REALIZAR UN ANÁLISIS DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN DEL PROCESO GESTIÓN DE CALIDAD Y SATISFACCIÓN AL USUARIO DE LA EMPRESA “ASMET SALUD EPS-S”

MAYERLY PLATA PEREZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2011

REALIZAR UN ANÁLISIS DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN DEL PROCESO GESTIÓN DE CALIDAD Y SATISFACCIÓN AL USUARIO DE LA EMPRESA "ASMET SALUD EPS-S"

MAYERLY PLATA PEREZ

Trabajo de grado presentado para optar al título de
Especialista en Telecomunicaciones

Director
Ing. Siler Amador Donado
Especialista en Redes y Servicios Telemáticos

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FISICOMECANICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2011

CONTENIDO

pág.

LISTA DE CUADROS

Pág.

GLOSARIO

ACTIVO: cualquier cosa que tiene valor para la organización. (ISO 27001 numeral 3.2).

AMENAZA: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 27002 numeral 2.16).

ANÁLISIS DEL RIESGO: uso sistemático de la información para identificar las fuentes y estimar el riesgo. (ISO 27001 numeral 3.3).

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO 27001 numeral 3.4).

CONTROL: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (ISO 27002 numeral 2.2).

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO 27001 numeral 3.6).

ESTIMACION DEL RIESGO: proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. (ISO 27005 numeral 3.5).

GESTIÓN DEL RIESGO: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. (ISO 27001 numeral 3.9).

IDENTIFICACION DEL RIESGO: proceso para encontrar, enumerar y caracterizar los elementos de riesgo. (ISO 27005 numeral 3.6).

IMPACTO: cambio adverso en el nivel de los objetivos del negocio logrados. (ISO 27005 numeral 3.1).

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (ISO 27001 numeral 3.10).

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO 27001 numeral 3.11).

RIESGO: Combinación de la probabilidad de un evento y sus consecuencias. (ISO 27002 numeral 2.9).

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*accountability*), no repudio y fiabilidad. (ISO 27001 numeral 3.13).

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. (ISO 27001 numeral 3.14).

VULNERABILIDAD: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas. (ISO 27002 numeral 2.17).

RESUMEN

TITULO: REALIZAR UN ANÁLISIS DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN DEL PROCESO GESTIÓN DE CALIDAD Y SATISFACCIÓN AL USUARIO DE LA EMPRESA "ASMET SALUD EPS-S"*

AUTOR: MAYERLY PLATA PEREZ**

PALABRAS CLAVES: Riesgo, análisis del riesgo, seguridad de la información

DESCRIPCION

La realización de un análisis del riesgo en la seguridad de la información del proceso gestión de calidad y satisfacción al usuario, le permite a Asmet Salud EPS-S identificar los activos de información tanto primarios como de soporte, las amenazas y las vulnerabilidades a las cuales están expuestos, así como revisar la eficacia de los controles que se encuentran implementados, permitiendo determinar escenarios de incidentes, los cuales se valoran de acuerdo a su probabilidad de ocurrencia e impacto en la organización.

La información de quejas y reclamos, satisfacción al usuario y soporte documental del proceso gestión de calidad y satisfacción al usuario, se constituye en un activo muy importante para la organización y es prioridad la preservación de la confidencialidad, integridad y disponibilidad, características fundamentales para mantener la imagen institucional, cumplir con las obligaciones legales y para la toma de decisiones que impacten en la calidad de los servicios prestados a los afiliados.

En este trabajo a través de una metodología cualitativa, se determina el nivel de riesgo para cada uno de los diferentes escenarios de incidentes identificados, clasificándolos como bajo, medio, alto y muy alto, haciendo énfasis en aquellos que presentan los niveles de riesgo más altos; igualmente se recomienda a la organización realizar el ejercicio de valoración de riesgos para todos los demás procesos, el cual incluye un proceso formal de identificación y clasificación de activos de información, un proceso para el registro de incidentes de seguridad donde se documente el análisis y la gestión realizada para los casos presentados, y finalmente determinar de acuerdo a sus prioridades un plan de tratamiento de riesgos.

* Trabajo de grado

** Facultad de ingenierías físicomecánicas. Escuela de ingenierías eléctrica, electrónica y de telecomunicaciones. Director: Ing. Siler Amador Donado.

ABSTRACT

TITLE: DO AN ANALYSIS OF DATA SECURITY RISK IN THE QUALITY MANAGEMENT PROCESS AND CLIENT SATISFACTION IN THE "ASMET SALUD EPS-S" COMPANY[*].*

AUTHOR: MAYERLY PLATA PEREZ[**]

KEY WORDS: Risk, Risk Analysis, Data Security.

DESCRIPTION

Doing an analysis of data security risk of the quality management process and client satisfaction, let Asmet Salud EPS-S identify active data active both primary and medium, threats and vulnerabilities to which they are exposed to, also check the efficacy in the controls implemented, letting determine sceneries of incidents which are valued according to their probability of frequency and impact in the organization.

Complaints data, client satisfaction and document medium of the quality management process and client satisfaction are constituted in a very important active for the organization and it is priority to preserve confidentiality, integrity and availability. These characteristics are fundamental to maintain the institutional image, fulfill legal duties and to make decisions that impact in the quality of services offer to the users.

In this Project through a qualitative method is determined the risk level for each of the different sceneries of incidents identified, classifying them as low, medium, highand very high, emphasizing those which present a higher risk level. Also, it is recommended to the organization to carry out the risk evaluation exercise for all the other processes which includes a formal process of identification and classification of data actives, a process to register security incidents in which it is documented the analysis and the management carried out for the cases presented. And finally, to determine according to their priorities a threat risk plan.

[*] Graduation Project

[**] Faculty of Physical-Mechanical Engineering. School of Electric, Electronic and Telecommunication Engineering. Director: Eng. Siler Amador Donado.

INTRODUCCION

Un análisis de riesgos sobre el proceso “gestión de calidad y satisfacción al usuario” le permitirá a Asmet Salud identificar y valorar los activos de información, las amenazas y vulnerabilidades a las que se encuentran expuestos, identificar los controles existentes y la eficacia de los mismos, y finalmente determinar las consecuencias potenciales para la información de quejas y reclamos, satisfacción al usuario (encuestas) y soporte documental.

Este análisis le permitirá a la organización tener una indicación general del nivel del riesgo y revelar los riesgos más importantes a los que se encuentra expuesta esta información.

La metodología que se emplea para realizar la valoración de los riesgos, es cualitativa, está permitirá tener un primer panorama de riesgos, y de acuerdo a las necesidades, si se considera pertinente se podrá realizar un análisis más específico de los riesgos importantes para la organización.

Este trabajo se convierte en una importante referencia para la empresa, que servirá como base para que el trabajo de identificación de riesgos se replique a otros procesos de la organización, con el fin de tener un panorama de riesgos a nivel general y definir el enfoque para la gestión del riesgo.

1. ESTABLECIMIENTO DEL CONTEXTO

1.1 EL ALCANCE Y LOS LÍMITES

Asmet Salud es una empresa promotora de salud, que administra y presta servicios a sus afiliados en el marco de la protección y bienestar social; para cumplir con este propósito ha definido una estructura de gestión por procesos, los cuales están orientados al cumplimiento de los objetivos estratégicos.

Como parte de la estructura de gestión por procesos, ha sido definido el proceso gestión de calidad y satisfacción del usuario, el cual cumple un rol y unas responsabilidades claramente definidas como son: la defensa de los derechos de los afiliados, partiendo de la escucha de la voz del cliente a través de la resolución de quejas y reclamos; mediciones de las satisfacción de los afiliados frente a los servicios recibidos en la red prestadora de servicios de salud y en las propias oficinas; y el manejo del sistema de gestión documental de la organización.

De acuerdo a lo anterior, la información de quejas y reclamos, satisfacción de los afiliados, y gestión documental, de la cual es responsable el proceso gestión de calidad y satisfacción al usuario, se convierte en un activo muy importante de la empresa y es prioridad la preservación de la confidencialidad, integridad y disponibilidad, características fundamentales para mantener la imagen institucional, cumplir con las obligaciones legales y para la toma de decisiones que impacten en la calidad de los servicios prestados a los afiliados.

1.1.1 Información de quejas y reclamos. Las quejas o reclamos, son un mecanismo reactivo del usuario que permite identificar dificultades con la prestación de servicios de salud y generar las acciones coyunturales, de seguimiento y preventivas que permitan resolver la situación.

- Las fuentes de información para la resolución de quejas y reclamos son las peticiones presentadas por los usuarios.
- Estas peticiones son registradas en el formato Registro de peticiones.
- Las peticiones se ingresan al aplicativo la Voz Del Usuario – VDU.
- El acceso al aplicativo se realiza a través de la página web ubicando el icono de acceso Quejas & Reclamos.

1.1.2 Información de encuestas. El objetivo que se persigue con la medición de la satisfacción de los afiliados, es escuchar la voz de los usuarios con relación a su percepción en cuanto a la oportunidad y calidad en la prestación de los servicios de salud y a la atención prestada en las propias oficinas, para lo cual se aplican encuestas impresas.

Las encuestas para medir la satisfacción se aplican a afiliados que reciben servicios ambulatorios, hospitalarios y medicamentos en las IPS, también se incluyen usuarios atendidos en las instalaciones de la empresa.

- Estas encuestas son registradas en los formatos de encuestas ambulatorias, hospitalarias y medicamentos.
- Las encuestas se ingresan al aplicativo Encuestas.
- El acceso al aplicativo se hace a través de la página web ubicando el icono de acceso sistema de encuestas.

1.1.3 Información del soporte documental. El sistema de gestión documental contiene toda la información relacionada con los procesos de la organización.

- La documentación almacenada corresponde a caracterizaciones, procedimientos, instructivos, manuales que describen la operación de la empresa.
- Esta información se soporta en el aplicativo Gestión documental.
- El acceso al aplicativo se hace a través de la página web ubicando el icono de acceso sistema de gestión documental.

1.2 OBJETIVO GENERAL

Realizar un análisis del riesgo en la seguridad de la información del proceso gestión de calidad y satisfacción

1.3 OBJETIVOS ESPECÍFICOS

- Identificar las amenazas y vulnerabilidades que afectan las bases de datos que contienen la información de quejas y reclamos, encuestas y gestión documental.

- Valorar los riesgos asociados a estas bases de datos.

1.4 REQUERIMIENTOS LEGALES

A continuación se presentan los requerimientos legales que aplican a la organización y que soportan la operación del proceso gestión de calidad y satisfacción del usuario:

Decreto 3556 del 16 de Septiembre de 2008. Por el cual se modifica el decreto 515 de 2004, "por el cual se define el sistema de habilitación de las entidades administradoras de régimen subsidiado, ARS (hoy entidades promotoras de salud del régimen subsidiado - EPS'S)".

Resolución 1445 del 8 de Mayo de 2006. “Por la cual se definen las funciones de la Entidad Acreditadora y se adoptan otras disposiciones”. Manuales de estándares del sistema único de acreditación.

Circular externa 049 del 2 de abril de 2008. Superintendencia nacional de salud. Asunto: modificación a las instrucciones generales y remisión de información para la inspección, vigilancia y control contenidas en la circular externa no. 047 (circular única).

ISO9001 Requisitos de la documentación. En un sistema de gestión de calidad, La documentación permite la comunicación del propósito y la coherencia de la acción. Su utilización contribuye a lograr la conformidad con los requisitos del cliente, a proveer la formación apropiada sobre el Sistema de Gestión de Calidad SGC, a hacer posible la repetibilidad y la trazabilidad, a proporcionar evidencias objetivas y a evaluar la eficacia y la adecuación continua del SGC. Puede estar en cualquier formato o tipo de soporte y su extensión depende de cada organización, según su tamaño, complejidad de los procesos e interacciones, competencia del personal.

1.6 NORMAS SEGURIDAD DE LA INFORMACION

Las normas de seguridad de la información que se consultaron para la realización de este trabajo son:

Instituto Colombiano de Normas Técnicas. NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información. Norma que brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

Instituto Colombiano de Normas Técnicas. NTC-ISO/IEC 27002 Código de práctica para la gestión de la seguridad de la información. Norma que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Instituto Colombiano de Normas Técnicas. NTC-ISO/IEC 27005 Gestión del Riesgo en la seguridad de la información. Norma que proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización.

Ley 1273 de Enero 5 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

2. ANÁLISIS DEL RIESGO

El análisis del riesgo es el uso sistemático de la información para identificar las fuentes y estimar el riesgo; éste se debe realizar en dos etapas, una de identificación y otra de estimación del riesgo, en cada una de ellas se deben desarrollar actividades tal y como se describe a continuación:

- Identificación del riesgo
  - Identificación de los activos
  - Identificación de las amenazas
  - Identificación de los controles existentes
  - Identificación de las vulnerabilidades
  - Identificación de las consecuencias

- Estimación del riesgo
  - Metodologías para la estimación del riesgo
  - Valoración de las consecuencias
  - Valoración de los incidentes
  - Nivel de estimación del riesgo

2.1 IDENTIFICACIÓN DEL RIESGO

2.1.1 Introducción a la identificación del riesgo. El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.

2.1.2 Identificación de los activos. Los activos de información son aquellos elementos que tienen valor para la organización, se pueden identificar dos clases de activos: primarios y de soporte.

De acuerdo a lo enunciado anteriormente, el proceso en el que se centrará el análisis del riesgo, es el proceso gestión de calidad y satisfacción al usuario, el cual responde por la información de quejas y reclamos, satisfacción al usuario y soporte documental de la organización, esta información se constituye en nuestros activos primarios:

Cuadro 1. Activos primarios

Activo	Clasificación	Nombre	Descripción
Activos primarios	Procesos y actividades del negocio	Proceso gestión de calidad y satisfacción al usuario	Proceso organizacional
	Información	Información de quejas y reclamos	Información de las peticiones presentadas por los usuarios.
		Información de satisfacción de usuarios	Información de la medición de satisfacción de los usuarios.
		Información del soporte documental	Información del sistema de gestión documental de la empresa.

Los activos de soporte, son aquellos de los cuales dependen los activos primarios, estos activos tienen vulnerabilidades que son explotables por las amenazas cuya meta es deteriorar los activos primarios; son de varios tipos: hardware, software, red, personal, sitio y organización.

La identificación de los activos de soporte fue realizada por personal de los procesos gestión tecnológica y gestión de calidad y satisfacción al usuario, a través de entrevistas, que permitieron analizar cómo se realiza el procesamiento de esta información en la organización, identificando los siguientes activos de soporte:

Cuadro 2. Activos de soporte

Activo	Clasificación	Nombre	Descripción
Hardware	Equipo de procesamiento de datos (activo)	Servidor Homero	Almacena las bases de quejas y reclamos, y encuestas.
		Servidor Xeon	Almacena la base de soporte documental, DNS interno secundario.
		Servidor Kanno	Servidor web, DNS externo secundario.
		Servidor Dino	DNS interno principal

Cuadro 2. Activos de soporte

Activo	Clasificación	Nombre	Descripción
		Servidor Janus	DNS externo principal
		Servidor Adonis	Firewall perimetral (iptables)
		Servidor Kaspersky	Antivirus instalado en equipos Windows
		Servidor Morfeo	Servidor de copias de seguridad
		Servidor Xamundi	Servidor de copias alternas en oficina valle
		Computador de escritorio	Equipos de escritorio usados por los usuarios del sistema de información.
	Medios para datos (pasivo)	Discos duros externos	Discos usados para almacenamiento de copias de seguridad.
Software	Sistema operativo	Linux	Linux Centos 5.5 sistema operativo para servidores
		Windows	Windows XP Profesional, Windows Vista, Windows Seven sistema operativo para computadores de escritorio
	Paquetes de software o software estándar	Firebird	Sistema de Gestión de Base de Datos
		Iptables	Reglas para el firewall
		Kaspersky antivirus	Software que protege contra virus y programas espía.
		Crontab	Software para la realización de copias de seguridad de las bases de datos a través de scripts
		Apache (php-firebird)	Servidor de aplicaciones con librerías de php y firebird
		Bind	Software de gestión DNS
		Suite de oficina	Suite de oficina que incluye herramientas como procesador de texto, hoja de cálculo, presentaciones.
	Aplicaciones del negocio	Encuestas	Aplicación que permite tabular las encuestas destinadas a la medición de la satisfacción de los usuarios y consultar sus correspondientes resultados.
		VDU – La Voz Del Usuario	Aplicación que permite radicar quejas/reclamos, sugerencias y apreciaciones positivas, así como registrar el trámite correspondiente.
		Gestión documental	Aplicación que permite realizar el control sobre todo el soporte documental, permite la creación, eliminación de los documentos y el manejo de los mismos por versiones.
Red	Medios y soportes	Redes de área local	Redes ethernet en las oficinas departamentales y sede nacional.
		Canales WAN	Canales con capacidad 1, 2, 4 y 8 MB a través del cual se interconectan las sedes departamentales con la

Cuadro 2. Activos de soporte

Activo	Clasificación	Nombre	Descripción
			ciudad de Popayán.
		Canal de internet (dedicado y banda ancha)	Conexión oficinas municipales 2048 Kbps. Permite el acceso al servidor web con todos sus aplicativos.
	Transmisión pasiva o activa	Switch	Switch de borde al cual se conectan los usuarios.
		Router ISIS	Switch CISCO Core, administra las subredes internas en la sede nacional y la conectividad con las sedes departamentales.
		Acces Point	Estos dispositivos se encuentran en las diferentes sedes, nos permiten la interconexión de clientes inalámbricos, usuarios internos y proveedores.
Personal	Persona a cargo de la toma de decisiones	Gerente de Calidad	Responsable del proceso gestión de calidad y satisfacción del usuario.
	Usuarios	Profesional de Servicio al Afiliado	Persona que accede al sistema de información para realizar sus labores diarias.
		Auxiliar de Monitoreo y Satisfacción	Persona que accede al sistema de información para realizar sus labores diarias.
		Gestor Local	Persona que accede al sistema de información para realizar sus labores diarias.
		Técnico Gestión de Calidad	Persona que administra los aplicativos a nivel nacional.
	Personal de operación / mantenimiento	Profesional Administrador de Servidores	Persona responsable del óptimo funcionamiento de los servidores.
		Profesional Administrador de Red	Persona responsable del optimo funcionamiento de las redes de cableado estructurado y la conectividad entre ellas.
		Profesional seguridad de la información	Persona responsable de la seguridad de la Información.
		Técnico de Sistemas	Persona responsable de la realización y manejo de copias de seguridad.
	Desarrolladores	Vector Naranja	Empresa encargada del desarrollo y mantenimiento de las aplicaciones específicas del negocio: encuestas, voz del usuario y gestión documental.
Sitio	Ubicación	Centro de procesamiento de datos	Se encuentra ubicado en el tercer piso de las instalaciones donde funciona la empresa.
	Servicios	Acondicionadore	Sistema de refrigeración ubicado en el centro de

Cuadro 2. Activos de soporte

Activo	Clasificación	Nombre	Descripción
	esenciales	s de aire	procesamiento de datos.
		Fuentes de suministro e instalaciones eléctricas	Se cuenta con suministro de energía por parte de la empresa CEO, sistema de UPS y planta eléctrica automática.
Organizac ión	Estructura de la organizació n	Procedimientos organizacionales	Procedimientos establecidos por la organización

2.1.3 Identificación de las amenazas. Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural (ambiental) o humano y podrían ser accidentales o deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización.

Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación se presenta la lista de amenazas a las que están expuestos los activos que soportan la información de quejas y reclamos, satisfacción al usuario y soporte documental, ésta se ha obtenido con la información suministrada por los usuarios, el profesional responsable de los servidores y se ha usado el catalogo de amenazas que trae como guía la norma ISO 27005.

Cuadro 3. Listado de amenazas

Tipo	Amenaza	Origen		
		Accide ntal	Deliber ada	Ambie ntal
Daño físico	Fuego	A	D	
	Daño por agua	A		E
	Accidente importante	A	D	
	Destrucción del equipo o los medios	A	D	E
	Polvo, corrosión, congelamiento	A		

Cuadro 3. Listado de amenazas

Tipo	Amenaza	Origen		
		Accidental	Deliberada	Ambiental
Eventos naturales	Fenómenos meteorológicos			E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A	D	
	Pérdida de suministro de energía	A	D	E
	Falla en el equipo de telecomunicaciones	A	D	
Compromiso de la información	Espionaje remoto		D	
	Escucha encubierta		D	
	Hurto de medios o documentos		D	
	Hurto de equipo		D	
	Manipulación con software	A	D	
Fallas técnicas	Falla del equipo	A		
	Saturación del sistema de información	A	D	
	Mal funcionamiento del software	A		
	Incumplimiento en el mantenimiento del sistema de información	A	D	
Compromiso de las funciones	Error en el uso	A	D	
	Abuso de derechos	A	D	
	Incumplimiento en la disponibilidad del personal	A	D	E

2.1.4 Identificación de los controles existentes. Un control es un medio para gestionar el riesgo, puede incluir políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Es importante identificar los controles planeados o implementados en la organización, así como su correcto funcionamiento, si este no funciona como se espera, puede causar vulnerabilidades.

La organización ha definido una serie de políticas de seguridad, que tienen por objetivo la protección de la información, éstas se encuentran documentadas y han sido socializadas con todo el personal.

Con base en estas políticas documentadas, la organización ha realizado auditorías internas en el año inmediatamente anterior, con el objetivo de verificar el funcionamiento de estos controles, revisando esta información y con los datos suministrados por el personal de gestión tecnológica, se puede determinar el nivel de funcionamiento de los controles implementados.

La valoración de la eficacia de los controles implementados se realizó con la siguiente escala:

Cuadro 4. Criterios para evaluar controles

Valor	Criterio
5	Control que funciona correctamente
3	Control que falla en su funcionamiento
1	Control que no funciona

Cuadro 5. Listado de controles existentes

Activos	Controles	Eficacia
Hardware	Mantenimiento de los equipos, cumplimiento del cronograma de mantenimiento	3
	Control para el ingreso y salida de equipos, este se realiza a través del diligenciamiento de un formato y bajo la revisión de los guardas de seguridad.	5
	Almacenamiento en caja fuerte de los discos duros con copias de seguridad	5
Software	Controles contra códigos maliciosos	5
	Copias de seguridad para bases de datos, archivos de gestión de los usuarios, archivos de configuración de servidores y aplicativos, así mismo se cuenta con un sitio alterno para almacenamiento de estas copias.	5
	Procedimiento para el registro y cancelación de usuarios que acceden al sistema de información	3
	Control de vulnerabilidades técnicas de los aplicativos del negocio	1

Cuadro 5. Listado de controles existentes

Activos	Controles	Eficacia
Red	Control de enrutamiento en la red	5
Personal	Inclusión de obligaciones de cada uno de los empleados en términos de seguridad de la información en el reglamento interno de trabajo.	5
	Consideraciones de la seguridad en los acuerdos con terceras partes	3
	Educación, formación y concientización sobre la seguridad del personal	3
Sitio	Definición de un plan de contingencia y continuidad	3
	Controles de acceso físico (tarjetas y huella digital) al centro de procesamiento de datos.	5
	Protección contra amenazas externas como vigilancia 24 horas, cámaras de seguridad.	5
	Detectores de humo, alarma contra incendios, brigada de emergencia.	5
	Revisión periódica de filtración de agua en las instalaciones	3
	Sistema de refrigeración de centro de procesamiento de datos	3
	Equipos protegidos contra fallas en el suministro de energía, uso de UPS y planta eléctrica.	5
Organización	Política de seguridad documentada y socializada	3

2.1.5 Identificación de las vulnerabilidades. Se deberían identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o la organización.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla y una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo.

Para la identificación de las vulnerabilidades se usó como guía el listado de la norma ISO 27005, se entrevistó a usuarios y personal del proceso de gestión tecnológica; y se revisó un informe de análisis de vulnerabilidades realizado sobre los aplicativos web encuestas, vdu y gestión documental.

Cuadro 6. Listado de vulnerabilidades

Activo	Vulnerabilidades
Hardware	Almacenamiento sin protección
	Susceptibilidad a la humedad, el polvo y la suciedad
	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento
	Almacenamiento sin protección
	Copia no controlada
Software	Fechas incorrectas
	Configuración incorrecta de parámetros
	Fallas en el funcionamiento del antivirus
	Defectos bien conocidos en el software
	Ausencia de copias de respaldo
	Ausencia de pistas de auditoría
Red	Tráfico sensible sin protección
	Arquitectura insegura de la red
	Conexión deficiente de los cables
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
	Configuración incorrecta de parámetros
	Configuración incorrecta de parámetros
Personal	Ausencia del personal
	Uso incorrecto de software y hardware
	Entrenamiento insuficiente en seguridad
Sitio	Ausencia de protección física de la edificación, puertas y ventanas
	Filtración de agua en instalaciones
	Instalaciones eléctricas provisionales
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Susceptibilidad a las variaciones de temperatura
	Red energética inestable
Organización	Ausencia de planes de continuidad
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
	Ausencia de procedimientos sobre seguridad de la información

Cuadro 6. Listado de vulnerabilidades

Activo	Vulnerabilidades
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes

2.1.6 Identificación de las consecuencias. De acuerdo al enfoque organizacional, las consecuencias que pueden ser causadas por un escenario de incidente (una amenaza que explota una vulnerabilidad), corresponden a:

- Incumplimiento de la normatividad vigente.
- Pérdida de credibilidad en el sistema de información interno.
- Alteración de la operación interna
- Daño en la reputación.

2.2 ESTIMACIÓN DEL RIESGO

El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron a la organización.

La empresa, en el marco de su sistema integral de control, ha realizado una identificación y valoración cualitativa de los riesgos asociados a los procesos que impactaban en el cumplimiento de los objetivos organizacionales.

Por tal motivo, se cree conveniente para este primer momento, continuar con una metodología de estimación cualitativa que permita ser consistentes con el enfoque que la organización utiliza para el proceso de valoración de riesgos.

Esta valoración tiene como objetivo determinar un primer panorama de riesgos e identificar para cuales activos se encuentran las valoraciones más altas, sin embargo, es importante mencionar que, si la organización lo considera conveniente puede realizar

posteriormente un análisis de tipo cuantitativo que dé un nivel más profundo de detalle frente a los riesgos encontrados.

La estimación cualitativa utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales y la probabilidad de que ocurran dichas consecuencias.

2.2.1 Valoración de las consecuencias. Para la valoración de las consecuencias se debe tener en cuenta los valores asignados a los activos identificados.

El valor del impacto del negocio se va a expresar de manera cuantitativa y el valor de los activos identificados estará determinado por:

- El valor de reemplazo del activo.

- Las consecuencias adversas para la empresa como son: incumplimiento de la normatividad vigente, pérdida de credibilidad en el sistema de información interno, alteración de la operación interna y/o daño en la reputación; por la pérdida de la confidencialidad, integridad y disponibilidad de la información, y otros activos de información.

El valor, determinado por las consecuencias adversas para la empresa, es en general significativamente superior al simple costo del reemplazo.

Las consecuencias para la organización se expresarán con base en los siguientes criterios:

Cuadro 7. Criterios para evaluar las consecuencias

Valor	Criterio
5	• Probablemente cause un incumplimiento muy grave de alguna norma vigente. • Probablemente afecte gravemente la credibilidad en el sistema de información interno. • Probablemente cause un serio impacto en la operación interna de la organización.

Cuadro 7. Criterios para evaluar las consecuencias

Valor	Criterio
	• Probablemente cause un daño muy grave a la reputación de la organización.
3	• Probablemente cause un incumplimiento grave de alguna norma vigente. • Probablemente afecte en forma significativa la credibilidad en el sistema de información interno. • Probablemente cause impacto significativo en la operación interna de la organización. • Probablemente cause un daño grave a la reputación de la organización.
1	• Probablemente cause un incumplimiento leve de alguna norma vigente. • Probablemente afecte en forma leve la credibilidad en el sistema de información interno. • Probablemente cause un impacto leve en la operación interna de la organización. • Probablemente cause un daño menor a la reputación de la organización.

El valor de los activos se calculará sumando los siguientes valores = valor del reemplazo, consecuencias por la pérdida de confidencialidad, consecuencias por la pérdida de integridad, consecuencias por la pérdida de disponibilidad, los resultados se asociarán a la siguiente escala:

Cuadro 8. Criterios para asociar el valor de un activo a una escala

Valor	Criterio
Muy alto	Valor del riesgo >16
Alto	Valor del riesgo >12 y <=16
Medio	Valor del riesgo >8 y <=12
Bajo	Valor del riesgo <=8

A continuación se presenta la valoración realizada de los activos identificados, con base en los criterios anteriormente definidos:

Cuadro 9. Listado de activos valorados

Activo	Nombre	($)	C	I	D	Total	Valor
Activos primarios	Información de quejas y reclamos	5	1	5	5	16	Alto
	Información de satisfacción de usuarios	5	1	5	5	16	Alto
	Información del soporte documental	5	5	5	5	20	Muy alto
Hardware	Servidor Homero	3	1	3	3	10	Medio
	Servidor Xeon	1	5	3	3	12	Medio
	Servidor Kanno	5	3	3	3	14	Alto
	Servidor Dino	1	1	3	3	8	Bajo
	Servidor Janus	1	1	3	3	8	Bajo
	Servidor Adonis	1	5	5	3	14	Alto
	Servidor Kaspersky	1	1	1	1	4	Bajo
	Servidor Morfeo	3	5	3	3	14	Alto
	Servidor Xamundi	3	5	3	1	12	Medio
	Computador de escritorio	1	1	1	1	4	Bajo
	Discos duros externos	1	5	5	5	16	Alto
Software	Linux	3	1	5	5	14	Alto
	Windows	1	1	1	1	4	Bajo
	Firebird	3	1	5	5	14	Alto
	Iptables	1	1	1	1	4	Bajo
	Kaspersky antivirus	1	1	1	1	4	Bajo
	Crontab	3	1	5	5	14	Alto
	Apache (php-firebird)	3	1	5	5	14	Alto
	Bind	1	1	3	1	6	Bajo
	Suite de oficina	1	1	3	1	6	Bajo
	Encuestas	3	1	5	5	14	Alto
	VDU – La Voz Del Usuario	3	1	5	5	14	Alto
	Gestión documental	3	5	5	5	18	Muy alto
Red	Redes de área local	5	3	3	3	14	Alto
	Canales WAN	5	3	3	3	14	Alto
	Canal de internet (dedicado y banda ancha)	5	3	3	3	14	Alto
	Switch	3	3	3	3	12	Medio
	Router ISIS	5	3	5	5	18	Muy alto
	Acces Point	1	3	1	1	6	Bajo
Personal	Gerente de Calidad	5	3	1	1	10	Medio
	Profesional de Servicio al Afiliado	5	1	1	1	8	Bajo
	Auxiliar de Monitoreo y Satisfacción	5	1	1	5	12	Medio
	Gestor Local	5	1	1	5	12	Medio
	Técnico Gestión de Calidad	5	5	1	5	16	Alto
	Profesional Administrador de Servidores	3	5	1	3	12	Medio
	Profesional Administrador de Red	3	1	1	3	8	Bajo
	Profesional seguridad de la información	3	1	1	1	6	Bajo
	Técnico de Sistemas	3	5	1	3	12	Medio
	Vector Naranja	5	5	1	3	14	Alto

Cuadro 9. Listado de activos valorados

Activo	Nombre	($)	C	I	D	Total	Valor
Sitio	Centro de procesamiento de datos	3	3	3	3	12	Medio
	Acondicionadores de aire	3	1	1	5	10	Medio
	Fuentes de suministro e instalaciones eléctricas	5	1	1	5	12	Medio
Organización	Procedimientos organizacionales	3	1	1	3	8	Bajo

2.2.2 Valoración de los incidentes. Después de identificar los escenarios de incidentes, es necesario evaluar la probabilidad (P) de cada escenario y el impacto (I) de que ocurra.

Para esta valoración, se tomaron en consideración los siguientes aspectos:

- La experiencia del personal de gestión tecnológica, quienes tienen conocimiento acerca de incidentes de seguridad ocurridos.
- La percepción de atracción y vulnerabilidad de los activos estudiados.
- Factores de riesgo identificados en el quehacer diario.
- Eficacia de los controles implementados.

La valoración del impacto y la probabilidad se realizó mediante las siguientes escalas.

Cuadro 10. Criterios para valorar el impacto

Valor	Criterio
5	• Si el escenario de incidente se presentara, probablemente cause un incumplimiento muy grave de alguna norma vigente. • Si el escenario de incidente se presentara, probablemente afecte gravemente la credibilidad en el sistema de información interno. • Si el escenario de incidente se presentara, probablemente cause un serio impacto en la operación interna de la organización. • Si el escenario de incidente se presentara, probablemente cause un daño muy grave a la reputación de la organización.
3	• Si el escenario de incidente se presentara, probablemente cause un incumplimiento grave de alguna norma vigente. • Si el escenario de incidente se presentara, probablemente afecte en forma significativa la credibilidad en el sistema de información interno. • Si el escenario de incidente se presentara, probablemente cause impacto significativo en la operación interna de la organización.

Cuadro 10. Criterios para valorar el impacto

Valor	Criterio
	• Si el escenario de incidente se presentara, probablemente cause un daño grave a la reputación de la organización.
1	• Si el escenario de incidente se presentara, probablemente cause un incumplimiento leve de alguna norma vigente. • Si el escenario de incidente se presentara, probablemente afecte en forma leve la credibilidad en el sistema de información interno. • Si el escenario de incidente se presentara, probablemente cause un impacto leve en la operación interna de la organización. • Si el escenario de incidente se presentara, probablemente cause un daño menor a la reputación de la organización.

Cuadro 11. Criterios para valorar la probabilidad

Valor	Criterio
5	Es muy factible que el escenario de incidente se presente.
3	Es factible que el escenario de incidente se presente.
1	Es poco factible que el escenario de incidente se presente.

Cuadro 12. Valoración de impacto y probabilidad

Activo	Amenazas	Controles	Vulnerabilidades	I	P
Hardware	Hurto de equipo	Control para el ingreso y salida de equipos, este se realiza a través del diligenciamiento de un formato y bajo la revisión de los guardas de seguridad.	Almacenamiento sin protección	5	1
	Polvo, corrosión, congelamiento		Susceptibilidad a la humedad, el polvo y la suciedad	5	3
	Incumplimiento en el mantenimiento del sistema de información	Mantenimiento de los equipos, cumplimiento del cronograma de mantenimiento	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3

Cuadro 12. Valoración de impacto y probabilidad

Activo	Amenazas	Controles	Vulnerabilidades	I	P
	Destrucción del equipo o los medios	Almacenamiento en caja fuerte de los discos duros con copias de seguridad	Almacenamiento sin protección	5	1
	Hurto de medios o documentos		Copia no controlada	5	5
Software	Error en el uso		Fechas incorrectas	3	5
	Mal funcionamiento del software	Copias de seguridad para bases de datos, archivos de gestión de los usuarios, archivos de configuración de servidores y aplicativos, así mismo se cuenta con un sitio alterno para almacenamiento de estas copias.	Configuración incorrecta de parámetros	1	5
	Manipulación con software	Controles contra códigos maliciosos	Fallas en el funcionamiento del antivirus	5	1
	Manipulación con software	Control de vulnerabilidades técnicas de los aplicativos del negocio	Defectos bien conocidos en el software	5	5
	Mal funcionamiento del software	Copias de seguridad para bases de datos, archivos de gestión de los usuarios, archivos de configuración de servidores y aplicativos, así mismo se cuenta con un sitio alterno para almacenamiento de estas copias.	Ausencia de copias de respaldo	5	1
	Abuso de derechos		Ausencia de pistas de auditoría	5	5
Red	Escucha encubierta		Tráfico sensible sin protección	3	5
	Espionaje remoto		Arquitectura insegura de la red	3	5
	Falla en el equipo de telecomunicaciones		Conexión deficiente de los cables	5	5

Cuadro 12. Valoración de impacto y probabilidad

Activo	Amenazas	Controles	Vulnerabilidades	I	P
	Saturación del sistema de información	Control de enrutamiento en la red	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	5	1
Personal	Incumplimiento en la disponibilidad del personal		Ausencia del personal	5	5
	Error en el uso		Uso incorrecto de software y hardware	5	5
	Error en el uso	Educación, formación y concientización sobre la seguridad del personal	Entrenamiento insuficiente en seguridad	3	3
Sitio	Destrucción del equipo o los medios	Controles de acceso físico (tarjetas y huella digital) al centro de procesamiento de datos.	Ausencia de protección física de la edificación, puertas y ventanas	5	1
	Daño por agua	Revisión periódica de filtración de agua en las instalaciones	Filtración de agua en instalaciones	5	3
	Fuego	Detectores de humo, alarma contra incendios, brigada de emergencia.	Instalaciones eléctricas provisionales	5	3
	Accidente importante	Protección contra amenazas externas como vigilancia 24 horas, cámaras de seguridad.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	5	1
	Falla en el sistema de suministro de agua o de aire acondicionado	Sistema de refrigeración de centro de procesamiento de datos	Susceptibilidad a las variaciones de temperatura	5	3
	Pérdida de suministro de energía	Equipos protegidos contra fallas en el suministro de energía, uso de UPS y planta eléctrica.	Red energética inestable	5	1
Organización	Destrucción del equipo o los medios	Definición de un plan de contingencia y continuidad	Ausencia de planes de continuidad	3	1
	Hurto de medios o documentos	Inclusión de obligaciones de cada uno de los	Ausencia de procesos disciplinarios definidos en el	3	3

Cuadro 12. Valoración de impacto y probabilidad

Activo	Amenazas	Controles	Vulnerabilidades	I	P
		empleados en términos de seguridad de la información en el reglamento interno de trabajo.	caso de incidentes de seguridad de la información		
	Abuso de derechos		Ausencia de procedimientos de identificación y valoración de riesgos	5	5
	Abuso de derechos		Ausencia de reportes de fallas en los registros de administradores y operadores	5	5
	Abuso de derechos	Procedimiento para el registro y cancelación de usuarios que acceden al sistema de información	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	1	3
	Error en el uso	Política de seguridad documentada y socializada	Ausencia de procedimientos sobre seguridad de la información	5	3
	Abuso de derechos	Consideraciones de la seguridad en los acuerdos con terceras partes	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	5	3

2.2.3 Nivel de estimación del riesgo. La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias.

El valor del riesgo se calculará multiplicado los siguientes valores = valor del activo * valor del impacto * valor de la probabilidad, y los resultados se asociarán a la siguiente escala:

Cuadro 13. Criterios para asociar el valor del riesgo a una escala

Valor	Criterio
Muy alto	Valor del riesgo >350
Alto	Valor del riesgo >200 y <=350
Medio	Valor del riesgo >100 y <=200
Bajo	Valor del riesgo <=100

A continuación se estima el nivel de riesgo para todos los escenarios de incidente identificados.

Cuadro 14. Listado de activos con su nivel de riesgo

Activo	Nombre	Valor	Amenazas	Vulnerabilidades	I	P	Valor	Riesgo
Hard ware	Servidor Homero	10	Hurto de equipo	Almacenamiento sin protección	5	1	50	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	150	Medio
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	150	Medio
	Servidor Xeon	12	Hurto de equipo	Almacenamiento sin protección	5	1	60	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	180	Medio
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	180	Medio
	Servidor Kanno	14	Hurto de equipo	Almacenamiento sin protección	5	1	70	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	210	Alto
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	210	Alto
	Servidor Dino	8	Hurto de equipo	Almacenamiento sin protección	5	1	40	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	120	Medio

Cuadro 14. Listado de activos con su nivel de riesgo

Activo	Nombre	Valor	Amenazas	Vulnerabilidades	I	P	Valor	Riesgo
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	120	Medio
	Servidor Janus	8	Hurto de equipo	Almacenamiento sin protección	5	1	40	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	120	Medio
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	120	Medio
	Servidor Adonis	14	Hurto de equipo	Almacenamiento sin protección	5	1	70	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	210	Alto
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	210	Alto
	Servidor Kaspersky	4	Hurto de equipo	Almacenamiento sin protección	5	1	20	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	60	Bajo
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	60	Bajo
	Servidor Morfeo	14	Hurto de equipo	Almacenamiento sin protección	5	1	70	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	210	Alto
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	210	Alto
	Servidor Xamundi	12	Hurto de equipo	Almacenamiento sin protección	5	1	60	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	180	Medio
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	180	Medio

Cuadro 14. Listado de activos con su nivel de riesgo

Activo	Nombre	Valor	Amenazas	Vulnerabilidades	I	P	Valor	Riesgo
	Computador de escritorio	4	Hurto de equipo	Almacenamiento sin protección	5	1	20	Bajo
			Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad	5	3	60	Bajo
			Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento	5	3	60	Bajo
	Discos duros externos	16	Destrucción del equipo o los medios	Almacenamiento sin protección	5	1	80	Bajo
			Hurto de medios o documentos	Copia no controlada	5	5	400	Muy alto
Softw are	Linux	14	Error en el uso	Fechas incorrectas	3	5	210	Alto
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	70	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	70	Bajo
	Windows	4	Error en el uso	Fechas incorrectas	3	5	60	Bajo
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	20	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	20	Bajo
	Firebird	14	Error en el uso	Fechas incorrectas	3	5	210	Alto
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	70	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	70	Bajo
	Iptables	4	Error en el uso	Fechas incorrectas	3	5	60	Bajo
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	20	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	20	Bajo
	Kaspersky antivirus	4	Error en el uso	Fechas incorrectas	3	5	60	Bajo
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	20	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	20	Bajo
	Crontab	14	Error en el uso	Fechas incorrectas	3	5	210	Alto
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	70	Bajo

Cuadro 14. Listado de activos con su nivel de riesgo

Activo	Nombre	Valor	Amenazas	Vulnerabilidades	I	P	Valor	Riesgo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	70	Bajo
	Apache (php-firebird)	14	Error en el uso	Fechas incorrectas	3	5	210	Alto
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	70	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	70	Bajo
	Bind	6	Error en el uso	Fechas incorrectas	3	5	90	Bajo
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	30	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	30	Bajo
	Suite de oficina	6	Error en el uso	Fechas incorrectas	3	5	90	Bajo
			Mal funcionamiento del software	Configuración incorrecta de parámetros	1	5	30	Bajo
			Manipulación con software	Fallas en el funcionamiento del antivirus	5	1	30	Bajo
	Encuestas	14	Manipulación con software	Defectos bien conocidos en el software	5	5	350	Alto
			Mal funcionamiento del software	Ausencia de copias de respaldo	5	1	70	Bajo
			Abuso de derechos	Ausencia de pistas de auditoría	5	5	350	Alto
	VDU – La Voz Del Usuario	14	Manipulación con software	Defectos bien conocidos en el software	5	5	350	Alto
			Mal funcionamiento del software	Ausencia de copias de respaldo	5	1	70	Bajo
			Abuso de derechos	Ausencia de pistas de auditoría	5	5	350	Alto
	Gestión documental	18	Manipulación con software	Defectos bien conocidos en el software	5	5	450	Muy alto
			Mal funcionamiento del software	Ausencia de copias de respaldo	5	1	90	Bajo
			Abuso de derechos	Ausencia de pistas de auditoría	5	5	450	Muy alto
Red	Redes de área local	14	Escucha encubierta	Tráfico sensible sin protección	3	5	210	Alto
	Canales WAN	14	Espionaje remoto	Arquitectura insegura de la red	3	5	210	Alto

Cuadro 14. Listado de activos con su nivel de riesgo

Activo	Nombre	Valor	Amenazas	Vulnerabilidades	I	P	Valor	Riesgo
	Canal de internet (dedicado y banda ancha)	14	Falla en el equipo de telecomunicaciones	Conexión deficiente de los cables	5	5	350	Alto
	Switch	12	Saturación del sistema de información	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	5	1	60	Bajo
	Router ISIS	18	Falla del equipo	Configuración incorrecta de parámetros	5	1	90	Bajo
	Acces Point	6	Falla del equipo	Configuración incorrecta de parámetros	1	5	30	Bajo
Personal	Gerente de Calidad	10	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	250	Alto
			Error en el uso	Uso incorrecto de software y hardware	5	5	250	Alto
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	90	Bajo
	Profesional de Servicio al Afiliado	8	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	200	Medio
			Error en el uso	Uso incorrecto de software y hardware	5	5	200	Medio
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	72	Bajo
	Auxiliar de Monitoreo y Satisfacción	12	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	300	Alto
			Error en el uso	Uso incorrecto de software y hardware	5	5	300	Alto
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	108	Medio
	Gestor Local	12	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	300	Alto
			Error en el uso	Uso incorrecto de software y hardware	5	5	300	Alto
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	108	Medio
	Técnico Gestión de Calidad	16	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	400	Muy alto
			Error en el uso	Uso incorrecto de software y hardware	5	5	400	Muy alto
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	144	Medio

Cuadro 14. Listado de activos con su nivel de riesgo

Activo	Nombre	Valor	Amenazas	Vulnerabilidades	I	P	Valor	Riesgo
	Profesional Administrador de Servidores	12	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	300	Alto
			Error en el uso	Uso incorrecto de software y hardware	5	5	300	Alto
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	108	Medio
	Profesional Administrador de Red	8	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	200	Medio
			Error en el uso	Uso incorrecto de software y hardware	5	5	200	Medio
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	72	Bajo
	Profesional seguridad de la información	6	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	150	Medio
			Error en el uso	Uso incorrecto de software y hardware	5	5	150	Medio
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	54	Bajo
	Técnico de Sistemas	12	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	300	Alto
			Error en el uso	Uso incorrecto de software y hardware	5	5	300	Alto
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	108	Medio
	Vector Naranja	14	Incumplimiento en la disponibilidad del personal	Ausencia del personal	5	5	350	Alto
			Error en el uso	Uso incorrecto de software y hardware	5	5	350	Alto
			Error en el uso	Entrenamiento insuficiente en seguridad	3	3	126	Medio
Sitio	Centro de procesamiento de datos	12	Destrucción del equipo o los medios	Ausencia de protección física de la edificación, puertas y ventanas	5	1	60	Bajo
			Daño por agua	Filtración de agua en instalaciones	5	3	180	Medio
			Fuego	Instalaciones eléctricas provisionales	5	3	180	Medio
			Accidente importante	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	5	1	60	Bajo

Cuadro 14. Listado de activos con su nivel de riesgo

Activo	Nombre	Valor	Amenazas	Vulnerabilidades	I	P	Valor	Riesgo
	Acondicionadores de aire	10	Falla en el sistema de suministro de agua o de aire acondicionado	Susceptibilidad a las variaciones de temperatura	5	3	150	Medio
	Fuentes de suministro e instalaciones eléctricas	12	Pérdida de suministro de energía	Red energética inestable	5	1	60	Bajo
Organización	Procedimientos organizacionales	8	Destrucción del equipo o los medios	Ausencia de planes de continuidad	3	1	24	Bajo
			Hurto de medios o documentos	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	3	3	72	Bajo
			Abuso de derechos	Ausencia de procedimientos de identificación y valoración de riesgos	5	5	200	Medio
			Abuso de derechos	Ausencia de reportes de fallas en los registros de administradores y operadores	5	5	200	Medio
			Abuso de derechos	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	1	3	24	Bajo
			Error en el uso	Ausencia de procedimientos sobre seguridad de la información	5	3	120	Medio
			Abuso de derechos	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	5	3	120	Medio

3. CONCLUSIONES

Del análisis del riesgo realizado a la seguridad de la información de quejas y reclamos, satisfacción al usuario y gestión documental, del proceso gestión de calidad y satisfacción al usuario, se puede concluir que:

- Se valoraron los activos con base en su costo de reposición y las consecuencias para la organización de la pérdida de confidencialidad, integridad y disponibilidad de los mismos.

- Se identificaron escenarios de incidente, mediante la selección de amenazas y vulnerabilidades que aplicaban para los activos.

- Se revisaron los controles existentes, determinando mediante unos criterios establecidos, la eficacia de los mismos.

- Se valoraron la probabilidad e impacto que podría tener cada escenario de incidente, según criterios definidos.

- Por último se realizó una estimación del riesgo para cada escenario de incidente, este se calculó multiplicando los valores del activo, impacto y probabilidad.

- Se identificaron los escenarios de riesgo que tienen un nivel de riesgo bajo, medio, alto y muy alto.

- De acuerdo al análisis realizado, los escenarios de riesgo que tienen un nivel de riesgo “muy alto” corresponden a:

Cuadro 15. Activos con nivel de riesgo más alto

Activo	Nombre	Amenazas	Vulnerabilidades
Hardware	Discos duros externos	Hurto de medios o documentos	Copia no controlada
Software	Gestión documental	Manipulación con software	Defectos bien conocidos en el software
		Abuso de derechos	Ausencia de pistas de auditoría
Personal	Técnico Gestión de Calidad	Incumplimiento en la disponibilidad del personal	Ausencia del personal
		Error en el uso	Uso incorrecto de software y hardware

- La ocurrencia de estos escenarios de incidentes podría afectar la operación interna de la organización, la credibilidad en el sistema de información interno y la reputación de la organización.

- Se debe analizar estos escenarios y determinar la forma como se hará el tratamiento de los riesgos identificados.

4. RECOMENDACIONES

La organización a lo largo de los últimos años ha incrementado su actuar frente a la seguridad de la información, activo que hoy se considera crítico para la operación; en consecuencia se han venido tomando una serie de medidas que garanticen su adecuada protección; sin embargo este es un proceso que requiere tiempo y un nivel de concientización de las partes interesadas, por tanto se hace necesario tener en cuenta los siguientes aspectos que ayuden a mejorar la seguridad en la organización:

- Realizar un proceso formal de levantamiento de activos de información, al igual que un proceso de clasificación de la información que permita determinar los niveles de criticidad de la misma.

- Implementar un proceso formal para el registro de incidentes de seguridad de la información, donde se documente el análisis y la gestión realizada para los casos presentados.

- Fortalecer el proceso de formación continua sobre seguridad de la información a todo el personal de la organización, logrando mayores niveles de concientización acerca de su protección.

- Revisar los controles que se han implementado en la organización, al igual que su pertinencia, de tal forma que se analice su eficacia y si es necesario, se tomen medidas correctivas en forma oportuna.

- Definir el enfoque de riesgo de la organización y realizar un análisis del riesgo de la información crítica, así como el plan de tratamiento del riesgo acorde con los criterios que se establezcan.

BIBLIOGRAFIA

ASMET SALUD EPS-S. Sistema de gestión documental. Popayán. 2011.

GUEVARA CAMPO, Carolina y MERA, Fabián Andrés. Criterios para establecer políticas de seguridad de la información y plan de contingencia, caso de estudio el centro de datos de la Universidad del Cauca. Universidad del Cauca. 2008. 132 p.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Sistemas de Gestión de la Seguridad de la Información. Bogotá D.C: ICONTEC, 2006. 37p. NTC-ISO/IEC 27001.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Código de práctica para la gestión de la seguridad de la información. Bogotá D.C: ICONTEC, 2007. 133p. NTC-ISO/IEC 27002.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Gestión del Riesgo en la seguridad de la información. Bogotá D.C: ICONTEC, 2009. 67p. NTC-ISO/IEC 27005.

MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información. Universidad Politécnica de Madrid. 2009. 306 p.

SANTOS, Luz Marina. Guía para la evaluación de seguridad en un sistema. Universidad de Pamplona. 12p.