analizar y evaluar la incidencia, estimando los tiempos de interrupción y los servicios

afectados, para luego con la recopilación de la mayor información posible convocar el equipo del Comité con el fin de evaluar la situación.

9.4.2 Evaluación

El Comité analizará la situación y deberá tomar la decisión de activar o no el Plan de continuidad. En caso de que la decisión sea no activar el Plan de Continuidad porque la gravedad del incidente no lo requiere, se requerirá gestionar el incidente para que no aumente su gravedad.

9.4.3 Ejecución del Plan

Una vez que el Comité de Crisis ha decidido poner en marcha el Plan de Recuperación, deberá comunicarse con los responsables del equipos de recuperación informando el inicio de las actividades del plan para que inicien los procedimientos de actuación de cada uno de ellos.

9.5. Fase de Transición

Puesto en marcha el plan, se deberá acudir a la oficina alterna. Uno de los miembros del comité se encargará de la logística, deberá iniciar con el traslado de personas a la oficina alterna y del material requerido (Copias de software crítico, Copias de seguridad, material de oficina, documentación, etc), para poner en marcha dicha oficina y así dar inicio a la intervención del equipo de recuperación, con el fin de establecer la infraestructura necesaria, tanto de software como de comunicaciones, etc.

Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como oficina alterna o cualquier otro designado por el Comité de Dirección de Crisis.

9.6. Fase de Recuperación

Establecidas las bases para dar inicio a la recuperación, se iniciará con la carga de datos y a la restauración de los servicios críticos, comprobando su funcionamiento con el fin de reanudar el negocio con las máximas garantías de éxito.

9.7. Fase de Vuelta a la Normalidad

Luego de haber solucionado la contingencia y haberse recuperado las actividades críticas de la empresa Aguas del Chocó, se deben establecer los mecanismos necesarios para volver a la normalidad del “día a día” de las actividades. Se debe llevar a cabo un análisis de impacto con el fin de valorar de forma detallada los daños presentados (equipos, instalaciones averiadas, etc), para así definir la estrategia de vuelta a la normalidad, dichas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

9.8. Generación de Informes y Evaluación

Cuando se determina el fin del incidente y se ha vuelto a la normalidad, se requiere que cada equipo realice un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados, dificultades con las que se encontraron, etc, y así las directivas podrán valorar la funcionalidad del plan o si se presentaron fallos similares corregirlos de una forma más rápida y oportuna.

9.9. Fin de la Contingencia

Dependiendo de la gravedad del incidente, la vuelta a la normalidad de operación puede variar entre horas, días o meses, lo realmente importante es que durante el transcurso de este tiempo de vuelta a la normalidad, el servicio a los clientes y empleados sea prestado y que la incidencia afecte lo menos posible a la empresa Aguas del Chocó.

9.9.1 Razones de Selección de Metodologías Para Auditoría de Sgsi Para el Diseño de los Formatos de la Empresa Aguas del Chocó

La auditoría utiliza el método deductivo-inductivo, pues realiza el examen y evaluación de los hechos empresariales objetos de estudio partiendo de un conocimiento general de los mismos, para luego dividirlos en unidades menores que permitan una mejor aproximación a la realidad que los originó para luego mediante un proceso de síntesis emitir una opinión profesional.

Por lo anterior, se escoge Magerit como la metodología indicada para la realización de estos formatos, puesto que Magerit contempla diferentes actividades o proceso que puede manejar una empresa y enmarca los activos que esta posee para el tratamiento de la información, a la vez permite separarlos de acuerdo a la función que cumplan dentro de la organización, para un auditor será más fácil elaborar formatos a aplicar en una auditoría teniendo como base los conceptos de activos esenciales, servicios interno, equipos informáticos (hardware), comunicaciones, soportes de información: discos, cintas, el entorno, energía, climatización, las instalaciones físicas, el personal, usuarios, operadores y administradores.

También es esencial en cuanto se refiere a las dimensiones de seguridad, puesto que la metodología Magerit contempla la confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad, en un sistema de información, no dejando de lado las amenazas que se presentan en la organización y el impacto que tendrán estas si llegan a materializarse.

Otra razón es que conociendo la metodología Magerit al momento de auditar los controles establecidos por la empresa Aguas del Chocó, se podrá determinar un plan de auditoría y crear formato para verificar, hacer seguimiento, supervisión y revisión de estos controles.

10. CONCLUSIONES

Toda organización sin importar su tamaño requiere utilizar un estándar o metodología de análisis, de evaluación y gestión de riesgos, que se actualicé periódicamente y que sea flexible con el tamaño y el propósito que tiene la organización para así poder detectar las vulnerabilidades, amenazas que puedan materializarse y producir daños en los activos informáticos.

Para disminuir los riesgos informáticos de la empresa Aguas del Chocó, fue necesario implementar dentro del marco de la norma ISO 27001, ANÁLISIS DE RIESGO INFORMÁTICO, DECLARACIÓN DE APLICABILIDAD, POLÍTICA DE SEGURIDAD PARA PROVEEDORES, PLAN DE CONTINUIDAD, aplicando dentro de cada uno las respectivas metodologías que permitieron minimizar los riesgos llegándolos hasta el punto de ser tratados en un impacto bajo.

Siempre y cuando se aplique de manera correcta las Políticas de Seguridad con este SGSI, se garantiza la disminución del riesgo a un 98%, igualmente la disminución del impactito y el tratamiento del mismo, sin desconocer que es indispensable mantener el SGSI actualizado.

La metodología de análisis de riesgo que es más flexible y que mejor se adecua a las organizaciones u empresas pequeñas como Aguas del Chocó, es OCTAVE-S debido a su flexibilidad y forma de realizar el análisis, la evaluación y gestión del riesgo.

Es supremamente importante saber escoger una metodología de rápida aplicación que implementa los pasos necesarios para analizar un sistema, identificar las amenazas, las vulnerabilidades asociadas, calcular la probabilidad de ocurrencia de esas amenazas, determinar del impacto en caso de su materialización y por último la obtención del riesgo al que se está expuesto.

Así que el Formato de Tratamiento de Riesgos, esta metodología es una herramienta de fácil implementación en una organización mediana ó pequeña como Aguas del Chocó que le permitiría identificar y gestionar los riesgos de tecnología de la información. El análisis de riesgos es el primer punto de la gestión de la seguridad de la información de una organización, y es necesario para realizar la gestión de los riesgos, es decir, tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos y controlarlos, es decir realizar la gestión de riesgos.

Para la empresa Aguas del Chocó, teniendo en cuenta el tamaño, los servicios, y la infraestructura de red que maneja, debe destinar un presupuesto considerable para la actualización constante del SGSI, ya que aplicación oportuna de las diferentes acciones garantiza la continuidad en la prestación de los servicios, así como un sistema sostenible en el tiempo, con un buen majo la tendencia de la empresa debe crecer, debido a la fortaleza de su SGSI.

La inversión realizada en el SGSI puede verse como un gasto innecesario, pero en el evento que haya un incidente crítico llevándolo al punto de activar los comités de crisis y reparación del riesgo, desde la gerencia se puede calcular los costos si no existiese implementado el SGSI, el solo hecho de restaurar una plataforma completa sin que los usuarios lo noten, podríamos decir no tanto el valor económico si no la efectividad del servicio que presta la Aguas del Chocó diferente a las demás en el mercado.

Para la empresa contar con un Plan De Continuidad en el SGSI, es de gran utilidad al momento de presentase algún daño o alguna situación no esperada, hace las veces de un plan de contingencia.

La lista de chequeo de Auditoría externas de un SGSI es importante para poder comprobar si se está cumpliendo con requerimientos básicos en la implantación de un SGSI, igualmente para una posterior actualización.

Finalmente hay que tener en cuenta las normas ISO 27001 y 27002 para continuar con las buenas prácticas de seguridad y las metodologías más reconocidas como la OCTAVE-S Y Magerit para aplicar las actualizaciones respectivas al SGSI de la empresa Aguas del Chocó, igualmente publicarlo en la página web oficial de la empres www.aguasdelchoco.gov.co

11. BIBLIOGRAFÍA

administracionelectronica.gob.es. (3 de 03 de 2012). Obtenido de administracionelectronica.gob.es: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VW-U2dJ_Oko

adriinfo22. (2014 de 04 de 01). *adriinfo22.blogspot.com*. Obtenido de http://adriinfo22.blogspot.com/2014_04_01_archive.html

Aguas del Chocó. (2013). *aguasdelchoco.gov.co*. Obtenido de http://www.aguasdelchoco.gov.co/index.php/quienes-somos

Arthur, D. M. (5 de Noviembre de 2012). *blog.utp.edu.co*. Obtenido de blog.utp.edu.co: http://blog.utp.edu.co/seguridadso/

desarrolloweb. (22 de 08 de 2001). *desarrolloweb.com*. Obtenido de http://www.desarrolloweb.com/articulos/513.php

ECURED. (s.f.). *www.ecured.cu*. Obtenido de www.ecured.cu: http://www.ecured.cu/index.php/Prueba_de_penetraci%C3%B3n

ISO. (2007). *iso27000.es.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

Jiménez, L. d. (2007). *descargas.abcdatos.com*. Obtenido de http://descargas.abcdatos.com/tutorial/descargarV111.html

riesgoscontrolinformatico.blogspot.es. (20 de 03 de 2014). Obtenido de riesgoscontrolinformatico.blogspot.es: http://riesgoscontrolinformatico.blogspot.es/tags/metodo-elegido-octave/

segu-info. (22 de 12 de 2000). *segu-info.com.ar*. Obtenido de https://www.segu-info.com.ar/malware/spam.htm

slideboom. (2007). *slideboom.com*. Obtenido de http://www.slideboom.com/presentations/497963/iso-270001

Speedy. (30 de 12 de 2014). *speedy.com.ar*. Obtenido de http://speedy.com.ar/cibermama/nota.php?not=77

Stallman, R. (8 de Mayo de 2003). *www.insecure.org*. Obtenido de www.insecure.org: http://insecure.org/tools/tools-es.html

Subinet. (13 de 10 de 2013). *subinet.es*. Obtenido de http://www.subinet.es/que-es-el-control-de-acceso-en-sistemas-informaticos/

Tarazona, C. A. (2013). *SEGURIDAD EN APLICACIONES WEB.* Bogotá: Creative Commons Attribution ShareAlike 3.0.

12. ANEXOS

Anexo A Lista de Chequeo – Auditoria Interna

FORMATO DE AUDITORIA INTERNA DEL SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCÓ

LISTA DE CHEQUEO – AUDITORIA INTERNA

Empresa:	**Aguas del Chocó**	**Evaluador:**	**Luis Carlos Palacios Mosquera**
Gerente:	**Juan Mena Rivas**	**Contacto:**	**3122099207**
Contacto:	**3137466711**	**Fecha:**	**10/05/2015**
Firma:		**Firma:**	

Ítem	Descripción	Cumple		Observación
		Si	No	
1	**Manual de Seguridad – Nivel 1**			
	a) Alcance del SGSI			
	- Cuentan con planes estratégicos y operativos de seguridad Informática.	**X**		
	- Cuentan con un plan de continuidad de Negocio	**X**		
	- Cuenta con soporte tecnológico de hardware e infraestructura	**X**		
	- Cuenta con sistema de Backus de la información	**X**		
	- Cuenta con soporte Lógico			
	- Cuentan con documentación de políticas, procedimientos y mejores practicas	**X**		
	b) Políticas y Objetivos			
	- Los criterios, principios y lineamientos de la seguridad informática son integrales	**X**		
	- La normativa y legislación son vigentes	**X**		

	- Cumple con los requerimientos contractuales referentes a la seguridad informática	**X**		
	- Cuenta con mecanismos de gestión de los riesgos.	**X**		
	c) Metodología de Evaluación de Riesgos			
	- Tiene un plan de evaluación de riesgos informáticos	**X**		
	- Cuentan con los procedimientos de evaluación de amenazas	**X**		
	- Cuentan con procedimientos de análisis de vulnerabilidades.	**X**		
	d) Informe de Evaluación de Riesgos			
	- Considera aplicar la metodología de evaluación anteriormente mencionada.	**X**		
	e) Plan de Tratamiento del Riesgo	**X**		
	- Cuenta con un documento que define las acciones para reducir, prevenir, transferir o asumir los riesgos informáticos	**X**		
2	**Procedimientos – Nivel 2**			
	- Cuentan con los documentos que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo medir la efectividad de los controles	**X**		
3	**Instrucciones/Formularios – Nivel 3**			
	- Cuenta con los documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.	**X**		
4	**Registros – Nivel 4**			
	- Cuenta con los documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI	**X**		

Anexo B **Formato de Lista de Chequeo - Plan de Continuidad del Negocio**

Empresa Aguas del Chocó	**PLAN DE CONTINUIDAD DEL NEGOCIO**	COD: 101 VERSION: 0.0
	FORMATO DE LISTA DE CHEQUEO	Página 1 de 1

ELEMENTOS DE CONTROL PARA LA SEGURIDAD DE LOS SISTEMAS OPERATIVOS
LISTA DE CHEQUEO

FECHA:	**NOMBRE DE LA EMPRESA:** **Aguas del Chocó**	**NIT: 900354051-1**
REPRESENTANTE LEGAL: Juan Mena Rivas.	**REVISADO POR: Luis Carlos Palacios**	**DEP/CUIDAD: Chocó - Quibdó**

PASOS	ITEMS	ALTA	MEDIA	BAJA	OBSERVACIONES	RECOMENDACIONES
Encargado de sistemas						
1	Cumple requisitos	X			BUEN PERFIL	
2	Nivel de experiencia	X			4 AÑOS EN ESTE TIPO DE CARGO	
3	Capacitación		X		CADA 6 MESES	
4	Actualización		X		CADA 6 MESES	
Encargado de Seguridad Informática						
5	Cumple requisitos	X			BUEN PERFIL	
6	Nivel de experiencia		X		2 AÑOS EN SGSI	
7	Capacitación			X	CADA AÑO	
8	Actualización			X	CADA AÑO	
Apoyo de la gerencia						
9	Contratación hacker ético			X	FALTA DE PERSONAL	
Implementación de SGSI						
10	Identificación de riesgos	X			SE RAALIZÓ	
11	Análisis de riesgos	X			SE RAALIZÓ	
12	Actualización de Normas y Modelos de SGSI		X		SE ESTÁ REALIZANDO	

13	Aplicación de Normas y Modelos de SGSI		X		SE ESTÁ REALIZANDO	
14	Plan de Contingencia		X		SE RAALIZÓ	
15	Aplicación de controles		X		SE ESTÁ IMPLEMENTANDO	
Auditorías Internas						
16	Plan de Contingencia		X		SE ESTÁ IMPLEMENTANDO	
17	Aplicación de controles		X		SE ESTÁ IMPLEMENTANDO	
18	Monitorización de actividades		X		SE ESTÁ IMPLEMENTANDO	
19	Aplicación de Ingeniera Social a empleados			X	PENDIENTE HACERLO	
Análisis de Infraestructura de Red						
20	Mantenimiento de equipos	X			DOS AL AÑO	
21	Mantenimiento de conectores	X			DOS AL AÑO	
22	Configuración de Equipos	X			CUANDO SE REQUIERE	
23	Historial y análisis de fallas		X		EN EL HELP DESK	
24	Documentación de Actividades		X		EQUIPO DE SISTEMAS	
Análisis de Infraestructura Eléctrica						
25	Mantenimiento de equipos		X		CUANDO LO REQUIERE	
26	Mantenimiento de conectores		X		CUANDO LO REQUIERE	
27	Historial y análisis de fallas			X	FALTA IMPLEMENTARLA	
28	Documentación de Actividades		X		EN EL HELP DESK	
29	Funcionamiento de planta eléctrica	X			BUEN MANTENIMIENTO	FALTA REDUNDANCIA
30	Funcionamiento de UPS	X			BUEN MANTENIMIENTO	FALTA REDUNDANCIA
Análisis de vulnerabilidad de aplicaciones						
31	Software de Backup			X	NO EXISTE	
32	Software Antivirus	X			LICENCIADO	
33	Aplicaciones basadas en PHP			X	NO APLICA	

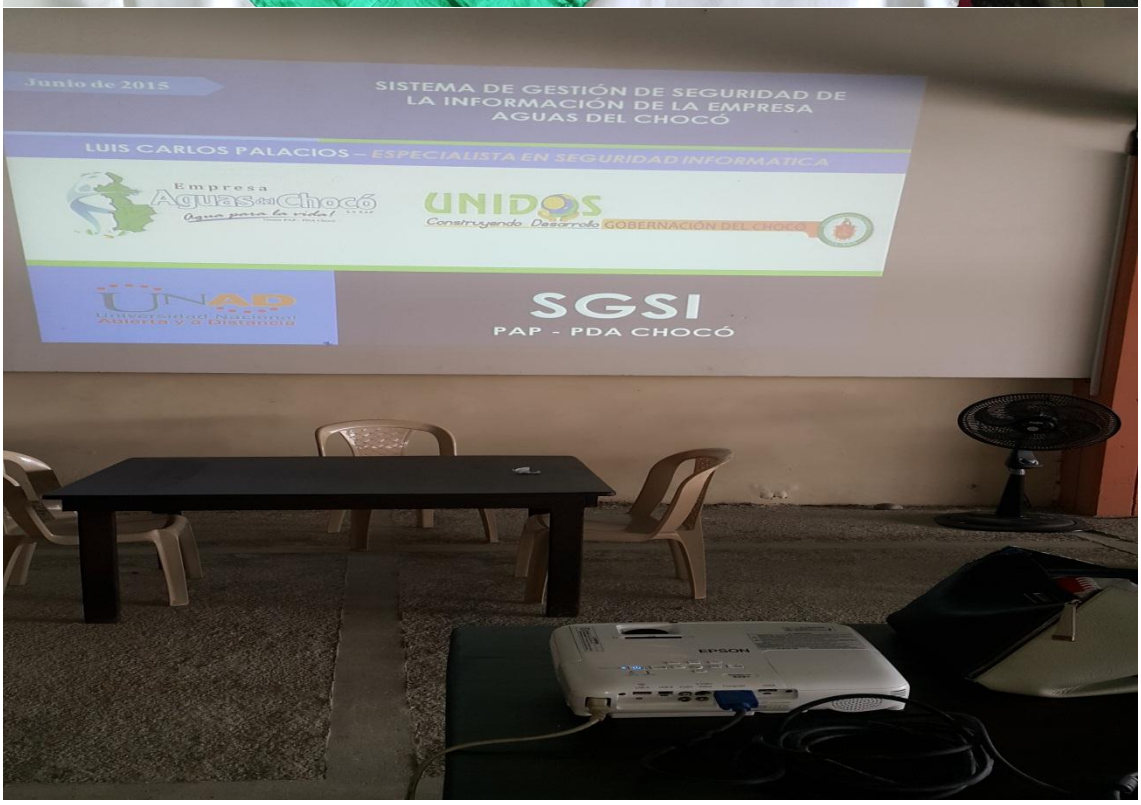
34	Software para Base de Datos	X			SI HAY	
35	Aplicaciones para Compartir Ficheros	X			ES BASICO PARA LAS LABORES	
36	Software DNS	X			EN EL SERVIDOR DNS	
37	Aplicaciones de Mensajería Instantánea			X	PENDIENTE INSTALAR PARA LA COMUNICACIÓN INTERNA	
38	Navegadores	X			VARIOS	
Análisis de vulnerabilidades de sistemas operativos						
39	Servicios de Windows	X			BIEN	
40	Internet Explorer	X			BIEN	
41	Versiones de Windows sin soporte			X	NO HAY WINDOWS XP	
42	Microsoft Office y Outlook Express	X			BIEN	
43	Debilidades de Configuración de Windows	X			NINGUNA	
Análisis de vulnerabilidades de Red						
44	Backup de software		X		MUY BASICO	
45	Backup de información			X	NO ESTÁ MUY BIEN PROTEJIDA	
46	Control de acceso a la red		X		TIENE VULNERABILIDAD	
Control de claves y privilegios de administración						
47	Análisis de correos		X		CON EL ANTIVIRUS	
48	Creación de Usuarios		X		VULNERABILIDAD EN CLAVES	
49	Clasificación de la información		X		TABLA DE RETENCION	
50	Clasificación de usuarios	X			SI EXISTE	
51	Nivel de seguridad de contraseñas			X	TIENE VULNERABILIDAD	
Política de Seguridad						
52	Documento de Política de Seguridad de la Información			X	FALTA CAPACITACION AL PERSONAL	

53	Revisión de la Política de Seguridad de la Información			X	FALTA ACTUALIZACION	
54	Documentación de Procesos Internos y externos		X		EN IMPLEMENTACION	

Anexo C Historial de modificaciones SGSI Aguas del Chocó

Fecha	Versión	Creado por	Descripción de la modificación
26/05/2015	0.1	Luis Carlos Palacios Mosquera	IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCO

Anexo D EVIDENCIAS SOCIALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCÓ.


Junio de 2015
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCÓ
LUIS CARLOS PALACIOS – ESPECIALISTA EN SEGURIDAD INFORMATICA
Empresa Aguas del Chocó
Agua para la vida!
UNIDOS
Construyendo Desarrollo
GOBERNACIÓN DEL CHOCÓ
UNAD
Universidad Nacional Abierta y a Distancia
SGSI
PAP - PDA CHOCÓ
EPSON


ACTIVOS INFORMÁTICOS Y ACTIVOS DE


Junio de 2015
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCÓ
LUIS CARLOS PALACIOS – ESPECIALISTA EN SEGURIDAD INFORMATICA
Empresa Aguas del Chocó
UNIDOS
Construyendo Desarrollo GOBERNACIÓN DEL CHOCÓ
UNAD
SGSI
PAP - PDA CHOCÓ
Brisas del Viralo


TAFORMA ESTRATÉGICA
Mayo de 2015

Anexo ELISTADO DE ASISTENCIA SOCIALIZACIÓN SGSI AGUAS DEL CHOCÓ

Empresa Aguas del Chocó S.A. E.S.P. — Agua para la vida!

SOCIALIZACIÓN DEL SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

FECHA	NOMBRE Y APELLIDOS	CEDULA	CARGO	TELEFONO	FIRMA
5/06/15	ANNY SANCHEZ	35894332	ASESORA TEC. ASEO	3216401174	ANNY SANCHEZ
5/06/15	Alba Nilsa Lopera Rojo	1037579815	Lider Plan Ambiental	3176822328	
5/06/15	Esther Guerrero	66942800	ASesora Te. Alc.	3147996420	
5/06/15	EDWAR ESTIVEN LEDESMA	72'020.406	COORDINADOR G.E	3218514369	
05/06/15	Jesus David Mosquera	1077.420.450	Apoyo Gestion S.	3144505707	
05/06/2015	Wilber yair Ruiz Ordoñez	11813986	Ing. de Apoyo.	311 608 4106	Wilber yair Ruiz O.
05/06/2015	Leonor Leyva de Cerdo	1.077443396	Apoyo A. Gestion S		
05/06/2015	Marelina Cuesta Borja	1038797832	Apoyo A Tecnico	3118597868	Marelina Cuesta B.
05/6	Zeelis Lopez	31289638	auxiliar de servicio	3128099249	
05-06/15	carla Palacios Quinto	1128280460	Auxiliar de servicio General	3136225848	Carla Palacios
05-06/15	Luis Angel Palacios Moya	1047441965?	Archivista	3143217937	
05-06-15	Javier Albert Cordoba Cano	12.029.130	Ing. Profesional Apoyo	3206380662	
05-6/15	Natanael Díaz Chaverra	11786792	Mensajero	3168933717	
05/6/15	[illegible]	87.383.794	[illegible]	3146957731	
05-6/15	Natanael Díaz Chaverra	11786792	Mensajero	3168933717	
05-6/15	Eduin A. Perlaza S.	11'790.497	Auxiliar Archivo	3053900870	
05-06/2015	Ruby Ariz Becerra	1074130373	Abogada	3135819173	

Empresa Aguas del Chocó E.S.P. — Agua para la vida!

SOCIALIZACIÓN DEL SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

FECHA	NOMBRE Y APELLIDOS	CEDULA	CARGO	TELEFONO	FIRMA
05/06/15	Mirley Cambod Buenaños	35899124	Trabajadora Social	3114111548	
05/06/15	YAIS DE FRANCISCO CORDOBA	1180993	P FILA 2	3117759020	
05/06/15	Blyderson Arboleda Montañez	1.128.420.991	Profesional en Procesos	3142732097	
05/06/15	Sonen Emilio Moreno Perea	82362996	Asesor Juridico Gestion Empresarial	3143106542	Sonen
05/06/15	Brigida Mena Romaña	35602621	Auxiliar Administrativo	3146536429	
05/06/15	Cristian Echeverry Cordoba	1077431375	Apoyo gestion empresarial	3145403993	
05/06/15	Luz Estella Becerra Hinestroza	52.020488	Profesional T.S.	3206157157	
05/06/15	Yosleidy Mesa Saavedra	1077457033	Recepcionista	3113030970	Yuneidy
11 11 11	Nancy Martinez Garcés	35'601.678	Mensajeria	3127603320	
	Soledad Becerra G.	35805296	Apoyo Area financiera	3113760458	
	Ruby Milena Diaz Rios	35-604.528	Secretaria Plan Ases	3126139452	
05/06/15	MARICARMEN SERNA PALACIOS	35891243	APOYO AREA JURIDICA	3207217202	
05/06/15	Yanila Cordoba Murillo	1077433748	Apoyo Area juridica	3148177543	
05/06/15	Alexander Cogollo Q.	79.908.705	Apoyo area juridica	3105938807	
05/06/15	Fabiola Valencia Córdoba	26.265.334	Apoyo a Contabilidad	3207440210	
05/06/15	William Palacios Moreno	80.237.352	Contador Publico.	3137946460	

Empresa Aguas del Chocó S.A. E.S.P. ¡Agua para la vida!

SOCIALIZACIÓN DEL SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

FECHA	NOMBRE Y APELLIDOS	CEDULA	CARGO	TELEFONO	FIRMA
05/05/15	Eduardo G. Arce Mona	79962411	Control Interno	3108210119	
" " "	Heiler David Bermudez Mosquera	11807943 Q.	conductor	3207650835	
05/06/15	Angela Maria Villamil O.	52950644	Secretaria	3118332132	
05/06/15	Leddy Urrutia Arboleda.	35.890.755Q	Apoy. As. Gerencia	3207906586	Leddy Urrutia.
05/06/15	Yolanda Palacios Palacios	35545613	Asesora tecnica A.	3136047904	
05/06/15	Jessica Leonor Mosquera Rentería	1077430837	Financiera	3217770005	
05/06/15	Ana Cecilia Lloreda Cq.	52098169.	Asesora Juridica	3212525769	
05/06/15	Juan E. Mena Rivas	11'806.336	Tesorero	3137466711	

Anexo F CERIFICACION DE IMPLANTACION SGSI AGUAS DEL CHOCÓ

EL SUSCRITO COORDINADOR ADMINISTRATIVO DE LA EMPRESA AGUAS DEL CHOCÓ S.A E.S.P. NIT 900.354.051-1

CERTIFICA QUE

El ingeniero de sistemas de la empresa Aguas del Chocó, **LUIS CARLOS PALACIOS MOSQUERA** identificada con cedula de ciudadanía número 11.812.448 de Quibdó, implantó el Sistema de Gestión de Seguridad de la Información (SGSI), cumpliendo a cabalidad con los protocolos de la empresa, finalizando con una capacitación el día 05 de junio de 2015, donde asistieron la mayoría de los empleados.

Se expide la presente certificación a los 10 días del mes de JUNIO de 2015.

HEILER PALACIOS CORDOBA
Coordinador Administrativo

Anexo G SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DEL CHOCÓ PUBLICADO

Para conservar los datos confidenciales se publicó en la página web de la empresa el PLAN DE CONTINUIDAD, documento que se puede descargar del siguiente link: http://aguasdelchoco.gov.co/images/SGSI/SGSI.pdf

Como se observa en la siguiente imagen en el menú vertical se dirige a la pestaña oficina virtual, luego en SGSI.

Disponible en: link: http://aguasdelchoco.gov.co/index.php/oficina-virtual/2015-06-10-23-22-14