DISEÑO DE LAS POLÍTICAS DE CONTROL DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SEDE CENTRAL DE LA GOBERNACIÓN DEL PUTUMAYO (MOCOA)

LEYDA LILIANA CORDOBA ARAUJO
WILSON CAMILO DELGADO TRUJILO

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MOCOA PUTUMAYO
2016

DISEÑO DE LAS POLÍTICAS DE CONTROL DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SEDE CENTRAL DE LA GOBERNACIÓN DEL PUTUMAYO (MOCOA)

LEYDA LILIANA CÓRDOBA ARAUJO
WILSON CAMILO DELGADO TRUJILLO

Trabajo de grado para optar el título de especialista en Seguridad Informática

Directora
YINA ALEXANDRA GONZÁLEZ SANABRIA
Ingeniera de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MOCOA PUTUMAYO
2016

Notas de aceptación:

_____

_____

_____

_____

_____

_____

Jurado

_____

Asesor/Director

Mocoa Putumayo, _____

Quiero dedicar el presente trabajo en primer lugar a Dios, a mi familia quienes me han apoyado en muchas jornadas de este proyecto, si bien a de terminar esta etapa me queda la satisfacción de haber compartido con personas muy valiosas, les doy las gracias por su apoyo y afecto.

Leyda Liliana Córdoba Araujo

A Dios, por haberme permitido realizar este proyecto de vida y haberme dado salud para lograr los objetivos propuestos, además de su infinita misericordia y amor. A mis familiares, mi padre Néstor Delgado y Aura Trujillo por ser ejemplos de responsabilidad y perseverancia, y me han inculcado esos valores para salir adelante. A mis hermanos Jairo Delgado por ser ejemplo como hermano mayor y estar siempre atento con las necesidades de la familia. A mis Hijos y esposa: Samuel camilo, Danna Catalina y esposa Susana por ser el motivo y la fuente de energía para salir adelante, para ser así un ejemplo para ellos de superación y buena persona.

Wilson Camilo Delgado Trujillo

AGRADECIMIENTOS

En primer lugar, agradecer a Dios por permitirnos llegar hasta este punto y lograr cumplir nuestras metas, además de su infinita bondad y amor; a los diferentes funcionarios de la Gobernación de Putumayo quienes nos facilitaron los medios e información requerida para el desarrollo del proyecto en especial a jefe de área de la Oficina de Sistemas, Ingeniero Andrés Trejo. Al tutor del curso Proyectos II el ingeniero Wilson Castaño quien nos apoyó en el desarrollo y fundamentación del anteproyecto. A La ingeniera YINA ALEXANDRA GONZÁLEZ SANABRIA Directora del proyecto quien con su compromiso, apoyo, dedicación y sus conocimientos nos permitió llevar a cabo este proyecto y cumplir con éxito los objetivos planteados.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

FIREWALL: Puede ser sistemas de software o hardware configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de políticas y otros criterios.

MAGERIT: Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

EAR / PILAR: Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

SSH: Secure Shell, es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

FTP: File Transfer Protocol - Protocolo de Transferencia de Archivos, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

TELNET: Telecommunication Network, es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

HTTP: HyperText Transfer Protocol - Protocolo de transferencia de hipertexto, es el método más común de intercambio de información en la world wide web, el método mediante el cual se transfieren las páginas web a un ordenador.

SERVIDOR: Es un ordenador o máquina informática que está al “servicio” de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información.

SNIFFER: Aplicación de monitorización y de análisis para el tráfico de una red, los analizadores de paquetes tienen diversos usos, como monitorear redes para detectar y analizar fallos, o para realizar ingeniería inversa en protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc.

DENEGACIÓN DE SERVICIO (DDoS): Es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos.

TRAZABILIDAD: Consiste en asociar sistemáticamente un flujo de información a un flujo físico de mercancías de manera que se pueda reencontrar en un instante determinado la información requerida relativa a los lotes o grupos de productos específicos.

DISPONIBILIDAD: Asegurar que acceso y el uso de información sea oportuno y confiable.

CONFIDENCIALIDAD: Preservar restricciones autorizadas en el acceso y publicación de información, incluyendo medidas para proteger la privacidad personal y la información propietaria.

INTEGRIDAD: Proteger la información de modificación o destrucción no autorizada, incluyendo los medios para asegurar el no repudio y la autenticidad de la información.

DEGRADACIÓN: Acción de degradar o hacer perder una cualidad o un estado característico, por ejemplo la degradación de un entorno natural es la pérdida de calidad de este, debida generalmente a la acción del hombre.

UPS: Uninterruptible power supply - son dispositivos que por sus baterías u otros elementos almacenadores de energía permiten proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que estén conectados.

ZENMAP: Zenmap es la interfaz gráfica oficial de nmap, válida tanto para Windows como para Ubuntu y otros sistemas (MAC OS, BSD,...), es gratuita y de código abierto, esta aplicación permite realizar escáner de puertos que nos puede dar mucha información acerca de una máquina.

SWITCHES: es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.[1]

SERVICIO VOZ/IP: Proviene del inglés Voice Over Internet Protocol - Voz sobre protocolo de internet, es un método por el cual tomando señales de audio analógicas del tipo de las que se escuchan cuando uno habla por teléfono se las transforma en datos digitales que pueden ser transmitidos a traves de internet hacia una dirección IP determinada.

[1] La Nueva Era Del Comercio/the New Era of Commerce: El Comercio Electrónico ... en Google Libros.

RESUMEN

La gobernación de Putumayo, es una entidad pública de orden territorial, como lo ordena la Constitución y la Leyes la promotora del desarrollo integral y sostenible de nuestro departamento a través del cumplimiento del plan de desarrollo y el mutuo acuerdo con los Municipios se encarga de garantizar a los habitantes del territorio putumayense, la prestación de los servicios esenciales impulsando el desarrollo económico y social en el marco de una economía, licita, rentable, competitiva y sostenible; promoviendo la participación comunitaria, bajo los criterios de eficiencia, eficacia, transparencia, responsabilidad y equidad.

Con los avances de las nuevas tecnologías de la información y las comunicaciones se han logrado avances significativos permitiendo que las entidades estén en la capacidad de ampliar la cobertura de los servicios que ofrecen, lo cual le permite a sus usuarios tener diferentes opciones al momento de requerirlos los tramites/servicios ofrecidos; sin embargo, estos nuevos procesos administrativos ha ocasionado que la información de las entidades tienda a ser más vulnerable o que sea el objetivo de ataque de personas mal intencionadas que desean obtener, modificar, eliminar y/o dañar la información. Por tal razón es indispensable la implementación de sistemas de gestión de seguridad informática que a través de las técnicas y metodologías apropiadas puedan proteger la información y evitar posibles ataques.

El presente trabajo está dirigido a la elaboración de un diagnóstico de las vulnerabilidades existentes en los sistemas de información que dispone la Gobernación de Putumayo, mediante la revisión de la infraestructura tecnológica, la evaluación del riesgo, el análisis de los controles existentes y el diseño de una serie de políticas y procesos que permitan mitigar, prevenir y controlar la seguridad de la información en la Entidad.

Lo anterior con el fin de garantizar la integridad, coherencia y confiabilidad en la información y los servicios que se realicen a través de medios electrónicos y permitan la disponibilidad de las operaciones de la administración departamental.

PALABRAS CLAVE: Seguridad informática. Vulnerabilidades, amenazas y riesgos. Políticas de seguridad de la información. Tecnologías de información y las comunicaciones.

ABSTRAC

The governorship of Putumayo, is a public entity of territorial order, as mandated by the Constitution and the law. Is the promoter of integral and sustainable development of our territory through the implementation of the development plan and mutual agreement with the municipalities , it is responsible for ensure the provision of essential services of the inhabitants of Putumayo territory and to boost economy growth and social development in the context of a licit , profitable, competitive and sustainable economy; in other hand is the promoter of the community participation, under the criteria of efficiency, effectiveness, transparency, accountability and fairness.

With the development of the new information technologies and communications they have been made significant progress allowing entities to expand the coverage of services provided, which allows its users to have different options in the moment of a requirement. However, these new administrative processes has caused the company information tends to be more vulnerable or is the target of attack from hackers or people with bad intentions who want to obtain, modify, remove and / or damage data. For this reason it is essential the implementation of computer systems security management that with the application of techniques and methodologies guarantee the protection of the information and prevent possible attacks.

This project is aimed to make a diagnosis of existing vulnerabilities in information systems available in the Governorship of Putumayo, by reviewing the technological infrastructure, risk assessment, analysis of existing controls and the design of a series of policies and processes to mitigate, prevent and control information security in the entity.

This in order to ensure the integrity, consistency and reliability of the information and services that are processes through electronic media and guarantee the availability of the operations of the public administration.

KEYWORDS: Computer Security. Vulnerabilities, threats and risks. Policy Information Security, Information Technology and Communications.

INTRODUCCIÓN

El comienzo del siglo XVII fue marcado altamente por una serie de inventos que dieron paso a la creación de lo que hoy conocemos como la computación, la cual no es un concepción de alguien en particular, sino el resultado evolutivo de ideas y realizaciones de muchas personas relacionadas con áreas tales como la electrónica, la mecánica, los materiales semiconductores, la lógica, el álgebra y la programación.[2] Todo este proceso ha servido para facilitar las tareas cotidianas del ser humano.

Actualmente existen muchos adelantos tecnológicos especialmente en el área de las redes de telecomunicaciones, que imponen nuevos y grandes retos, y en la medida en que se pueda responder a estos desafíos y se orienten todas las acciones en construir respuestas adecuadas, se puede lograr un desarrollo con altos niveles de competitividad. Es importante resaltar que estos avances han afectado positivamente todas las áreas de desempeño del ser humano, siendo una de ellas la Seguridad de la Información, la cual se conoce como las medidas preventivas que buscan mantener la confidencialidad, la disponibilidad e integridad de los datos de las organizaciones y de los sistemas de información de las mismas.

Teniendo en cuenta que la tecnología avanza a pasos agigantados se hace necesario implementar mejoras en las políticas de control de riesgos de la seguridad de la información, enfocando este proyecto al aprovechamiento de la tecnología ya existente en la Gobernación del Putumayo Sede Central (Mocoa) para lograr un excelente diseño de seguridad que blinde la información de la entidad. Este diseño ayuda a disminuir los riesgos de pérdida o robo de la información, permitiendo el control de la seguridad de la misma, además de brindar un referente para que otras entidades puedan implementarlo.

[2] Historia computación: Disponible en: http: //es.wikipedia.org/wiki/Historia_de_la_computaci%C3%B3n. Consultado el 21 de agosto de 2012.

1. FORMULACIÓN DEL PROBLEMA

Los grandes volúmenes de información y la importancia de los datos que manejan las entidades públicas ya sean de carácter municipal o departamental, son necesarias y fundamentales para el ejercicio y funcionamiento de todas sus áreas y procesos administrativos y las cuales pueden estar expuestas a muchas vulnerabilidades, amenazas y problemas de seguridad; tales como el hurto de información o la alteración de la misma con fines fraudulentos. Teniendo en cuenta estos aspectos, cabe hacerse la pregunta si las entidades del Estado están debidamente protegidas contra las fuentes de amenazas (internas y externas) a las cuales se encuentran expuestas.

Por las razones antes planteadas y teniendo en cuenta que este proyecto se centra en una sola entidad, resulta necesario dar repuesta al siguiente interrogante:

¿Cuáles son las Políticas de control de riesgo que debe implementar la Gobernación del Putumayo?

2. JUSTIFICACIÓN

La información, independiente de su naturaleza tiene un alto valor, es un activo de gran significado para cualquier tipo de organización, la frase aquella que dice que quien tiene la información tiene el poder está llena de sabiduría y realidad, y por tal razón existen muchas personas y grupos que se quieren hacer de la información, aun cuando tengan que robarla de otros, la realidad de nuestro país en cuanto a seguridad informática es bastante pobre, para la muestra basta con revisar algunas noticias que se han generado al respecto: el 21 de marzo de este año, el diario El Espectador publicó una nota con el titular ***Colombia, líder en inseguridad informática en América Latina***[3], y ponía en evidencia los hallazgos de la empresa McAffe en relación a la seguridad y que menciona los serios problemas que posee Colombia. Años atrás, en julio del 2008, la revista Dinero señaló: ***Colombia tiene que mejorar en seguridad informática***[4]y menciona como en ese año los estudios desarrollados por Cisco dieron a nuestro país un puntaje de 62, por debajo del promedio en Latinoamérica.

Los anteriores sucesos permiten plantear el análisis de una entidad de esta naturaleza para hacer un estudio de su situación actual y las políticas de gestión de riesgos que se proponen para minimizar este tipo de problemas, teniendo en cuenta que tienen un alta posibilidad de ser aplicadas, o por lo menos fácilmente adaptadas, a otras entidades de naturaleza similar. Además la Gobernación de Putumayo por ser una entidad de orden territorial debe cumplir los lineamientos establecidos en el Decreto Nacional N° 2573 del 201 4 "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.*" y en el cual se dispone que Colombia suscribió la Alianza para el Gobierno Abierto declarando su compromiso de realizar acciones para el aprovechamiento de las tecnologías, facilitando mayor apertura en el gobierno, mejorando la prestación de los servicios y la participación ciudadana en los asuntos públicos, y promoviendo la innovación y la creación de comunidades más seguras con el propósito de que el gobierno sea más transparente, sensible, responsable y eficaz; y de acuerdo a ello es necesario complementar los lineamientos de la estrategia de Gobierno en Línea, especialmente en temas de seguridad, privacidad, gestión de tecnologías de información e interoperabilidad, de tal manera que se avance integralmente en la provisión de servicios electrónicos de alta calidad para los ciudadanos.

[3] http://www.elespectador.com/tecnologia/colombia-lider-inseguridad-informatica-latina-articulo-482097

[4] http://www.dinero.com/negocios/tecnologia/articulo/colombia-tiene-mejorar-seguridad-informatica/65807

En el Artículo 5°, del mencionado decreto establece los cuatro (4) componentes de la estrategia, entre ellos el último denominado: **Seguridad y privacidad de la Información** el cual "*comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada"*.[5]

Teniendo en cuenta que el actual Plan de Desarrollo Nacional (2014-2018) se encuentra en Proyecto de ley se toma como referencia también el artículo 227 de la vigente Ley 1450 de 2011, por la cual se expide el Plan Nacional de Desarrollo 2010 - 2014, en la cual dispone que el Gobierno Nacional debe garantizar, mediante la implementación de sistemas de gestión para la seguridad de la información, que el acceso a las bases de datos y la utilización de la información sean seguros y confiables para no permitir su uso indebido.

Los directivos de la Gobernación del Putumayo demuestran gran interés en identificar la situación actual de la seguridad de la entidad, descubrir las posibles vulnerabilidades que se presentan y que no se encuentran protegidas con los debidos controles de seguridad, tecnológicas y políticas de seguridad que se pueden tener en cuenta para favorecer la seguridad informática.

La entidad pretende proteger sus activos de personas no autorizadas que puedan atentar con la prestación del servicio o la continuidad del negocio, por lo cual la Gobernación del Putumayo quiere definir y diseñar un sistema de seguridad informático que proteja toda la información confidencial, los equipos y su centro de comunicación, así como también fortalecer su seguridad, optimizar los recursos, mejorar los tiempos de servicios y mejorar el rendimiento de sus empleados.

[5]Decreto Nacional N° 2573. Ministerio de tecnología de la Información y la Comunicaciones, Bogotá, Colombia, del 2014, 12 de diciembre 2014.

3. OBJETIVO GENERAL Y ESPECÍFICOS

3.1 OBJETIVO GENERAL

Diseñar las políticas de control de riesgos de la seguridad de la información en la Gobernación de Putumayo (Sede Central) con el fin de disminuir los posibles riesgos en el tema de Seguridad Informática, garantizar la conservación y la correcta administración de los datos.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar y valorar los activos de información de la gobernación del Putumayo.

- Identificar las vulnerabilidades y amenazas existentes en los sistemas de información que dispone la Gobernación de Putumayo mediante una revisión de la infraestructura tecnológica.

- Realizar el análisis de los controles (salvaguardas) existentes y determinar la evaluación del riesgo.

- Diseñar una serie de políticas y procesos que permitan mitigar, prevenir, controlar o actuar frente a una situación en la cual se comprometa la información basados en la norma ISO 27000.

4. MARCO DE REFERENCIA

4.1 MARCO CONTEXTUAL

4.1.1 Historia

El suroccidente del departamento era territorio de los indígenas Cofán, el noroccidente de los Kamentxá, el centro y sur de pueblos de lenguas tukano como los Siona y el oriente por pueblos de lenguas witoto.3 Parte del territorio Kamentxá fue conquistado por el Inca Huayna Cápac en 1492, que tras atravesar el territorio Cofán, estableció en el valle de Sibundoy una población quechua, que hoy se conoce como Ingas. Tras la derrota de los incas en 1533, la región fue invadida por los españoles desde 1542 y administrada desde 1547 por sucesivas misiones católicas. Durante la época de la colonia el territorio putumayense formó parte de la provincia de Popayán; durante la Gran Colombia, y en las primeras décadas republicanas hizo parte del inmenso "Departamento de Asuay" que incluía territorios de las hermanas repúblicas de Ecuador y Perú, el cual comprendía parte de la actual Amazonía ecuatoriana y peruana.

Después comienza un largo proceso de redistribuciones territoriales: en el año 1831, pasó nuevamente a ser parte de la provincia de Popayán, y del territorio del Caquetá; en 1857 dependió del estado federal del Cauca; en 1886, al departamento del Cauca; en 1905, el general Rafael Reyes ordenó la creación de la intendencia del Putumayo; en 1909, formó parte de la intendencia del Caquetá y del departamento de Nariño; en 1912, fue creada la comisaría especial del Putumayo, la que en 1953 fue anexada al departamento de Nariño y en 1957, desanexada para volver a su condición independiente; en 1968, la ley 72, creó la intendencia del Putumayo con capital en la ciudad de Mocoa, siendo inaugurada en 1969; y finalmente, el 4 de julio de 1991, la Asamblea Nacional Constituyente creó el departamento del Putumayo, conservando a Mocoa como la capital de la nueva división político administrativa.

La mayor parte de la población migró desde finales del siglo XIX, acentuándose a mediados y finales del siglo XX. Los momentos mayores de poblamiento han estado ligados a las bonanzas extractivistas como la quina, el caucho, las maderas y pieles preciosas. Sin embargo, el grueso de la población definitivamente lo conforman las corrientes migratorias originadas por la extracción petrolífera y el asentamiento definitivo que en su momento lo impulsó el cultivo de

coca. En la actualidad el departamento presenta un importante flujo migratorio producto de los programas asistencialistas del Estado.[6]

4.1.2 Ubicación y localización geográfica

El departamento de Putumayo, está situado en el sur del país, en la región de la Amazonía, localizado entre 01°26'18'' y 01°27'37'' de latitud norte, y 73°50'39' y 77º4'58'' de longitud oeste.

Figura 1. **Localización del departamento de Putumayo en Colombia**

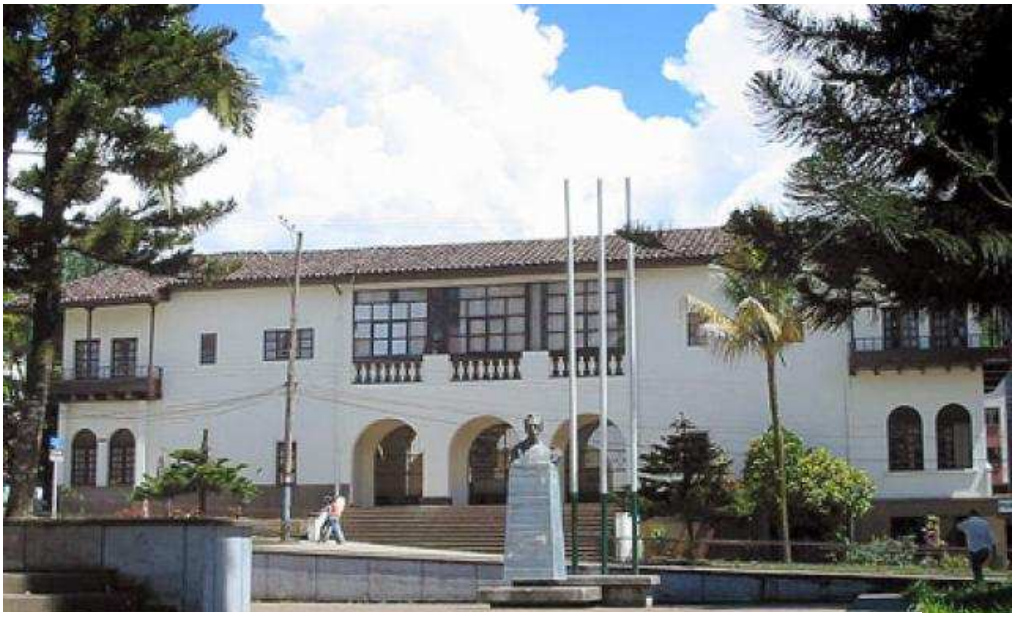
Fuente: Página web www.putumayo.gov.co

[6]Plan de Desarrollo Departamental 2012-2015 Sistema Integrado Gobernación de Putumayo

4.1.3 Descripción de la Entidad

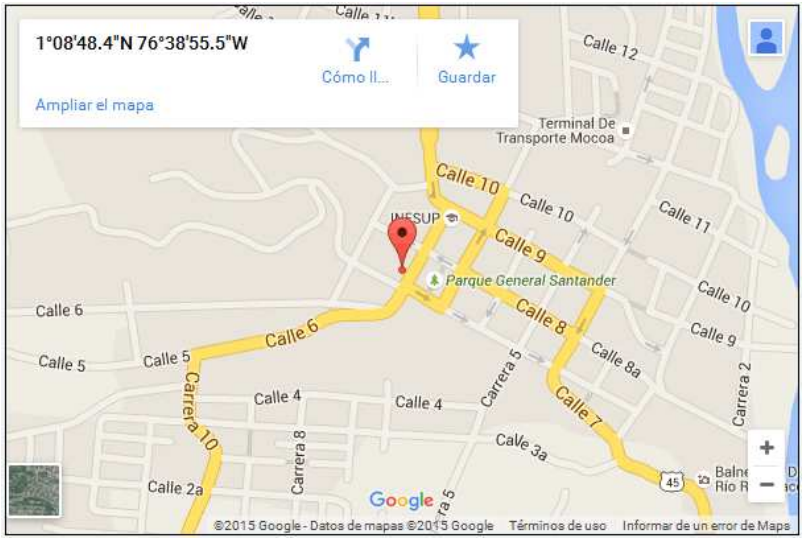
La gobernación de Putumayo es una entidad pública que se encuentra ubicada en la calle 8N° 7-40 del municipio de Mocoa departame nto de Putumayo, según el Decreto 100 del 2009, tiene adscritas diez secretarias departamentales.

Figura 2. Foto Gobernación de Putumayo.



Fuente: Registro fotográfico página web

Figura 3. Ubicación-Mapa.



Fuente: Google 2015 – datos de Mapas

La entidad Cuenta con 158 funcionarios de nómina y en la sede central se encuentra ubicadas las siguientes dependencias:

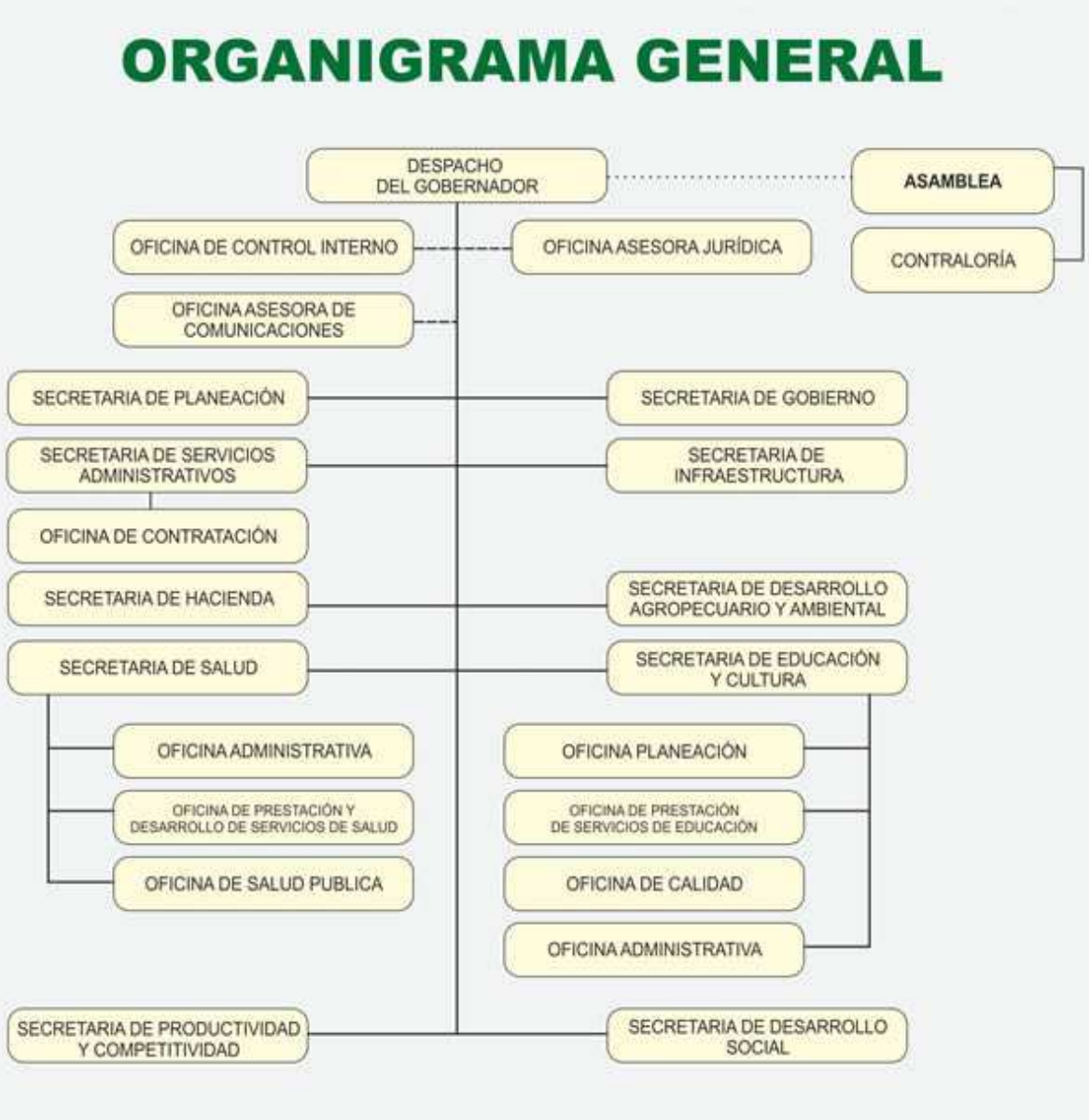
Tabla 1. Dependencias y oficinas del edifio dentral de la Gobernación.

Secretarias/Dependencias	Oficinas
Servicios Administrativos	Oficina recepción
	Oficina Sistemas
	Recursos humanos
	Pensiones
	Almacén departamental
	Salud ocupacional
Secretaria de Hacienda	Recepción
	Presupuesto
	Contabilidad
	Tesorería
	Rentas departamentales
Secretaria de Gobierno	Recepción
	Gestión de riesgo/ victimas
Secretaria de Planeación	Recepción
	Banco de proyectos
	Archivo de proyectos
	Plan departamental de aguas
	Asistencia municipal
	Oficina de Calidad
Secretaria de infraestructura	Recepción y Oficina profesionales
Sec. Desarrollo Agropecuario y Medio Ambiente	Recepción
	Oficina profesionales
Contratación	Contratación
Secretaria de Competitividad y productividad	Recepción
Jurídica	Oficina Jurídica
Control interno de Gestión	Oficina control interno

Fuente: Información entregada en la entidad.

4.1.4 Organigrama

Figura 4. Organigrama Gobernación de Putumayo



Fuente: Página web www.putumayo.gov.co

4.1.5 Plataforma estratégica

4.1.5.1 Misión

La Gobernación del Putumayo es la entidad promotora del desarrollo integral y sostenible de su territorio, a través del cumplimiento del Plan de Desarrollo, con talento humano comprometido y competente, de conformidad con la constitución y el ordenamiento jurídico Colombiano.

4.1.5.2 Visión

Para el año 2020, la Gobernación del Putumayo será entidad modelo de gerencia y gestión pública, actuando sobre la base de la Legalidad, Transparencia, Equidad, Dignidad Humana, Eficiencia y Eficacia, Participación Comunitaria.

4.1.5.3 Política de calidad

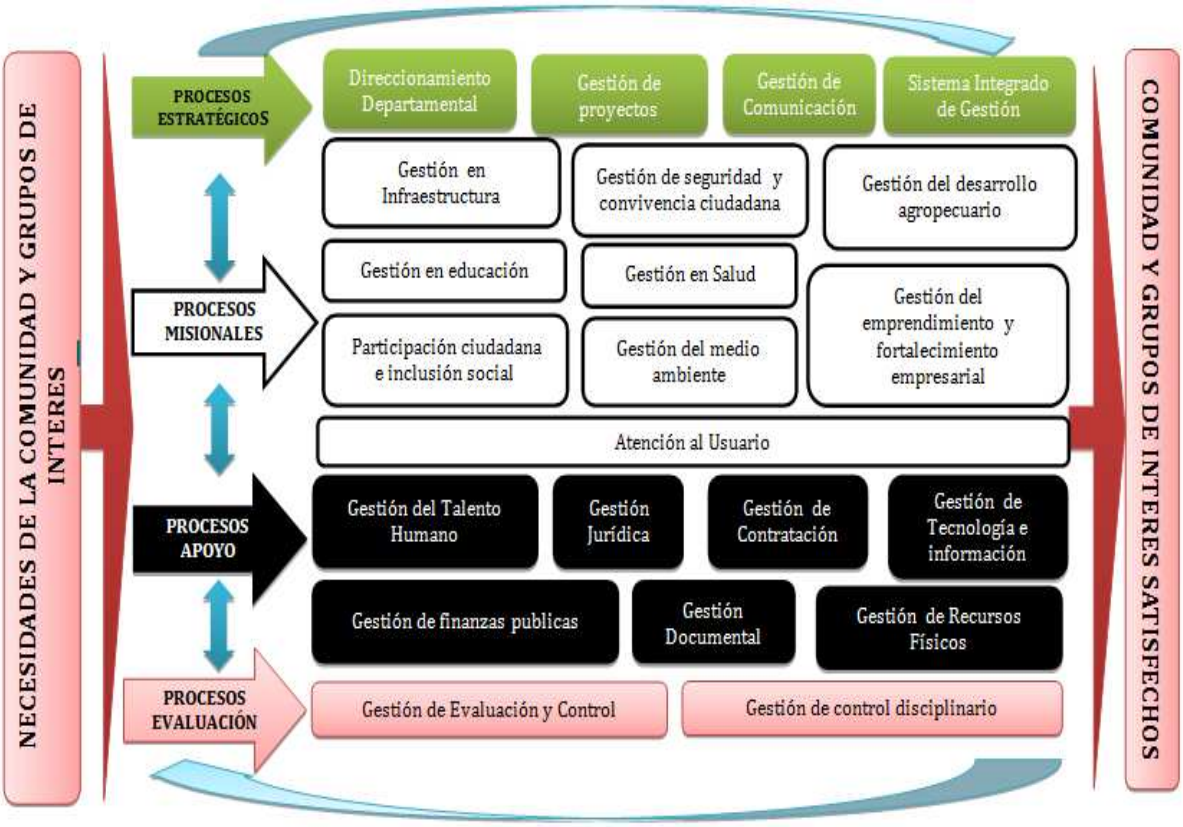
La Gobernación se compromete con la comunidad Putumayense y sus grupos de interés, a la satisfacción de sus necesidades median-te el cumplimiento del Plan de Desarrollo, el mejoramiento continuo de sus procesos, con talento humano idóneo, contribuyendo con el desarrollo sostenible y la calidad de vida de la Región.[7]

4.1.5.4 Mapa de procesos

La gobernación de Putumayo se encuentra en proceso de certificación al sistema integrado de Gestión **NTCGP 1000:2009—MECI 2014**, para lo cual la oficina de Sistemas se encarga del proceso de Gestión de Tecnología e información, el cual se encuentra ubicado dentro del mapa de procesos como *Procesos de Apoyo*:

[7]Documentación Sistema Integrado Gobernación de Putumayo

Figura 5. Mapa de Procesos V.1.0



Fuente: Documentación oficina Calidad Gobernación de Putumayo.

Proceso: Gestión de Tecnología e Información

Alcance: El proceso de Gestión de tecnología e información inicia con la elaboración del plan de acción y termina con la implementación de acciones de mejora.

Objetivo: Realizar la dirección, planeación, coordinación, organización, evaluación, supervisión y seguimiento de los sistemas de información y las comunicaciones de la Gobernación del Putumayo.

Entre los procedimientos que lo conforman se encuentran:

1. PT-GTI-001 Procedimiento para administración, gestión de la red de datos
2. PT-GTI-002 Procedimiento para la administración y soporte de correos institucionales
3. PT-GTI-003 Procedimiento seguridad informática
4. PT-GTI-004 Procedimiento de mantenimiento preventivo de equipos de sistemas
5. PT-GTI-005 Procedimiento de mantenimiento correctivo de hardware
6. PT-GTI-006 Procedimiento para la administración de la página web
7. PT-GTI-007 Procedimiento de respaldo y protección de la información
8. PT-GTI-008 Procedimiento de Asistencia Técnica de Software

A continuación se presenta la estructura del procedimiento PT-GTI-003: Seguridad Informática:

Figura 6. PT-GTI-003 Procedimiento seguridad informática

PUTUMAYO GOBERNACIÓN NIT. 800.094.164-4	SISTEMA INTEGRADO DE GESTIÓN	CÓDIGO: PT-GTI-003
	PROCEDIMIENTO DE SEGURIDAD INFORMÁTICA	VERSIÓN: 01
		FECHA: 25/03/2015

4. CONTENIDO

No.	FLUJOGRAMA	ACTIVIDAD	RESPONSABLE	REGISTRO
0	Inicio	Inicio		
1	Levantamiento de riesgos	Identificación de los posibles riesgos de seguridad informática.	Profesional universitario área de sistemas	No aplica
2	Se realiza inducción	Se realiza un proceso de inducción al personal en el manejo de la disminución de los riesgos de seguridad informática.	Profesional universitario área de sistemas	Listado de asistencia FT-GTH-001
3	Se capacita al personal	Se capacita al personal	Profesional universitario área de sistemas	Listado de asistencia FT-GTH-001
4	Adquisición de software	Adquisición de software de prevención	Almacén	No aplica
5	Implementación de actividades	Implementación de actividades de prevención de fallas de seguridad.	Profesional universitario área de sistemas	No aplica
6	Se realiza ajustes	Se procede a realizar los ajustes respectivos.	Profesional universitario área de sistemas	No aplica
7	Fin	Fin		

Fuente: Documentación oficina Calidad Gobernación de Putumayo

4.2 ESTADO DEL ARTE

En Colombia se han desarrollado diferentes estudios sobre la seguridad de la información y el diseño de políticas para ser aplicados en diferentes sistemas de información tanto de entidades públicas como de empresas privadas las cuales han sido lideradas por Instituciones Educativas como la universidad de la UNAD, estos proyectos han permitido conocer otras propuestas similares que han dado excelentes resultados, las cuales se convierten en fuentes alternativas de estudio para el proyecto, a continuación se da a conocer algunas de ellas:

En San Juan de Pasto en el año 2014, Luis Olmedo Patiño Alpala desarrolló el proyecto denominado PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA CORPORATIVA, PROPOLSINECOR, como opción de grado de la Especialización en seguridad informática de la universidad nacional abierta y a distancia "UNAD", con este proyecto el autor plantea dar solución a la problemática que se presenta en la empresa PROPOLSINECOR, la cual tiene implementado un sistema de seguridad sin documentación de respaldo y sin ser socializado con el personal de la empresa, el autor evidencia que la organización hace uso de herramientas y sistemas sensibles y detecta que la empresa ha tenido un crecimiento muy importante, que esta es ahora más vulnerable y susceptible a sufrir ataques que afecten la integridad y confidencialidad de la información, es por esto que con la necesidad y la problemática identificada, realiza y estipula una serie de políticas de seguridad enfocadas a proteger los activos de información de la empresa PROPOLSINECOR.

En Pamplona en el año 2015, Jorge Enrique Ramírez Montañez desarrolló el proyecto denominado ANÁLISIS, EVALUACIÓN DE RIESGOS Y ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DE PAMPLONA - NORTE DE SANTANDER, como opción de grado de la Especialización en seguridad informática de la universidad nacional abierta y a distancia "UNAD".

En la ciudad de Popayán en el año 2014, John Jairo Perafán Ruiz y Mildred Caicedo Cuchimba desarrollaron el proyecto denominado ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓNUNIVERSITARIA COLEGIO MAYOR DEL CAUCA; como opción de grado de la Especialización en seguridad informática de la universidad nacional abierta y a distancia "UNAD".

En la ciudad de Bogotá en el año 2015, Hina Luz Garavito robles desarrolló el proyecto denominado ANÁLISIS Y GESTIÓN DEL RIESGO DE LA INFORMACIÓN EN LOS SISTEMASDE INFORMACIÓN MISIONALES DE UNA ENTIDAD DEL ESTADO, ENFOCADOEN UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN; como opción de grado de la Especialización en seguridad informática de la universidad nacional abierta y a distancia “UNAD”.

Otro de los proyectos referenciados es el denominado IMPLEMENTACIÓN DE LOS CONTROLES ASIGNADOS AL DOMINIO “GESTIÓN DE ACTIVOS”, BAJO LOS LINEAMIENTOS ESTABLECIDOS POR LA NORMA ISO/27001 ANEXO A, PARA LAS EMPRESAS MUNICIPALES DE CALI, EMCALI E.I.C.E-ESP, realizado por Paul Rosemberg Enriquez Espinosa, presentado en Cali el julio del 2013, este fue realizado para atender las necesidades presentadas en las empresas municipales de Cali EMCALI, específicamente dentro del área de los sistemas de información, la cual en el año 2013 estaba en busca la certificación ISO 27000, el autor de la obra plantea el diseño de un SGSI para apoyar en el proceso de fortalecer el eje de seguridad de la empresa, para este trabajo se inició con la identificación y evaluación de sus activos de información, para luego con estas bases sólidas plantear los controles asociados a estos activos, todo este proceso permitió que EMCALI minimizara los riesgos sobre la información relevante que procesa la empresa y así identificar los controles del SGSI.

Dentro del proyecto objeto de estudio se desarrolla la metodología de investigación Magerit, la cual plantea una serie de lineamientos para aplicar y levantar de forma correcta los controles de seguridad de la información, otra metodología que se tiene como referencia es el modelos PHVA, esta es muy importante ya que plantea un modelo de mejora continua dentro de las políticas desarrolladas, es decir se pueden agregar o evaluar para ver el desarrollo de estas frente a los incidentes de seguridad presentadas.

Entre algunos de los estudios también centrados en el ámbito de este proyecto se puede mencionar el siguiente realizado en Madrid España en el año 2011, Sandra Ontoria Gonzalo desarrollo el proyecto denominado GOBIERNO Y MODELADO DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES, como opción de grado de la de Ingeniería Técnica en Informática de Gestión de la Escuela Politécnica de Madrid del Universidad Carlos III de Madrid, en este proyecto la autora realiza el estudio del gobierno de seguridad de la información con el fin de realizar un diseño de un nuevo gobierno de la seguridad, tomando como base la normatividad ISO 27000 y modelos en seguridad muy robustos para la realización de Gobiernos de la seguridades como lo son COBIT e ITIL, La autora también plantea el uso de herramientas del mercado para la gestión de seguridad, con estas metodologías y normas aplicadas

a las organizaciones se plantea proteger la información confidencial de las personas y la misma organización.

4.3 MARCO TEÓRICO

Para la realización este proyecto se tendrá como base la norma ISO 27000que proporciona un marco para la gestión de la seguridad de la información y especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar los controles de seguridad implementados en la Gobernación del Putumayo, además de sus complementos 27001 a 27005.

La norma 27001 especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización. La 27002 es una guía de buenas prácticas sobre las medidas a tomar para asegurar los sistemas de información en una organización. La 27003 que consiste en una guía de implementación de SGSI y por consiguiente plantea el modelo para establecer los controles de seguridad a implementar en la gobernación del putumayo, todo esta información haciendo uso del modelo PHVA y de los requerimientos de sus diferentes fases. La 27004 que especifica las métricas y técnicas de medidas para determinar la eficacia de los controles de seguridad ya implementados. La 27005 que establece las directrices para la gestión del riesgo en la seguridad de la información y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Este conjunto de normas plantean modelos a seguir para lograr establecer la seguridad adecuada y así proteger los activos de información más vulnerables de la entidad, en nuestro caso la Gobernación del Putumayo e implementar las políticas de seguridad informáticas para reducir al máximo la perdida de la integridad, la disponibilidad y la confidencialidad de la información.

Con el fin de obtener información sobre la seguridad de la información se realizó un estudio para tomar referencias que expliquen de manera global lo que se requiere en un diseño de políticas de control de riesgo, encontrando los siguientes datos:

4.3.1 Concepción de la Seguridad De La Información[8]

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y se debe saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

Crítica: Es indispensable para la operación de la empresa; **Valiosa:** Es un activo de la empresa, muy valioso y **Sensible:** Debe de ser conocida por las personas autorizadas

Existen dos palabras muy importantes que son riesgo y seguridad: El **Riesgo** Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio y **Seguridad:** Es una forma de protección contra los riesgos.

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

Precisamente la reducción o eliminación de riesgos asociado a una cierta información es el objeto de la seguridad de la información y la seguridad informática. Más concretamente, la seguridad de la información tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información.[9]Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración. La correcta Gestión de la Seguridad de la Información busca

[8]Concepción de la seguridad de la información. Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Concepci.C3.B3n_de_la_seguridad_de_la_informaci.C3.B3n - Consultado el 11 de Junio de 2014.

[9]44 U.S. Code § 3542 - Definitions. Disponible en: http://www.law.cornell.edu/uscode/text/44/3542 - Consultado el 11 de Junio de 2014.

establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro.

4.3.2 Protocolos De Seguridad De La Información[10]

Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. Se componen de:

Criptografía (Cifrado de datos), se ocupa del cifrado de mensajes un mensaje es enviado por el emisor lo que hace es transposicionar u ocultar el mensaje hasta que llega a su destino y puede ser descifrado por el receptor.

Lógica (Estructura y secuencia). Llevar un orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuándo se va enviar el mensaje.

Identificación (Autenticación). Es una validación de identificación es la técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor.

4.3.3 El Manejo De Riesgos[11]

Dentro de la seguridad en la información se lleva a cabo la clasificación de las alternativas para manejar los posibles riegos que un activo o bien puede tener dentro de los procesos de organización. Esta clasificación lleva el nombre de manejo de riegos. El manejo de riesgos, conlleva una estructura bien definida, con un control adecuado y su manejo, habiéndolos identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

---

[10] Seguridad de la información. Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#cite_ref-1 - Consultado el 11 de Junio de 2014.

[11] Seguridad de la información. Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#cite_ref-1 - Consultado el 11 de Junio de 2014.

Evitar. El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades. **Ejemplo:** No instalar empresas en zonas sísmicas.
Reducir. Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación de controles y su monitoreo constante. **Ejemplo:** No fumar en ciertas áreas, instalaciones eléctricas anti flama, planes de contingencia.

Retener, Asumir o Aceptar el riesgo. Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente. **Ejemplo de asumir el riesgo:** Con recursos propios se financian las pérdidas.

Transferir. Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo, compartiéndolo con otras entidades. **Ejemplo:** Transferir los costos a la compañía aseguradora.

4.3.4 Sistema de Gestión de la Seguridad de la información – SGSI

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. [12]

[12] Disponible en: https://prezi.com/z3mqsmb25aun/herramientas-iso-27000/

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

4.3.5 ISO/IEC 27000

Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español aunque hay que prestar atención a la versión descargada.

4.3.6 ISO/IEC 27001

Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Actualmente, la última edición de 2013 este estándar se encuentra en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013. Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC

27001:2014. En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/ Cor 1:2015). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001), Chile (NCh-ISO27001) o Uruguay (UNIT-ISO/IEC 27001).

4.3.7 ISO/IEC 27002

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondo norma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita).

Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013.

4.3.8 ISO/IEC 27003

Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. En España, esta norma aún no está traducida, pero sí en Uruguay (UNIT-ISO/IEC 27003).

4.3.9 ISO/IEC 27004

Publicada el 15 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. En España, esta norma aún no está traducida, sin embargo sí lo está en Argentina (IRAM-ISO-IEC 27004) o Uruguay (UNIT-ISO/IEC 27004). El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.

4.3.10 ISO/IEC 27005

Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. El original en inglés puede adquirirse en iso.org. En España, esta norma no está traducida, sin embargo, sí lo está, para la versión de 2008, en países como México (NMX-I-041/05-NYCE), Chile (NCh-ISO27005), Uruguay (UNIT-ISO/IEC 27005) o Colombia (NTC-ISO-IEC 27005). Actualmente en proceso de revisión para su actualización.[13]

4.4 MARCO CONCEPTUAL

4.4.1 Confidencialidad

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

[13] Disponible en: http://www.iso27000.es/iso27000.html

4.4.2 Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información[14]

4.4.3 Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. [15]

4.4.4 Autenticación o autentificación

Es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso. [16]

[14] Disponible en: http://certificacionesensi.blogspot.com.co/
[15] Disponible en: http://laimportanciadelaseguridad.blogspot.com/
[16] Disponible en: http://seguridad-informatica5.webnode.es/news/confidencialidad-integridad-y-disponibilidad-de-la-informacion/

4.4.5 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. Actualizada en 2012 en su versión 3.[17]

El nombre de MAGERIT responde a "Metodología de Análisis y Gestión de Riesgos de IT", y es un método formal orientado a activos, cuya misión es descubrir los riesgos a los que se encuentran expuestos nuestros sistemas de información y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. [18]

4.4.6 Vulnerabilidades

Son todas aquellas condiciones del entorno que no han sido consideradas en la protección de los activos, son las debilidades que tienen los bienes y que pueden ser explotadas por una amenaza.

4.4.7 Amenazas

Son elementos o acciones que pueden atentar contra la seguridad de la información, estas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología. [19]

4.4.8 Activos de información

Es todo aquello que las entidades consideran importante o de alta validez para la para la organización y por tanto debe protegerse; los cuales pueden ser cualquier

[17] Disponible en: http://administracionelectronica.gob.es
[18] Disponible en: https://seguridadinformaticaufps.wikispaces.com
[19] Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

elemento que contiene o manipula información tales como ficheros y bases de datos, acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de una entidad se deben considerar todos los tipos de activos. [20]

4.4.9 Control de acceso

Hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos. Básicamente encontramos sistemas de controles de acceso en múltiples formas y para diversas aplicaciones. Por ejemplo, encontramos sistemas de controles de acceso por software cuando digitamos nuestra contraseña para abrir el correo, otro ejemplo es cuando debemos colocar nuestra huella en un lector para encender el PC. Estos casos, son ejemplos que permiten el acceso a datos. El concepto de control de acceso consta de tres pasos, los cuales son la identificación, autenticación y autorización, con el uso de estos principios un administrador del sistema puede controlar que recursos están disponibles para los usuarios de un sistema. [21]

4.4.10 SGSI

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

[20] Disponible en: http://myslide.es/documents/los-activos-de-seguridad-de-la-informacion.html
[21] Disponible en: https://prezi.com/hn46qk4stjtq/control-de-acceso/

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.[22]

4.4.11 EAR / PILAR - Herramienta para Análisis y Gestión de Riesgos

Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit, PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son[23]:

- ✓ ISO/IEC 27002:2005 - Código de buenas prácticas para la Gestión de la Seguridad de la Información
- ✓ ENS - Esquema Nacional de Seguridad

4.4.12 Análisis cualitativo en PILAR

PILAR puede realizar un análisis cualitativo, usando una serie de niveles discretos para la valoración de los activos. Un análisis cualitativo se recomienda siempre en primer lugar, antes de que se intente un análisis cuantitativo detallado. Un análisis cualitativo permite: identificar los activos más significativos, identificar el valor relativo de los activos, identificar las amenazas más relevantes, identificar las salvaguardas presentes en el sistema, establecer claramente los activos críticos (los que están sujetos a un riesgo máximo). [24]:

4.4.13 Ingeniería Social

Es una acción o conducta social destinada a conseguir información de las personas cercanas a un sistema por medio de habilidades sociales. Con esto se busca que el usuario comprometa al sistema y revele información valiosa por medio de variados tipos de engaños, tretas y artimañas. Por ejemplo, el usuario es tentado a realizar una acción necesaria para vulnerar o dañar un sistema, cuando recibe un mensaje que lo lleva a abrir un archivo adjunto. O puede suceder que el

[22] Disponible en: http://www.iso27000.es/sgsi.html.
[23] Disponible en: http://www.ar-tools.com/es/index.html
[24] Disponible en: http://es.slideshare.net/EBatistaHim/pilar-analisis-de-riesgo

usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos, en el caso del scam y el phishing

4.5 MARCO LEGAL

ISO/IEC 27000: Se toman como soporte los estándares de la norma ISO/IEC 27000 las siguientes y legislaturas tanto nacionales como internacionales:

Norma ISO/IEC 27001: Define los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).

Norma ISO/IEC 27002: (anterior ISO 17799). Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.

Norma ISO/IEC 27003: Proporciona ayuda y orientación sobre la implementación de un SGSI, incluye el método PHVA (planear, hacer verificar y actuar) contribuyendo con revisiones y mejora continua.

Norma ISO/IEC 27004: Especificará las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles. Aplicable específicamente en la fase del hacer (Do); de acuerdo con el método PHVA.

Norma ISO/IEC 27005: Suministra directrices para la gestión del riesgo en la seguridad de la información.

Ley 1273 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"..[25]

[25] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES (MinTIC).

Ley 1712 del 6 de marzo del 2014, “Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones”.

Decreto Nacional N° 2573 , “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.", [26]

Ley 1341 de 2009, “Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones

[26]PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA año 2014.

5. DISEÑO METODOLÓGICO

5.1 FUENTES DE INFORMACIÓN

A continuación se menciona las fuentes necesarias para obtener la información para llevar a cabo este proyecto:

- **Primaria**: Se obtuvo información mediante las técnicas de recolección de información como son la entrevista y encuesta. La técnica de la encuesta se llevó a cabo por medio de una serie de preguntas sencillas, claras y precisas y con diferentes opciones de respuesta, con las cuales se buscaba conocer de forma personalizada el nivel de conocimiento en cuanto al tema de Seguridad de la Información y algunas evidencias específicas de las políticas que se manejan en la entidad. De igual manera, se elaboró un formato de entrevista aplicada al profesional universitario del área de Sistemas de la Gobernación del Putumayo encargado del proceso de Gestión de Tecnología e Información, con el fin de conocer la información de la infraestructura física, lógica y metodológica de seguridad, como parte del estudio de la situación actual de la entidad (parte central); estas preguntas se elaboraron de forma clara y sencilla, con diferentes opciones de respuesta. Esta técnica es de gran utilidad porque permite fijar la atención en ciertos aspectos que se consideran esenciales dentro del proyecto.

- **Secundaria**: entre las fuentes secundarias utilizadas para el desarrollo del proyecto, está la revisión documental, tanto de documentos propios de la Entidad como de material bibliográfico, consultas a diferentes páginas web, que proporcionaron ayudas para definir el marco teórico del proyecto, también las normas, estándares, modelos y metodologías vigentes relacionadas con la seguridad de la información.

5.2 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El proyecto se apoyó en las siguientes herramientas con el fin de llevar a cabo las diferentes fases:

- Técnicas: Se realizaron procesos de análisis documental, estadísticas, y una serie de encuestas y entrevista a las personas involucradas con los procesos de seguridad de la información de administración departamental.

- Instrumentos: Para el desarrollo del proyecto se plantearon las siguientes herramientas:

  - ✓ **Encuestas y cuestionarios:** Se desarrollaron una serie de encuestas\cuestionarios dirigidos a las personas que de alguna forma se encuentran vinculados a los procesos de manejo de información; con el fin de y lograr determinar vulnerabilidades, conductas y el conocimiento que tenían los funcionarios sobre las políticas de seguridad de la información de la entidad, se. El proceso se realizó mediante documento físico ya que por facilidad de manejo por parte de los funcionarios fue el más adecuado.

  - ✓ **Entrevista**: Se desarrolló una entrevista con el responsable del área más sensible en cuanto a administración y seguridad de la información se refiere, apoyados en formatos establecidos y estudios previos.

  - ✓ **Observación y visitas de campo:** Se utilizó las visitas de campo a las diferentes áreas de la entidad así como también la observación para registrar patrones de conducta de los funcionarios y de los sistemas de información.

  - ✓ **Revisión documental:** Por otra parte también se realizó la revisión de la documentación que hace parte de los Sistemas de Seguridad de La Información tales como las normas NTCISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, la Metodología MAGERIT entre otros documentos que se incluyen en las referencias bibliográficas.

5.3 LÍNEA DE INVESTIGACIÓN

La Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI de la UNAD ha definido líneas de investigación por cada cadena de formación, de acuerdo al tema de estudio de este proyecto se enmarca dentro de la siguiente línea:

2. CADENA DE FORMACIÓN DE SISTEMAS	Línea 1. Gestión de sistemas.

5.4 POBLACIÓN

La población de la Gobernación de Putumayo de la sede central está conformada por 158 empleados de nómina de los cuales 12 funcionarios tienen cargos directivos incluidos el Señor Gobernador y secretarios de Despacho y 205 contratistas; sin tener en cuenta la Secretaria de Educación Departamental que estuvo intervenida por el Ministerio de Educación y tiene una planta de personal independiente. De total de personal de funcionarios y contratistas la entidad cuenta con 6 personas que laboran en áreas de sistemas de Información (técnicos, tecnólogos y Especialistas en áreas a fines). En cuanto a equipos de cómputo la gobernación dispone de 56 portátiles, 275 computadores de escritorio para un total de 331 según el inventario.

5.5 MUESTRA

Para efectos de la obtención de información se aplicó una encuesta a los usuarios de la Entidad, se tomó una muestra con el nivel de confianza de 75% de la población total. Para calcular el tamaño de la muestra de los funcionarios de nómina se aplicó la siguiente fórmula:

$$\mathbf{n=}\ \frac{Nz^2pq}{(N-1)\mathbf{d}^2 + z^2pq}$$

N: Tamaño de la población.
Z: El nivel de confianza (para este caso, 75%, es decir, α = 0.05 y z = 1.15).
pq: La varianza de la población. Se asume la mayor posible (pq = 0.25, esto es: p Para = 0.5 y q = 0.5).
d: El error muestral o error de estimación (d = 0.05).

$$n=\ \frac{(158)(1.15^2)(0.25)}{(158\text{-}1)(0.05^2) + (1.15^2)(0.25)}$$

Los valores de *k* más utilizados y sus niveles de confianza son:

n= 72.24 ≈ 72Funcionarios

Valor de *k*	1,15	1,28	1,44	1,65	1,96	2,24	2,58
Nivel de confianza	75%	80%	85%	90%	95%	97,5%	99%

De esta misma forma se realiza el cálculo para el grupo de población y como resultado tenemos: 72 funcionarios de nómina.

6. DESARROLLO METODOLOGICO

6.1 DIAGNÓSTICO SITUACIONAL

Según la información obtenida y la documentación facilitada en la entidad se evidencia que no existe un inventario unificado, ya que la oficina de Sistemas cuenta con los datos entregados por el área de almacén y otro sistema de información de software gratuito (GLPI) donde ingresan la información de los equipos de cómputo, referencias y características generales.

La gobernación cuenta con un centro de datos ubicado en la sede central de la entidad, en el cual se encuentra la central telefónica (voz-ip), Respaldo eléctrico, Firewall físico, switches y los servidores: de archivos, aplicaciones, SIG, de actualizaciones, dominio y WEB; configurados a través de la técnica de la virtualización; en cuanto al almacenamiento el centro de datos cuenta con una SAN (Storage área Network) que conecta los servidores.

La entidad posee un sistema de cableado estructurado Categoría 6 con aproximadamente 210 puntos de red (Anexo N° 7. Planos de la red datos) , los cuales están distribuidos a través de dos sub-centros ubicados de forma estratégica en algunas Secretarias de igual forma que el respaldo eléctrico, un Switch administrable de 48 puestos y el respaldo eléctrico con una UPS de 6 KVA. La red inalámbrica de la entidad dispone de una controladora Cisco configurada con 5 Acces-Point que brindan el servicio a toda la sede central. El servicio de internet se obtiene mediante canal dedicado de 6 MEGAS en fibra óptica, servicio brindado por el único proveedor en el departamento.

De acuerdo a la información recolectada en la entidad existe desconocimiento por parte de la mayoría de los funcionaros acerca de la importancia de la seguridad de la información, tanto de los datos que manejan diariamente como de sus propios datos personales. No existe en la entidad un documento que consolide las políticas de seguridad que deben aplicar las personas que laboran en la administración departamental, teniendo en cuenta sus respuestas también se evidencia la falta de procesos de concienciación tales como capacitaciones y talleres que les permita a los funcionarios conocer acerca de las vulnerabilidades y los diferentes ataques a los cuales pueden estar expuestos.

Una de las más grandes dificultades que se evidencia es la falta de políticas y controles en cuanto a las copias de seguridad de los equipos de cómputo de los

funcionarios, ya que según sus respuestas la mayoría reportaron que alguna vez han perdido información.

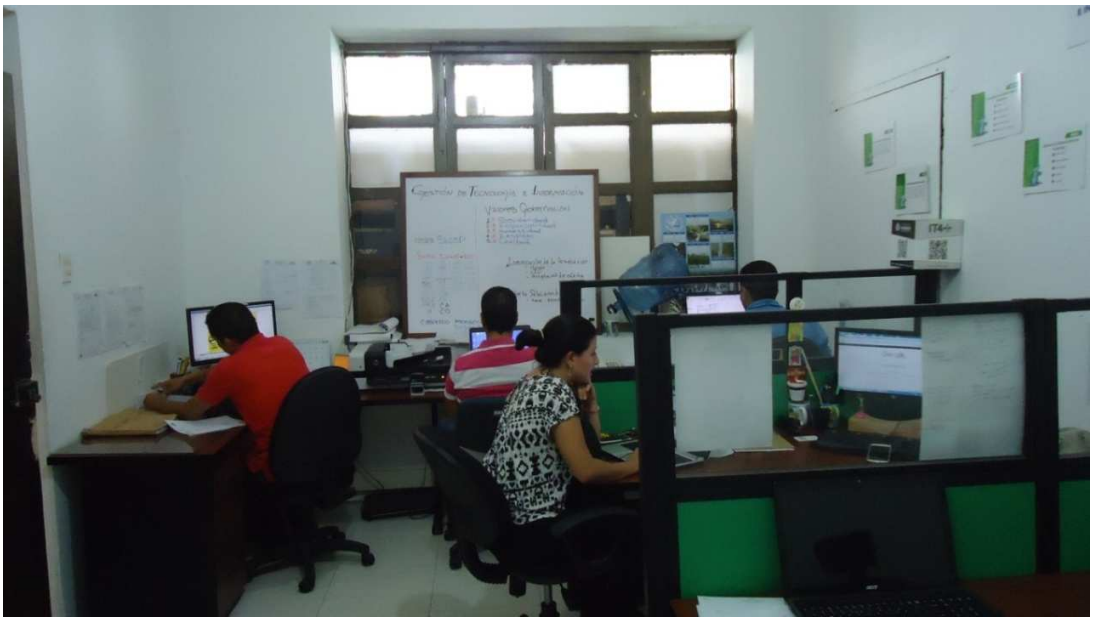
En general la Gobernación del Putumayo no cuenta con un sistema de seguridad informático establecido y tampoco cuenta con los controles y políticas definidas y documentadas que pueda brindar mayores garantías en el buen funcionamiento de sus diferentes servicios que ofrece esta importante entidad para el desarrollo de departamento del Putumayo.

Entre los principales problemas de seguridad se encuentra, el manejo de las contraseñas que habitualmente los empleados administran, teniendo en cuenta que existe un servidor de dominio configurado con directivas de contraseñas fuertes; pero por malas prácticas se evidencio en la visitas de campo que en muchos casos para fácil recordación, dejan sus contraseñas en lugares visibles; por lo que se deben empezar a concientizarlos de las vulnerabilidades y amenazas que se pueden presentar frente a estos hechos.

La empresa cuenta con un sistema de protección eléctrica (3 UPS), pero al realizar una verificación se evidencia que el tiempo de respaldo no es el adecuado y que a pesar de que existe una planta generadora de energía (20 KVA) esta puede presentar fallas de funcionamiento.

Al realizar las visitas de campo a las instalaciones de la organización se pudo evidenciar que no hay controles físicos en las áreas más críticas de la Gobernación; por lo que se deben implementar políticas para evitar manipulaciones de manera accidental tanto a los servidores como a los equipos de comunicación con los que se cuenta.

Figura 7. Oficina de Sistema

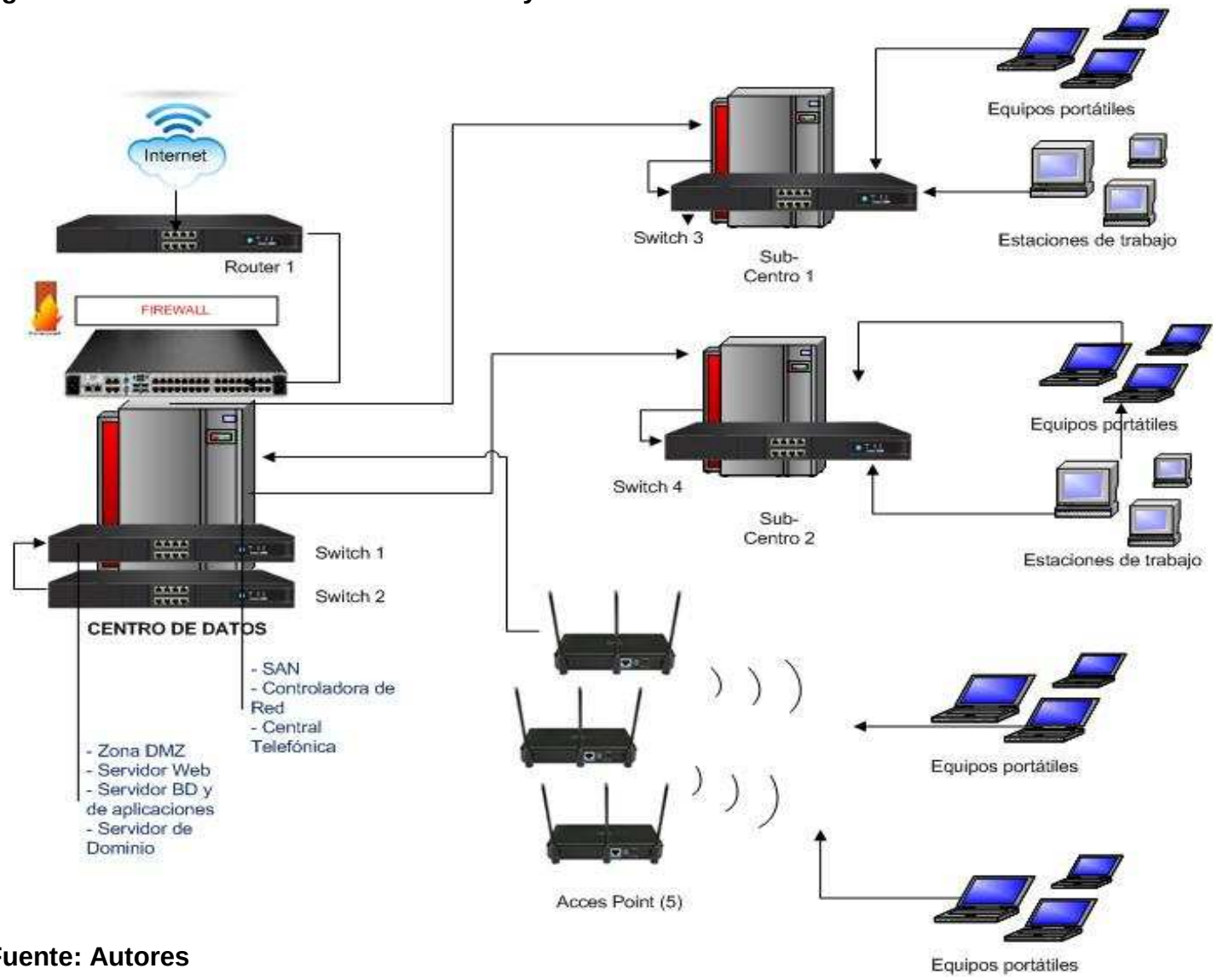


Fuente: Autores

Los funcionarios que tienen acceso a los sistemas de información también suponen un gran riesgo al mismo, ellos son los que pueden acceder a este, tanto físicamente como mediante conexión es por ellos que se realizó una entrevista a la oficina de recursos humanos y la oficina de contratación de la gobernación del Putumayo y se pudo identificar que no se tiene implementado en el documento del contrato los requisitos de seguridad informática que deben aplicar los funcionarios y tampoco se realiza procesos de inducción a los nuevos empleados en donde se les explique temáticas correspondientes a la seguridad de la información y al no estar documentado estos controles no se realizan campañas de culturización para fomentar en ellos concientización en la seguridad de la información.

A continuación se presenta un diagrama de la red donde se resume parte de la infraestructura de la Entidad:

- **Diagrama red datos Gobernación de Putumayo**



Fuente: Autores

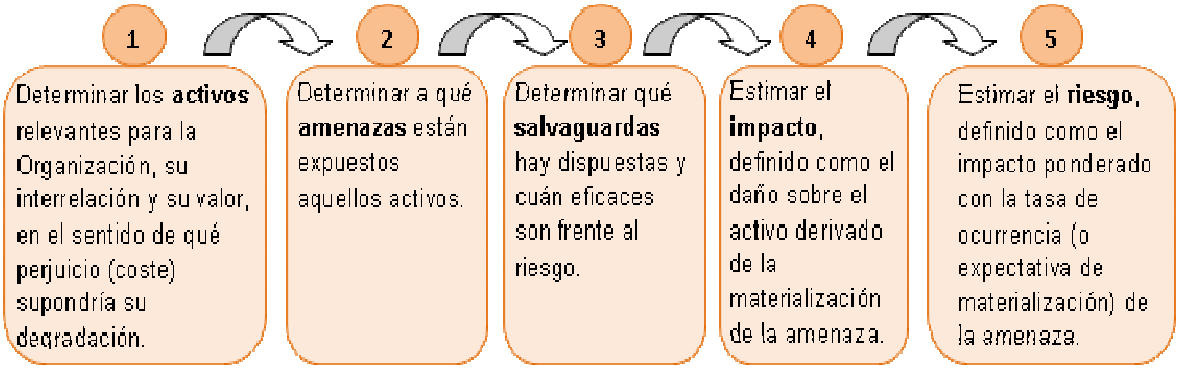
6.2 METODOLOGÍA PARA EL ANÁLISIS Y EVALUACIÓN DE RIESGOS MAGERIT / ISO 27001

Para el desarrollo del proyecto se utiliza la metodología de análisis y gestión de riesgos denominada MAGERIT, la cual fue elaborada por el Consejo Superior de Administración Electrónica de España, actualizada en 2012 a la versión 3; esta metodología contempla diferentes actividades relacionadas con los activos que tienen la organización. Esta metodología proporciona un método de evaluación y gestión del riesgo relacionada con la seguridad de la información, conforme a los requerimientos y lineamientos de los estándares internacionales en específico con la serie ISO/IEC 27000; MAGERIT busca los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. [27]

A continuación se relacionan cada uno de los pasos que se aplican según esta metodología para el análisis de riesgos, siguiendo los siguientes pasos y teniendo en cuenta un orden sistémico que permita concluir el riesgo actual en que se encuentra la Entidad:

Figura 8. Esquema de la Metodología



[27] http://administracionelectronica.gob.es

6.2.1 Inventario de activos

Actualmente la organización cuenta con los siguientes elementos, para su funcionamiento; el siguiente consolidado es el resultado de los datos de las diferentes fuentes de información entregados por la entidad (documentos de inventario de Almacén departamental) y los datos suministrados por los técnicos y demás profesionales del área de sistemas de acuerdo a las visitas realizadas:

En la tabla N° 4 se presenta la Clasificación de la información para entidades del estado, de acuerdo al Ministerio de Las TICS:

Tabla 2. Cuadro de Clasificación

Publicable	Pública no clasificada
No publicable	Top Secret, Secreta, Confidencial, Restringida
Información personal Semiprivada	Sensitiva En confianza

Fuente: Ministerio de Las TICS

6.2.1.1 Activos de Datos / Información

La información representa un activo abstracto que puede ser almacenado en los equipos de computo o soportes de información, los cuales pueden ser ficheros o bases de datos y pueden ser transferidos de un lugar a otros medios.

Tabla 3. Inventario de activos de Datos/información

INVENTARIO DE ACTIVOS					
[D] Datos / Información					
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario					
Tipo de Activo	**Nombre**	**Proceso**	**Propietario del activo**	**Clasificación de la Información**	**Áreas Asociadas**
Activos de Datos / Información	Actos administrativos	Gestión documental	Secretarias departamentales	Publicable (parcialmente)	Gobernación de Putumayo
	Datos de gestión interna	Gestión documental	Secretarias departamentales	No publicable	Gobernación de Putumayo
	Documentos contractuales (contratos, convenios)	Gestión documental Gestión de contratación	Jurídica, Contratación	Publicable	Gobernación de Putumayo
	Proyectos	Gest. Planeación.	Sec. de Planeación	Publicable (parcialmente)	Gobernación de Putumayo
	Credenciales (Contraseñas)	Gest. de tecnología e información, Gestión de comunicaciones	Sistemas	No publicable	Gobernación de Putumayo
	Copias de	Gestión de	Sistemas	No publicable	Gobernación de

	respaldo	tecnología e información,			Putumayo
	Base de datos de los sistemas de información	Gestión Hacienda. Gest. Planeación. Gest. de talento humano Gest. Gobierno	Secretarias departamentales	No publicable	Gobernación de Putumayo
	Archivo fotográfico y de video	Gestión de comunicaciones	Prensa	Publicable(parcialmente)	Despacho gobernador Sistemas, prensa
	Información página web	Gest. de tecnología e información, Gestión de comunicaciones	Sistemas	No publicable	Gobernación de Putumayo

Fuente: Autores

6.2.1.2 Servicios

En esta sección se presenta los servicios prestados por la Gobernación de Putumayo, es decir las funciones que satisfacen las necesidades de los usuarios:

Tabla 4. Inventario de activos de Servicios

INVENTARIO DE ACTIVOS					
[S] Servicios					
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario					
Tipo de Activo	**Nombre**	**Proceso**	**Propietario del activo**	**Clasificación de la Información**	**Áreas Asociadas**
Servicios	Correo electrónico		Área de sistemas	Publicable	Gobernación
	Mensajería interna (chat)		Área de sistemas	No publicable	Gobernación
	Página web		Área de sistemas	Publicable	Gobernación
	Liquidación de impuestos en línea		Rentas departamentales	Publicable (parcialmente)	Gobernación
	Consulta de pagos en línea		Secretaria de Hacienda	Publicable (parcialmente)	
	Internet		Área de sistemas	Publicable	Gobernación
	Intranet		Área de sistemas	No publicable	
	Ingreso y consultas de PQRD		Atención al usuario	Publicable	Gobernación
	Diferentes Trámites y servicios que realiza la gobernación.		Área de sistemas	No publicable	Gobernación
	Servicio VOZ/IP		Área de sistemas	-	Gobernación
	Ventanilla única		Área de sistemas	-	Gobernación

Fuente: Autores

6.2.1.3 Activos de Software /aplicaciones de informáticas

Se relaciona a continuación el software de base que usa la entidad: sistema operativo, software ofimático, software utilitario, otros:

Tabla 5. Inventario de activos de Software.

INVENTARIO DE ACTIVOS					
[SW]Software - Aplicaciones informáticas					
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario					
Tipo de Activo	**Nombre**	**Proceso (descripción)**	**Propietario del activo**	**Clasificación de la Información**	**Áreas Asociadas**
Software - Aplicaciones informáticas	PCT	Software de manejo de información contable y financiera.	Área de Hacienda.	No publicable	Contabilidad Presupuesto Almacén Tesorería
	SI Nomina	Aplicativo de manejo de nómina y pensiones.	Serv. Administrativos	No publicable	Gestión Humana Pensiones
	Liquidador Rentas	Liquidación de Estampillas	Rentas departamentales	No publicable	Área de Hacienda. Tesorería
	Gestión de PQRD	Herramienta para el manejo de Peticiones, quejas y reclamos en línea	Atención al usuario	Publicable (parcialmente)	Gobernación de Putumayo
	Gestión Documental	Aplicativo para el registro de la documentación que ingresa por la ventanilla única de la Gobernación	Ventanilla única	Publicable (parcialmente)	Gobernación de Putumayo
	SIREBPID	Manejo de información y	Área de	Publicable	Oficina del Banco de

		registros del banco de proyectos departamental. sirebpid.putumayo.gov.co	Planeación	(parcialmente)	proyectos. Presupuesto
	SISTRANP	Liquidador de Impuesto de vehículos automotores.	Área de Hacienda	Publicable	Oficina de rentas Oficina Tesorería.
	SIG	Sistema información geográfica.	Área de Planeación	Publicable	Gobernación
	ZIMBRA	Software del servidor y cliente de correo electrónico.	Área de sistemas	Publicable	Gobernación
	Aplicaciones web	Portal de la gobernación www.putumayo.gov.co	Área de sistemas	Publicable	Gobernación
	Gaceta putumayo	Herramienta web que permite la consulta de los actos administrativos de la entidad: ordenanzas, decretos, resoluciones y circulares de carácter general.	Área de sistemas	Publicable	Gobernación
	Mensajería interna Openfire y Spark.	Servidor/cliente del Sistema de mensajería instantánea GPL	Área de sistemas	Publicable	Gobernación
	SistemaIntegral de Información para la S.S.D	Compone de los siguientes módulos aseguramiento y validador de RIPS.	Secretaria de salud departamental	No publicable	Gobernación
	Sistema operativo	Windows 7 profesional	Área de sistemas	No publicable	Gobernación
	Ofimática	Office 2010	Área de	No publicable	Gobernación

			sistemas		
	Antivirus	Kaspersk Endpoint	Área de sistemas	No publicable	Gobernación
	Gestor de máquinas virtuales	VMware	Área de sistemas	No publicable	Gobernación

Fuente: Autores

6.2.1.4 Activos de Equipamiento informático (hardware)

Incluye toda infraestructura tecnológica como servidores, equipos terminales, UPS, y la red de datos:

Tabla 6. Inventario de activos Equipamiento informático

INVENTARIO DE ACTIVOS				
[HW] Equipamiento informático (hardware)				
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario				
Tipo de Activo	**Nombre**	**Proceso**	**Propietario del activo**	**Áreas Asociadas**
Equipamiento informático	Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	Servidor web – correo y DNS	Área de sistemas	Gobernación
		Servidor de Archivos	Área de sistemas	Gobernación
		Servidor SIG		Gobernación

		Servidor ViewPoint		Gobernación
		Servidor de actualizaciones		Gobernación
		Servidor de respaldo		Gobernación
		Serv. de Dominio y DHCP	Área de sistemas	Gobernación
		Serv. Aplicaciones (BD ORACLE)		Gobernación
	SAN (Storage área Network)	Equipos informáticos	Área de sistemas	Gobernación
	Equipo de cómputo (escritorio, portátil)	Equipos informáticos	Gobernación	Gobernación
	Periféricos (medios de impresión, Impresora, escáneres, etc)	Equipos informáticos	Gobernación	Gobernación
	FIREWALL Físico	Equipos informáticos	Área de sistemas	Gobernación

Fuente: Autores

6.2.1.5 Activos de Redes de comunicaciones

Incluye las instalaciones como servicios de comunicaciones contratados a terceros; en especial los medios de comunicación que llevan datos de un lugar a otro.

Tabla 7. Inventario de activos de Redes y comunicaciones

INVENTARIO DE ACTIVOS
[COM] Redes de comunicaciones
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario

	Nombre	Proceso	Propietario del activo	Áreas Asociadas
Redes de comunicaciones	Router (proveedor internet)	Redes de Comunicaciones	Área de sistemas	
	Switches	Redes de Comunicaciones	Área de sistemas	Gobernación
	Acces Point	Redes de Comunicaciones	Área de sistemas	Gobernación
	Swicth Consola KVM	Redes de Comunicaciones	Área de sistemas	Gobernación
	Rack	Redes de Comunicaciones	Área de sistemas	Gobernación
	Controladora de red (inalámbrica)	Redes de Comunicaciones	Área de sistemas	Gobernación
	Radios de enlace y Antena omnidireccional para AMO-2G10	Redes de Comunicaciones	Área de sistemas	Gobernación
	Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	Redes de Comunicaciones	Área de sistemas	Gobernación
	Central telefónica			
	Teléfonos IP	Redes de Comunicaciones	Área de sistemas	Gobernación

Fuente: Autores

6.2.1.6 Activos de Equipamiento auxiliar

En esta clase de activos se consideran otros equipos que se utilizan de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Tabla 8. Inventario de activos de Equipamiento auxiliar

INVENTARIO DE ACTIVOS				
[AUX] Equipamiento auxiliar				
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario				
	Nombre	**Proceso**	**Propietario del activo**	**Áreas Asociadas**
Equipamiento auxiliar	Totalizador, Tablero 2F-5H-120-208v	Equipamiento auxiliar	Área de sistemas	Gobernación
	Regulador de voltaje automático	Equipamiento auxiliar	Área de sistemas	Gobernación
	Estabilizador	Equipamiento auxiliar	Área de sistemas	Gobernación
	UPS	Equipamiento auxiliar	Área de sistemas	Gobernación
	Planta eléctrica	Equipamiento auxiliar		
	Aire acondicionado	Equipamiento auxiliar	Área de sistemas	Gobernación
	Cámaras IP	Equipamiento auxiliar	Área de sistemas	Gobernación

Fuente: Autores

6.2.1.7 Activos de Instalaciones

Este tipo de activos incluye las zonas donde se encuentran los sistemas de información y los equipos de comunicaciones.

Tabla 9. Inventario de activos de Instalaciones

INVENTARIO DE ACTIVOS				
[L] Instalaciones				
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario				
Tipo de Activo	**Nombre**	**Proceso**	**Propietario del activo**	**Áreas Asociadas**
	Gabinete Piso	Instalaciones	Área de sistemas	Gobernación
	Patch Panel AMP cat 6.	Instalaciones	Área de sistemas	Gobernación
	Puntos de cableado estructurado cat. 6	Instalaciones	Área de sistemas	Gobernación
	Canaleta red de voz/datos	Instalaciones	Área de sistemas	Gobernación

Fuente: Autores

6.2.1.8 Personal

En este grupo de activos hace referencia a los usuarios relacionadas con los sistemas de información: administrador sistema, administrador de red y usuarios finales.

Tabla 10. Inventario de activos de Personal.

INVENTARIO DE ACTIVOS				
[P] Personal				
Nombre del Área: Sistemas de Información Responsable: Profesional Universitario				
Tipo de Activo	**Nombre**	**Proceso (Funciones Generales)**	**Propietario del activo**	**Áreas Asociadas**
Personas	Jefe departamento de sistemas	• Administra el sistema de información central y mantener el sistema disponible para los funcionarios y usuarios. • Revisa los resultados de los procesos e incorporar acciones correctivas. • Vela porque el sistema se mantenga funcionando apropiadamente y realiza el seguimiento para detectar y corregir fallas. • Aplica las normas de seguridad y control establecidas. • Mantiene informado al jefe inmediato (Sec. Serv. Administrativos) sobre el funcionamiento del centro de cómputo.	Secretaria de Servicios Administrados	Secretaria de Servicios Administrados Oficina de Sistemas
	Operador de Base datos y aplicaciones	• Se encarga del funcionamiento normal del software con el que se cuenta para todas las dependencias.	Secretaria de Servicios Administrados	Secretaria de Servicios Administrados

		• Actualiza todos los sistemas realizando investigaciones de las nuevas tecnologías. • Realiza monitoreo del funcionamiento de las aplicaciones. • Realiza las copias de seguridad y mantenimiento de las Base de datos.		Oficina de Sistemas
	Web Máster	• Actualización y Manteamiento de los pórtales web de la entidad. • Soporte y manteamiento. del correo electrónico institucional	Secretaria de Servicios Administrados	Secretaria de Servicios Administrados Oficina de Sistemas
	Soporte técnico	• Se encarga de la instalación y configuración del software. • Planifica la modificación e instalación de nuevo software y hardware. • brinda soporte a los empleados de manera física o virtual cuando se presentan conflictos.	Secretaria de Servicios Administrados	Secretaria de Servicios Administrados Oficina de Sistemas
	Funcionarios de la Entidad	• Realizar sus actividades de acuerdo al manual de funciones.	Gobernación de Putumayo	Gobernación de Putumayo
	Usuarios /comunidad general	• Consulta de información de su interés de acuerdo a los trámites y servicios que realice,	-	-

Fuente: Autores

6.2.2 Valoración de activos

Para determinar el valor de cada activo y clasificarlos se realizó el proceso de acuerdo a la metodología MAGERIT Versión 3; en la tabla N° 7 se presenta las dimensiones de valoración tomadas del Libro II - Catálogo de Elementos:

Tabla 11. Dimensiones de Valoración

[D]	Disponibilidad
[I]	Integridad de los datos
[C]	Confidencialidad de la Información
[A]	Autenticidad
[T]	Trazabilidad

Fuente: Magerit V.3 - Libro II - Catálogo de

De igual forma se utiliza los Criterios de valoración de acuerdo a la escala estándar detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable para efectos de riesgo:

Tabla 12. Criterios de valoración.

Valor			**Criterio**
10	E	Extremo	Daño extremadamente grave
9	MA	Muy Alto	Daño muy grave
6-8	A	Alto	Daño grave
3-5	M	Medio	Daño importante
1-2	B	Bajo	Daño menor
0	D	Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

- **Valoración de Activos tipo: [D] Datos / Información**

Activo	**DIMENSIONES**				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Actos administrativos	[A]	[M]			
Datos de gestión interna	[A]	[M]			
Documentos contractuales (contratos, convenios)	[MA]	[A]		[A]	
Proyectos	[A]	[M]			
Credenciales (Contraseñas)	[M]	[MA]			

Copias de respaldo	[MA]	[MA]	[A]		
Base de datos de los sistemas de información	[MA]	[MA]	[MA]	[A]	
Archivo fotográfico y de video	[B]				
Información página web	[MA]	[A]	[A]	[A]	

- **Valoración de Activos tipo: [S] Servicios**

Activo	**DIMENSIONES**				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Correo electrónico	[A]	[M]	[M]	[A]	
Mensajería interna (chat)	[A]	[M]		[A]	
Página web	[MA]	[A]	[A]	[A]	
Liquidación de impuestos en línea	[M]	[A]	[A]	[A]	
Consulta de pagos en línea	[MA]	[M]	[A]	[A]	
Internet	[MA]				
Intranet	[A]	[A]	[A]	[MA]	
Ingreso y consultas de PQRD	[M]	[M]	[M]	[M]	
Diferentes Trámites y servicios que realiza la gobernación.	[A]				
Servicio VOZ/IP	[A]				
Ventanilla única	[A]				

- **Valoración de Activos tipo: [SW] Software - Aplicaciones informáticas**

Activo	**DIMENSIONES**				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
PCT	[MA]	[A]	[A]	[A]	
SI Nomina	[A]	[A]	[MA]	[A]	
Liquidador Rentas	[A]	[A]			
Gestión de PQRD	[M]				
Gestión Documental	[A]	[A]			
SIREBPID	[A]	[A]	[A]	[MA]	
SISTRANP	[A]	[A]			
SIG	[M]	[A]			
ZIMBRA	[MA]	[A]	[A]	[A]	
Aplicaciones web	[A]	[A]			
Gaceta Putumayo	[A]				
Mensajería interna Openfire y Spark.	[M]		[A]	[MA]	
Sistema Integral de Información para la S.S.D	[MA]	[A]			
Sistema operativo	[A]				
Ofimática	[A]				
Antivirus	[A]				

Gestor de máquinas virtuales	[A]		[M]	[M]	

- **Valoración de Activos tipo: [HW] Equipamiento informático (hardware)**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	[E]	[E]	[E]	[E]	
SAN (Storage área Network)	[E]				
Equipo de cómputo (escritorio, portátil)	[A]				
Periféricos (medios de impresión, Impresora, escáneres, etc)	[D]				
FIREWALL Físico	[MA]				

- **Valoración de Activos tipo: [COM] Redes de comunicaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Router (proveedor internet)	[MA]			[M]	
Switches	[MA]			[M]	
Acces Point	[A]				
Swicth Consola KVM	[M]				
Rack	[A]				
Controladora de red (inalámbrica)	[A]				
Radios de enlace y Antena omnidireccional para AMO-2G10	[A]				
Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	[MA]				
Central telefónica	[MA]				
Teléfonos IP	[M]				

- **Valoración de Activos tipo: [AUX] Equipamiento auxiliar**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Totalizador, Tablero 2F-5H-120-208v	[MA]				
Regulador de voltaje automático	[MA]				
Estabilizador	[MA]				
UPS	[MA]				
Planta eléctrica	[MA]				

Aire acondicionado	[A]				
Cámaras IP	[D]				

- **Valoración de Activos tipo: [L] Instalaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Gabinete Piso	[B]				
Patch Panel AMP cat 6.	[M]				
Puntos de cableado estructurado cat. 6	[A]				
Canaleta red de voz/datos	[MA]				

- **Valoración de Activos tipo: [P] Personas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Jefe departamento de sistemas	[MA]		[MA]		
Operador de Base datos y aplicaciones	[MA]		[A]		
Web Máster	[MA]		[A]		
Soporte técnico	[A]		[A]		
Funcionarios de la Entidad	[M]				
Usuarios /comunidad general	[D]				

6.2.3 Vulnerabilidades, Amenazas y Riesgos

Teniendo en cuenta la información recolectada a través de la entrevista (Anexo N° 6) y encuestas (Anexo N° 5) y también de las visitas de campo realizadas a la gobernación de Putumayo, se presenta el siguiente estudio de las amenazas, vulnerabilidades y riesgos:

6.2.3.1 Identificación las Vulnerabilidades

- **Vulnerabilidades Físicas:**

No existen controles de acceso para áreas o zonas de seguridad que sólo se permite el acceso a personal autorizado, de acuerdo a esta vulnerabilidad los activos afectados pueden ser Hardware, software y usuarios.

Dentro de las visitas de campo a la gobernación del Putumayo se identifica vulnerabilidad de acceso físicos, ya que puede acceder físicamente al sistema para robar, modificar o destruir la seguridad del mismo, este problema de seguridad se presenta por qué no se tiene implementado controles como el que los empleados deben llevar su identificación de carnet en un lugar visible, el personal de visita debe presentar su identificación y debe registrarse en el sistema de visitas ya sea sistematizado o manual y se les debe hacer entrega de su carnet de visita donde establezca que área se dirige, y se identifica que las áreas donde se encuentran los servidores, centro de cableado (áreas críticas) no están debidamente restringidas ya que puede tener la alerta de solo personal autorizado pero no cuenta con un dispositivo de seguridad que controle el acceso.

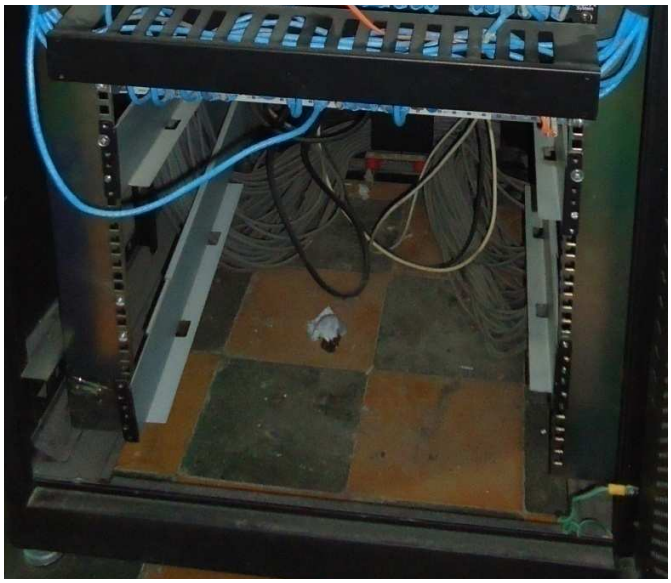
Otra vulnerabilidad que se presenta es la carencia de un centro de datos con las condiciones físicas adecuadas de acuerdo a los estándares que la norma que los regula (ANSI/TIA/EIA-568), se evidencia la falta de elementos para el combatir incendios e inundaciones, hay disposición desorganizada de cables de energía y de red, falta de vías de evacuación, puertas ignífugas, instalación de alarmas, control de humedad y temperatura, cerraduras electromagnéticas, cámaras de seguridad y pisos y techo en falso.

La protección física de los equipos informáticos o de comunicaciones de la entidad es muy importante, así como de los servidores que puedan contener información crítica y sensible, de esta manera lograr garantizar la continuidad del servicio.

Figura 9. Disposición de cables

Fuente: Autores

Figura 11. Condiciones de polvo en los gabinetes



Fuente: Autores

Figura 10. Falta de un sistema de control de acceso.

Fuente: Autores

- **Vulnerabilidades Naturales:**

Susceptibilidad a la humedad: Teniendo en cuenta la ubicación geográfica del departamento de Putumayo, situado en el sur del país presenta un nivel de humedad relativa del aire superior al 80%[28], situación que provoca que los equipos se deterioren o se afecten por este componente; de acuerdo a las visitas realizadas se evidencia que el centro de datos de la entidad no posee medidas o equipos de climatización específicos que les permitan controlar la humedad del ambiente.

Figura 12. Presencia de humedad paredes del centro de datos

Fuente: Autores

Entre algunas de las amenazas que se pueden presentar por el problema de humedad en el ambiente están las posibles descargas electroestáticas que se producen cuando la humedad baja y la corrosión que ocurre cuando un elemento metálico es expuesto al agua, ya sea porque se moja o se generan pequeñas gotas causadas por la condensación de agua en el aire, situación que ocurre cuando se presenta una humedad alta; teniendo en cuenta esta vulnerabilidad pueden ocurrir problemas de condensación en las partes electrónicas, fallas de polvo higroscópico, errores en medios de almacenamiento, problemas eléctricos, excesivo desgaste y corrosión.

[28] http://www.putumayo.gov.co/nuestro-departamento/informacion-general.html

- **Vulnerabilidad del Hardware y del software:**

Deficiencia en el Proceso de actualizaciones; de acuerdo a los datos obtenidos con el profesional del Área del sistemas se puede comprobar que la entidad no tiene implementada una política de actualización o parcheo de software de los sistemas operativos, servicios web, bases de datos y aplicaciones en general; dicha vulnerabilidad puede afectar la seguridad de los datos de la entidad y facilitar ataques efectuados por hacktivistas o por otro tipo de intrusos (Ciber delincuentes).

Es importante que los diferentes sistemas se encuentren con las últimas actualizaciones tanto a nivel de sistema operativo como en las aplicaciones de seguridad (antivirus, antimalware, etc.).

Ausencia de un eficiente control de cambios en la configuración; se evidencia que la entidad no cuenta con políticas y formatos (listas de chequeó) que les permitan registrar y gestionar de manera adecuada las nuevas configuraciones o cambios que se realicen tanto en servidores, equipos de cómputo, firewall, entre otros dispositivos que se manejan en el centro de datos.

Susceptibilidad a las variaciones de voltaje: En la zona donde está ubicada la entidad son muy frecuentes los Fallos eléctricos o picos de potencia (problemas eléctricos); a pesar de contar con 3 UPS y una planta generadora de energía eléctrica la entidad no cuenta con un raspado total de los equipos de cómputo, y la planta presenta fallas técnicas en la trasferencia automática.

Falta de cuidado en la disposición final: No existe un procedimiento definido para la eliminación, destrucción y reutilización de equipos; de acuerdo al estudio realizado se evidencia que la entidad no posee procesos documentados sobre cómo realizar la destrucción de los equipos de cómputo y medios que ya no se usen.

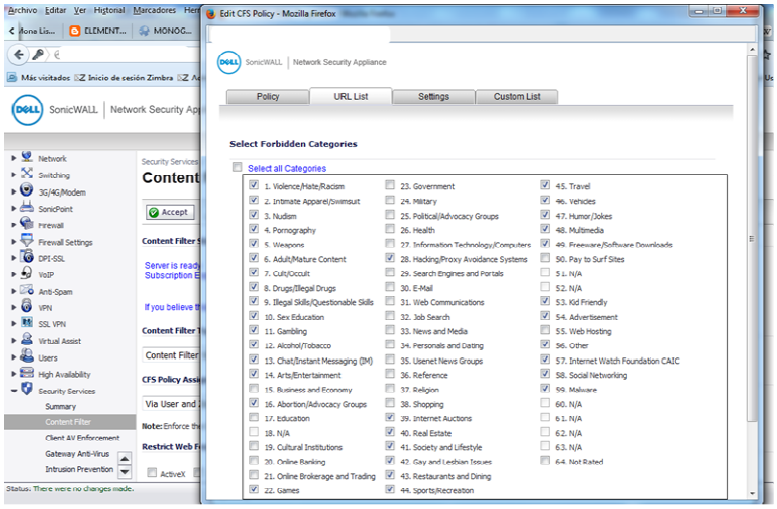
- **Vulnerabilidad de los Medios o Dispositivos:**

Disposición o reutilización de los medios de almacenamiento sin borrado adecuado: No existe un proceso definido y claro para la devolución de activos tecnológicos que estén a cargo de los empleados, contratistas al finalizar su vinculación laboral, contrato o convenio.

- **Vulnerabilidad de las Comunicaciones:**

Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería: se evidencia la falta de medidas y soportes que reglamenten estos servicios por ejemplo en el servicio de internet que se provee a los funcionarios, es importante mencionar que la entidad cuenta con un dispositivo firewall que les permite controlar los sitios web, servicios y puertos permitidos pero no cuentan con políticas formales que fortalezcan el proceso; según la fuente consultada este actividad se realiza de acuerdo a las necesidades diarias.

Figura 13. Pantallazo de configuración de categorías firewall físico



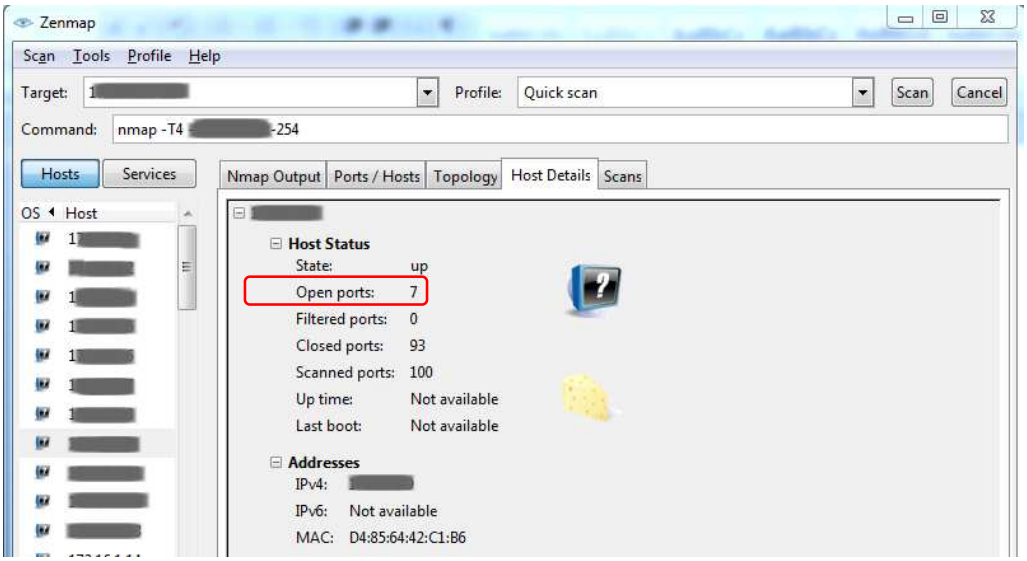
Fuente: Autores

No se aplica periódicamente pruebas de red con Sniffer (Analizador de paquetes) o alguna herramienta que les permita el diagnóstico remoto y la revisión de la configuración de puertos y el tráfico de la red de datos.

De acuerdo a las pruebas efectuadas con la aplicación Zenmap, permitió realizar una verificación de seguridad en la red mediante el análisis de los puertos abiertos en servidores y equipos de cómputo.

En la siguiente imagen se evidencia que el host analizado tiene 7 puertos abiertos, por seguridad no se indica cuales son:

Figura 14. Software Zenmap en ejecución



Fuente: Autores

Existen algunos puertos más vulnerables que pueden ser explotados por atacantes, teniendo en cuenta los servicios que corren por dichos puertos, entre los más conocidos y usados están los siguientes:

Tabla 13. Puertos vulnerables

Puerto	Protocolo	Servicio	Vulnerabilidad
21	TCP	FTP	✓ Buffer Overflow ✓ Denegación de Servicio (DoS) ✓ Ataque de Fuerza Bruta ✓ Punto de Acceso
22	TCP	SSH	✓ Buffer Overflow ✓ Ataque de Fuerza Bruta. ✓ Punto de Acceso
23	TCP	Telnet	✓ Buffer Overflow ✓ Denegación de Servicio (DoS) ✓ Ataque de Fuerza Bruta ✓ Punto de Acceso ✓ Posibilidad de sniffer
80	TCP	HTTP	✓ Ataque CGI ✓ Buffer Oveflow ✓ Denegación de Servicio (DoS)

			✓ Recogida de Información ✓ Punto de Acceso ✓ Posibilidad de sniffer.
139	TCP/UDP	Net Biosssn	✓ Denegación de Servicio (DoS) ✓ Ataque de Fuerza Bruta ✓ Punto de Acceso ✓ Recogida de Información
3389	TCP	Microsoft Windows NT Terminal Server	✓ Denegación de Servicio (DoS)

Fuente: http://dmrodriguez.50megs.com/portvulnerability.htm

- **Vulnerabilidades al recurso humano:**

Falta de compromiso de la dirección con la seguridad de la información: Es evidente que al ser una entidad Pública el tema no es prioridad para los mandatarios a pesar de estar incluido como componente de la estrategia de Gobierno en Línea que se convierte en una política pública de obligatorio cumplimiento para las entidades del estado.

Capacitaciones insuficiente en temas de seguridad: Según datos retomados de las preguntas de la encuesta aplicada a los funcionarios de la entidad, existe nula aplicación de procesos concienciación y educación sobre la seguridad de la información a los funcionarios y contratistas de la entidad, tanto en actualizaciones sobre las políticas y los procedimientos de la entidad como también de la aplicación de buenas prácticas de acuerdo a sus funciones laborales.

La mayoría de los funcionarios no realiza el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas; se evidencio que esta es unas de las vulnerabilidades más altas ya que a pesar de la complejidad de las contraseñas configuradas con las directivas del servidor de dominio las personas escriben las contraseñas en sitios visibles o de fácil acceso.

Los identificadores (ID's) no son removidos del sistema cuando un empleado es despedido.

6.2.3.2 Amenazas: Identificación y valoración

De acuerdo a la metodología usada para este proceso las amenazas se clasifican en cuatro (4) grupos:

Tabla 14. Clasificación amenazas

Código	Grupo	Descripción	Origen
[N]	Desastres naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.	Natural (accidental)
[I]	De origen industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	Entorno (accidental) Humano (accidental o deliberado)
[E]	Errores y fallos no intencionados	Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.	Humano (accidental)
[A]	Ataques intencionados	Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.	Humano (deliberado)

Fuente: Magerit V.3

Para el desarrollo de este proceso se han tomado las amenazas del catálogo de elementos que presenta la metodología MAGERIT en su libro II Versión 3.0 bajo la aplicación de la herramienta Pilar versión 5.4.5, teniendo en cuenta la siguiente tabla de rangos para la evaluación de la frecuencia:

Tabla 15. Rango frecuencia de amenazas

Frecuencia			Criterio	
4	Muy frecuente	MF	A diario	MA
3	Frecuente	F	Mensualmente	A
2	Normal	FN	Una vez al año	M
1	Poco frecuente	PF	Cada varios años	B

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

Para determinar la degradación de cada activo se procede a evaluar el valor que pierde el activo (en porcentaje) en caso que se materialice una amenaza.

Tabla 16. Valor de la degradación

Valor	Criterio	
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del activo
10	B	Degradación BAJA del activo
1%	MB	Degradación MUY BAJA del activo

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

Tabla 17. Amenazas posibles sobre los activos deInformación/Datos.

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
	[I.3] Contaminación mecánica	FN	A	A			
	[I.5] Avería de origen físico o lógico	FN	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	PF	A				
	[E.1] Errores de los usuarios	F	M	M			
	[E.2] Errores del administrador	FN	M	M			
	[E.15] Alteración accidental de la información	FN		B			

	[E.18] Destrucción de información	FN	B				
	[E.19] Fugas de información	F			M		
	[A.11] Acceso no autorizado	MF		M			

Justificación de las amenazas - [D] Información/Datos

[I.3] Contaminación mecánica: Los activos de información de datos físicos pueden verse afectados de manera alta su disponibilidad por daños causados por polvo o suciedad.

[I.5] Avería de origen físico o lógico: Una falla de los equipos o en los programas puede afectar en una escala Alta la disponibilidad de los activos de datos lógicos.

[I.7] Condiciones inadecuadas de temperatura o humedad: Las condiciones inadecuadas de temperatura pueden afectar de manera alta la disponibilidad por que pueden causar daños en los archivos físicos e interrumpir la continuidad del proceso.

[E.1] Errores de los usuarios: Los empleados de la gobernación pueden afectar la información por falta de capacitación en los procesos y mecanismos adecuados de inducción.

[E.2] Errores del administrador: El administrador puede afectar de manera mediana la integridad y la disponibilidad de la información, debido a que este tiene privilegios avanzados sobre estos activos.

[E.15] Alteración accidental de la información: El personal de la gobernación del Putumayo manifiesta que por motivos ajenos a su voluntad han alterado documentos de la entidad, afectando de manera baja la integridad de la misma.

[E.18] Destrucción de información: En los procesos de recolección de información realizados se puede evidenciar que información sensible se ha eliminado por accidente, perjudicando de una forma baja la disponibilidad de esta.

[E.19] Fugas de información: La entidad no plantea dentro de sus reglamentos o dentro de su proceso contractual las cláusulas de confidencialidad, por este hecho hay fugas de información que afectan de manera mediana la confidencialidad de la información.

[A.11] Acceso no autorizado: Uno de los problemas es el préstamo de contraseñas permitiendo el acceso no autorizado de personal no custodio ni propietario de la información a estos activos vulnerando de forma mediana la integridad de la información.

Tabla 18. Amenazas posibles sobre los activos de Servicios

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
[S] Servicios	[E.1] Errores de los usuarios	F	M	M	M		
	[E.2] Errores del administrador	FN	M	M	M		
	[E.15] Alteración de la información	FN		B			
	[E.20] Vulnerabilidades de los programas	FN	A				
	[A.5] Suplantación de la identidad del usuario	FN		A	A	MA	
	[A.8] Difusión de software dañino	F	A	M	M		
	[A.24] Denegación de servicio	PF	A				
	[A.7] Uso no previsto	F	B	M	M		
	[I.8] Fallo de servicios de comunicaciones	FN	M				
	[A.11] Acceso no autorizado	FN		M	A	MA	

Justificación de las amenazas - [S] Servicios

[E.1] Errores de los usuarios: Se considera que la afectación de esta amenaza es mediana y se presenta de manera frecuente, debido a que los errores de los usuarios pueden ocasionar perdida de acceso al servicio.

[E.2] Errores del administrador: Se considera que la afectación de esta amenaza es mediana y se presenta con una frecuencia normal, el administrador puede realizar un proceso de inadecuado sobre los activos de servicios perjudicando la confidencialidad, la integridad y la disponibilidad de la información.

[E.15] Alteración de la información: Se considera que la afectación de esta amenaza es baja con respecto a la integridad de la información, se puede presentar con una frecuencia normal, se puede dar la posibilidad de que los funcionarios modifiquen la información de la entidad intencionalmente o de manera accidental.

[E.20] Vulnerabilidades de los programas: Se considera que la frecuencia de esta amenaza es normal pero la afectación si llegara a presentarse seria alta, esto porque la entidad dispone de varios programas que van direccionados a la prestación del servicio.

[A.5] Suplantación de la identidad del usuario: Esta amenaza está considerada de alto grado en su dimensión de integridad y autenticidad, la entidad no tiene políticas de seguridad fuertes con respecto al no compartir contraseñas y programaciones periódicas de cambios de las mismas.

[A.8] Difusión de software dañino: Esta amenaza afecta de manera frecuente los activos de servicios, debido a que no se dispone de controles para el uso de memorias y medios de almacenamiento externo, estos se convierten en medios de trasmisión de software dañino a las herramientas de servicios.

[A.24] Denegación de servicio: Se ha realizado la evaluación de esta amenaza como alta en la dimensión de la disponibilidad, este tipo de amenaza bloquea por completo los sistemas y herramientas de servicio y su presentación dentro de la empresa es poco frecuente.

[A.7] Uso no previsto: La frecuencia de esta amenaza es frecuente pero la afectación del uso de las herramientas de servicio como el uso del internet para otros fines afectan de manera mediana la degradación del activo.

[I.8] Fallo de servicios de comunicaciones: Aunque la frecuencia de esta amenaza se cataloga como normal, su afectación en cuando a la degradación de la

disponibilidad es mediana. Las herramientas de comunicaciones son la base para la prestación de servicio en la entidad.

[A.11] Acceso no autorizado: La frecuencia de esta amenaza está catalogada como normal por el sistema de firewall que apoya mucho en su no materialización, pero si se presentara afectaría gravemente la confidencialidad del activo de información de servicios.

Tabla 19. Amenazas posibles sobre los activos de Software - Aplicaciones informáticas

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
[SW] Software - Aplicaciones informáticas	[I.5] Avería de origen físico o lógico	FN	A				
	[E.1] Errores de los usuarios	F	B	M	M		
	[E.2] errores del administrador	FN	M	M	M		
	[E.4] Errores de configuración	FN	MA				
	[E.8] Difusión de software dañino	F	M	M	M		
	[E.14] Escapes de información	F		M	A		
	[E.20] Vulnerabilidades de los programas (software	FN	B	M	M		
	[E.21] Errores de mantenimiento / actualización de programas (software)	F	B	B			
	[A.5] Suplantación de la identidad	FN		A	A	MA	
	[A.11] Acceso no autorizado	FN		M	A		
	[A.15] Modificación deliberada de la información	FN		A			

Justificación de las amenazas - [S] Software – Aplicaciones informáticas

[I.5] Avería de origen físico o lógico: Se establece que se puede presentar de forma recurrente, se presentan fallas ocasionales de las maquinas donde se encuentran los aplicativos esto afecta de manera alta la disponibilidad.

[E.1] Errores de los usuarios: Dentro del análisis de esta amenaza se establece que se puede presentar de forma frecuente, y que los usuarios afectan de manera baja la disponibilidad, al bloquear los aplicativos por falta de conocimiento.

[E.2] Errores del administrador: se considera que la afectación de este activo en cuanto a la disponibilidad es mediana, aunque su evaluación de la frecuencia es normal, puede perjudicar de manera crítica los sistemas de información de la entidad.

[E.4] Errores de configuración: La dimensión de esta amenaza afecta directamente la disponibilidad y se considera muy alta porque un problema de configuración puede afectar gravemente los sistemas de información de la Entidad.

[E.8] Difusión de software dañino: Se considera que la afectación de este activo en cuanto a la disponibilidad, integridad y la confidencialidad es media, y se puede presentar de manera frecuente, se da por la propagación de software dañino como gestores de descarga p2p y programas con códigos maliciosos.

[E.14] Escapes de información: Esta amenaza se presenta de manera frecuente y afecta en mayor proporción la confidencialidad por no haber reglamentos estipulados ni acuerdos de confidencialidad de la entidad.

[E.20] Vulnerabilidades de los programas (software): La posibilidad de esta amenaza está catalogada como normal, se presenta por fallas de seguridad en los programas, porque no se establecen parches de seguridad para solucionar posibles fallas, si se plasmará afectaría de manera media la integridad y la confidencialidad del activo de información.

[E.21] Errores de mantenimiento / Actualización de programas (software): Se considera que esta amenaza afecta de manera frecuente el activo y afecta de manera baja la disponibilidad de los sistemas, un mal procedimiento en el

mantenimiento de un programa o la actualización del mismo puede dañar su funcionamiento.

[A.5] Suplantación de identidad: Esta amenaza se puede efectuar con una frecuencia normal y si se plasmara afectaría de forma muy alta la autenticidad del activo y en menor proporción la integridad y confidencialidad de la información, esta amenaza se puede presentar en la entidad gracias al sistema de copias de seguridad se puede restablecer la información pero se requiere de controles para mitigar los accesos de personal ajeno.

[A.11] Acceso no autorizado: Esta amenaza se puede efectuar con una frecuencia normal y afecta de forma muy alta la confidencialidad de la información, si un intruso logra acceder a los sistemas críticos de la entidad puede dañar la imagen y revelar información sensible.

[A.15] Modificación deliberada de la información: Esta amenaza afecta la dimensión de la integridad de manera alta, ocurre por qué no se tienen establecidas validaciones estricticas en los sistemas para la modificación de la información por personal adecuado, y se puede efectuar según el análisis con una frecuencia normal.

Tabla 20. Amenazas posibles sobre los activos de Equipamiento informático.

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
[HW] Equipamiento informático (hardware)	[N.*] Desastres naturales	PF	MA				
	[I.5] Avería de origen físico o lógico	PF	A				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FN	A				
	[A.11] Acceso no autorizado	PF		A	MA		
	[A.22] Manipulación de los equipos	FN	M	A	A		
	[I.6] Corte del suministro eléctrico	F	A				
	[I.7] Condiciones inadecuadas de temperatura o humedad	FN	A				

	[E.2] Errores del administrador	FN	A	M	M		
	[E.25] Pérdida de equipos	PF	MA		MA		
	[A.25] Robo	PF	MA		MA		

Justificación de las amenazas - [HW] Equipamiento informático (hardware)

[N.*] Desastres naturales: Aunque la amenaza está evaluada como poco frecuente, la afectación en el equipamiento afectaría de manera muy alta la disponibilidad del hardware, esta amenaza dejaría los equipos sin servicio.

[I.5] Avería de origen físico o lógico: La afectación de la disponibilidad se considera alta, se puede afectar los servicios si el hardware presenta fallas por defectos de fábrica o de origen.

[E.23] Errores de mantenimiento / actualización de equipos (hardware): Esta amenaza tiene una evaluación de alto impacto, a pesar que se cuenta con una persona capacitada para realizar esta actividad no se tiene planes de mantenimiento periódicos a los equipos de la entidad, solo se atienden los que presenten fallas.

[A.11] Acceso no autorizado: La valoración de la amenaza afecta de manera muy alta la confidencialidad de la información, al tener acceso al hardware sin autorización se pueden provocar daños y manipulaciones que afecten este activo.

[A.22] Manipulación de los equipos: La degradación de esta amenaza es alta con respecto a la Integridad y la confidencialidad, en especial si se efectúa en dispositivos o equipos que tienen información sensible, la entidad no tiene políticas de uso exclusivo del personal para la manipulación de los equipos.

[I.6] Corte del suministro eléctrico: La evaluación de esta amenaza está catalogada como alta y afecta la disponibilidad de los equipos, en la región son constantes la interrupción del servicio eléctrico y en la entidad no hay sistemas de respaldos suficientes para garantizar la continuidad del servicio.

[I.7] Condiciones inadecuadas de temperatura o humedad: La degradación de esta amenaza afecta de manera directa la disponibilidad del activo de hardware, y es más sensible en las áreas donde se encuentran los servidores porque en esta se tienen aires acondicionados pero no tiene controles de cambios de temperatura y humedad.

[E.2] Errores del administrador: La frecuencia de esta amenaza está catalogada como normal y afecta en mayor medida la integridad del activo, se puede presentar casos que el administrador del sistema de forma inconsciente realice fallos en el hardware y así no permitir la disponibilidad del sistema.

[E.25] Pérdida de equipos: Para la evaluación de esta amenaza se considera que efectúa decremento sobre la confidencialidad y la disponibilidad del activo, aunque su frecuencia se evalúa como poca, se puede presentar perdida de equipos por la no implementación de políticas de control y revisión del personal interno y externo de la entidad.

[A.25] Robo: esta amenaza se puede presentar como poco frecuente pero afectaría de manera MUY ALTA la confidencialidad del activo de información, se puede presentar robos de los equipos de la entidad por la falta de políticas de control y revisión del personal interno y externo de la entidad.

Tabla 21. Amenazas posibles sobre los activos de Redes de comunicaciones

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
[COM] Redes de comunicaciones	[N.*] Desastres naturales	PF	MA				
	[I.1] Fuego	PF	MA				
	[I.5] Avería de origen físico o lógico	FN	A				
	[I.8] Fallo de servicios de comunicaciones	FN	A				
	[E.2] Errores del administrador	FN	M				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FN	M				

	[A.23] Manipulación del hardware	FN	MA				
	[A.24] Denegación de servicio	FN	MA				
	[A.26] Ataque destructivo	FN	MA				

Justificación de las amenazas - [COM] Redes de comunicaciones

[N.*] Desastres naturales: Se considera que es muy poco probable que se efectué, pero si se llegara a presentar afectaría de manera MUY ALTA la disponibilidad de los activos de comunicaciones, porque se perderían todos los servicios llevando a una paralización completa de las actividades de la entidad.

[I.1] Fuego: Se considera que es muy poco probable que se efectué, pero si se llegara a presentar afectaría de manera MUY ALTA la disponibilidad de los activos de comunicaciones, porque se perderían todos los servicios llevando a una paralización completa de las actividades de la Administración Departamental.

[I.5] Avería de origen físico o lógico: Esta amenaza está considerada que se puede presentar con regularidad, y afecta la disponibilidad del activo de manera ALTA, se pueden presentar averías en los dispositivos de comunicaciones por que las zonas donde fueron instalados no cumplen con todos los requerimientos para que estos funcionen correctamente.

[I.8] Fallo de servicios de comunicaciones: La evaluación de esta amenaza está considerada que afecta de manera ALTA la disponibilidad del activo, los fallos en los servicios de redes de comunicaciones se presentan por causas internas como fallas en los Routers, switches o externas como fallas en el proveedor del servicio contratado.

[E.2] Errores del administrador: Los errores causados por el administrador puede llegar a afectar de manera media la disponibilidad del activo así como en menor proporción la integridad y la confidencialidad, además existen equipos que no permiten administración porque son responsabilidad del operador contratado para este servicio.

[E.23] Errores de mantenimiento / actualización de equipos (hardware): Esta amenaza está considerada que se puede presentar con regularidad, y afecta la disponibilidad del activo en forma media, Esta amenaza se puede dar por falta de capacitación de soporte técnico para la manipulación de algunos elementos de comunicaciones que posee la gobernación.

[A.23] Manipulación del hardware: Esta amenaza está considerada que se puede presentar de forma normal, y puede llegar a afectar de manera muy alta la disponibilidad del activo, está muy ligada con la amenaza de Errores de mantenimiento, porque al hacer el mantenimiento de los equipos se manipula el Hardware y por la falta de capacitación de soporte técnico para la manipulación de algunos elementos de comunicaciones se pueden presentar afectaciones en el activo.

[A.24] Denegación del servicio: Esta amenaza se está catalogada que puede presentarse con una frecuencia normal. Esta se puede presentar una vez al año y su afectación está dada de manera MUY ALTA el dominio de la disponibilidad, un ataque de denegación de servicio deja los sistemas colapsados, afectando la continuidad del servicio de la entidad.

[A.26] Ataque destructivo: Esta amenaza se está catalogada que se puede presentar de manera normal, pero si llegara a materializarse afectaría de manera MUY ALTA para el dominio de la disponibilidad, por la ubicación de la entidad cerca de las fuerzas militares representa un riesgo que no se puede dejar de evaluar.

Tabla 22. Amenazas posibles sobre los activos de Equipamiento auxiliar

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
[AUX] Equipamiento auxiliar	[N.*] Desastres naturales	PF	MA				
	[I.1] Fuego	PF	MA				
	[I.2] Daños por agua	PF	A				
	[I.5] Avería de origen físico o lógico	FN	A				
	[I.6] Corte del suministro eléctrico	F	A				
	[I.7] Condiciones inadecuadas de	FN	A				

	temperatura o humedad						
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FN	M				
	[A.11] Acceso no autorizado	PF		A	MA		
	[A.23] Manipulación del hardware	FN	A				

Justificación de las amenazas - [AUX] Equipamiento auxiliar

[N.*] Desastres naturales: La materialización de esta amenaza afectaría de forma MUY ALTA la disponibilidad del activo de equipamiento auxiliar, los lugares donde se encuentran estos equipos pueden sufrir serios daños y pérdidas, lo que no garantiza la continuidad del servicio, aunque la valoración de la frecuencia está dada como poco frecuente se deben tomar medidas de control para evitar la materialización.

[I.1] Fuego: Se considera que la frecuencia en la que se puede presentar esta amenaza es poco frecuente, pero afectaría de manera MUY ALTA la disponibilidad del activo, aunque existen algunos extintores en la entidad estos no están ubicados teniendo en cuenta el estudio que debe realizar una entidad competente y no poseen sistemas de bombeo de agua para suplir la necesidad en caso de presentarse un incendio.

[I.2] Daños por agua: La degradación por esta amenaza es considerada ALTA en cuanto a la disponibilidad, puede presentarse una rotura en los ductos de agua que pasan por los lugares donde están ubicados estos activos y los aires pueden presentar goteos que a largo tiempo pueden dañar las UPS, todo esto por la no programación de mantenimientos periódicos sobre estos elementos de apoyo.

[I.5] Avería de origen físico o lógico: Tomando con referencia el análisis del periodo de presentación de esta amenaza se ha definido que se puede presentar con una frecuencia normal, La degradación que puede presentarse en cuanto a esta amenaza es ALTA, afectando la disponibilidad de este activo; porque las zonas donde se encuentran no están definidas como exclusivas, es decir algunas

tienen otras funciones como almacenamiento de otros equipos obsoletos, cajas, y material que puede dañar los equipos auxiliares.

[I.6] Corte del suministro eléctrico: La afectación de esta amenaza degrada la disponibilidad del activo de manera Alta, en las instalaciones se presentan cortes eléctricos provocados por la empresa que suministra el servicio y durante este tiempo la entidad no posee un sistema de respaldo bien estructurado para garantizar la prestación del servicio, esta amenaza se puede presentar de manera frecuente lo que agrava aún más la afectación de la dimensión del activo.

[I.7] Condiciones inadecuadas de temperatura o humedad: Se considera que la frecuencia con la que esta amenaza se puede presentar es normal, y afecta la disponibilidad del activo de forma ALTA, la justificación para esto, se debe a que en la entidad no se encuentran los equipos auxiliares bajo las condiciones de temperatura y humedad adecuadas permitiendo así que se materialice la amenaza.

[E.23] Errores de mantenimiento / actualización de equipos (hardware): Al presentarse este tipo de amenaza afectaría la disponibilidad de forma ALTA, se han presentado casos que los mantenimientos o actualizaciones no realizadas por el personal idóneo ha provocado daños y fallos en los equipos auxiliares interrumpiendo la continuidad del servicio.

[A.11] Acceso no autorizado: La valoración de la amenaza afecta de manera MUY ALTA la confidencialidad de la información, al tener acceso a cajas fuertes sin autorización se pueden provocar pérdidas de información y someter a la entidad a procesos judiciales, el análisis de periodicidad con la que esta amenaza se puede presentar se determina como poco frecuente.

[A.23] Manipulación del hardware: Esta amenaza se puede presentar de manera normal y la degradación que puede presentarse es ALTA, afectando la disponibilidad de este activo; los equipos auxiliares en algunos casos son muy complejos y no pueden ser manipulados por el personal técnico de la Gobernación.

Tabla 23. Amenazas posibles sobre los activos de Instalaciones

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
[L] Instalaciones	[N.*] Desastres naturales	FN	MA				
	[I.1] Fuego	FN	MA				
	[I.2] Daños por agua	FN	MA				
	[A.26] Ataque destructivo	PF	MA				

Justificación de las amenazas - [L] Instalaciones

[N.*] Desastres naturales: La materialización de esta amenaza afectaría de forma MUY ALTA la disponibilidad de las instalaciones, su ocurrencia está catalogada como normal, porque existe el riesgo de avalanchas en el municipio de Mocoa según informe de las autoridades competentes, además la zona cuenta con climas muy inestables por estar ubicado en la región amazónica.

[I.1] Fuego: Se considera que la frecuencia en la que se puede presentar esta amenaza es normal, pero afectaría de manera MUY ALTA la disponibilidad del activo, existen algunos extintores en la entidad pero estos no están ubicados de forma correcta, el personal no está capacitado para su uso, y no poseen sistemas de bombeo de agua para suplir la necesidad en caso de presentarse un incendio.

[I.2] Daños por agua: La degradación por esta amenaza es considerada ALTA en cuanto a la disponibilidad, puede presentarse una rotura en los ductos de agua que pasan por los lugares donde están ubicados los archivos de información y los aires pueden presentar goteos que a largo tiempo pueden dañar las instalaciones a largo plazo.

[A.26] Ataque destructivo: La degradación afectaría de manera MUY ALTA la disponibilidad de las instalaciones, aunque se tiene una evaluación de frecuencia muy poca, la instalaciones de la gobernación está ubicada junto al comando principal de la policía nacional, y corre el riesgo de ser blanco de atentados.

Tabla 24. Amenazas posibles sobre los activos de Personal

Tipo Activo	Amenazas	Frecuencia	Dimensiones				
			[D]	[I]	[C]	[A]	[T]
[P] Personas	[E.7] Deficiencias en la organización	F	A				
	[E.15] Alteración accidental de la información	FN		M			
	[A.30] Ingeniería social (picaresca)	FN	A	MA	MA		
	[E.19] Fugas de información	FN			M		
	[E.28] Indisponibilidad del personal	FN	M				
	[A.29] Extorsión	FN	A	MA	MA		

Justificación de las amenazas - [P] Personas

[E.7] Deficiencias en la organización: Esta amenaza está considerada como frecuente y afectaría de manera ALTA la disponibilidad de la información requerida, esto se debe a que la entidad está iniciando la implementación del sistema de gestión por procesos, maneja una planta global y algunos funcionarios realizan tareas que no están estipuladas en sus funciones o contratos.

[E.15] Alteración accidental de la información: La degradación de esta amenaza afecta de manera media la integridad de la información. El personal de la gobernación del Putumayo manifiesta que por motivos ajenos a su voluntad han alterado documentos de la entidad y se detecta que este proceso se repite varias veces.

[A.30] Ingeniería social (picaresca): La degradación de esta amenaza afecta de manera MUY ALTA la confidencialidad de los activos de información, en la entidad no se han realizado campañas de socialización para concientizar a los funcionarios que existen este tipo de ataques y que pueden ser muy perjudicial si esto se materializa.

[E.19] Fugas de información: La materialización de esta amenaza afecta medianamente la confidencialidad de la información, dentro de su proceso

contractual la entidad no plantea claramente las cláusulas de confidencialidad y tampoco el personal no tiene claro que la información que disponen está clasificada como confidencial.

[E.28] Indisponibilidad del personal: El análisis de esta amenaza se da con una frecuencia normal, esto se debe a que los permisos de los usuarios para ausentarse de su lugar de trabajo son constantes además no se tiene implementado metodologías de personal de respaldo para hacer las funciones críticas del personal ausentado.

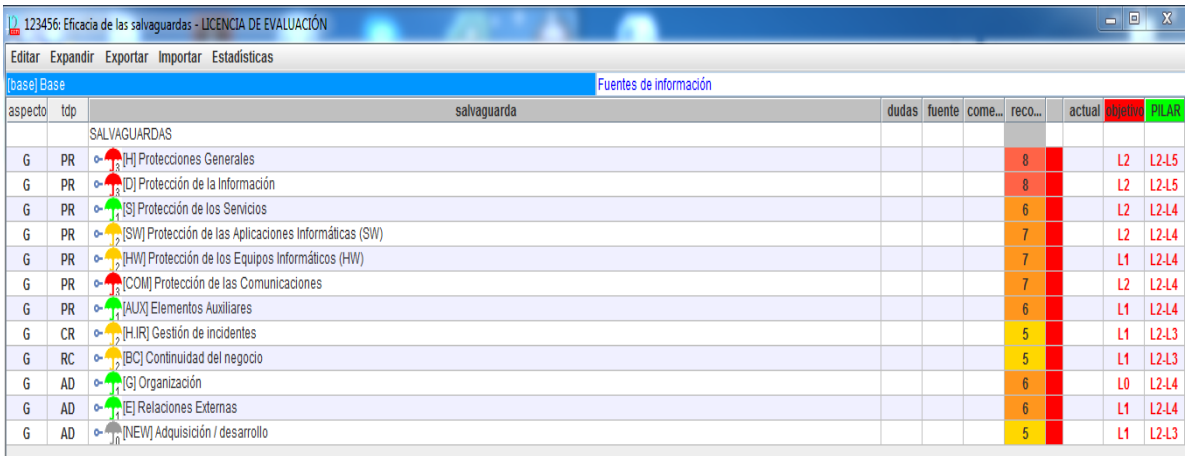
[A.29] Extorsión: La materialización de esta amenaza degrada de manera MUY ALTA la confidencialidad de la información y en menor escala la integridad y disponibilidad. Se han reportado casos de extorción dentro de la entidad y se han tomado las medidas correctivas correspondientes, pero este caso se debe a la materialización de otras amenazas como la fuga de información y acceso no autorizado.

6.2.3.3 Descripción salvaguardas (Identificación y Valoración)

Las salvaguardas o contramedidas reducen el grado de afectación de las amenazas y se definen según Magerit, como aquellos “procedimientos o mecanismos tecnológicos que reducen el riesgo”; teniendo en cuenta que la Gobernación de Putumayo cuenta con algunas medidas (salvaguardias) estas también se contemplan dentro del proceso de análisis de riesgos.

Para el desarrollo de este proceso se tiene en cuenta la relación de salvaguardas para cada grupo de activos que presenta metodología Magerit v 3.0 En el libro II, catálogo de elementos y se presenta a continuación el resumen de las salvaguardas tomadas del proyecto desarrollado en la herramienta EAR PILAR - Análisis y Gestión de Riesgos.

Figura 15. Evidencia del proyecto desarrollado en la herramienta PILAR



aspecto	tdp	salvaguarda	dudas	fuente	come...	reco...	actual	objetivo	PILAR
		SALVAGUARDAS							
G	PR	[H] Protecciones Generales				8		L2	L2-L5
G	PR	[D] Protección de la Información				8		L2	L2-L5
G	PR	[S] Protección de los Servicios				6		L2	L2-L4
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7		L2	L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7		L1	L2-L4
G	PR	[COM] Protección de las Comunicaciones				7		L2	L2-L4
G	PR	[AUX] Elementos Auxiliares				6		L1	L2-L4
G	CR	[H.IR] Gestión de incidentes				5		L1	L2-L3
G	RC	[BC] Continuidad del negocio				5		L1	L2-L3
G	AD	[G] Organización				6		L0	L2-L4
G	AD	[E] Relaciones Externas				6		L1	L2-L4
G	AD	[NEW] Adquisición / desarrollo				5		L1	L2-L3

Fuente: Proyecto Herramienta de Análisis de riesgos - PILAR (5.4.5)

Valoración de Salvaguardas:

Así como se estimaron las amenazas para cada activo de información, en el siguiente proceso se evalúan las salvaguardas que existen en la Entidad de acuerdo al valor de los activos y la frecuencia e impacto de las amenazas, teniendo en cuenta cada una de sus dimensiones: Autenticidad, Confiabilidad, Disponibilidad, Integridad, y Trazabilidad.

Para proceder a valorar las medidas existentes en la Entidad se aplica la escala dispuesta por la herramienta PILAR en la cual se evalúa los niveles de madurez de implementación y el grado de efectividad de dichas de las medidas de seguridad.

Tabla 25. Nivel y efectividad de salvaguardas

Nivel	Descripción	Efectividad
L0	Inexistente	**0%**
L1	Iniciado	**10%**
L2	Reproducible pero intuitivo Parcialmente realizado	**50%**
L3	Proceso definido En funcionamiento	**90%**
L4	Gestionado y medible Monitorizado	**95%**

L5	Optimizado Mejora continua	**100%**

Fuente: Herramienta de Análisis de riesgos - PILAR (5.4.5)

Salvaguardas de Protecciones generales u horizontales

Tabla 26. Protecciones generales u horizontales

Salvaguardas		Dimensión	Evaluación
H.AC	Control de acceso lógico	[A], [D], [C]	40%
H.tools.TM	Herramienta de monitorización de tráfico	[C], [I], [A], [D]	60%
DLP	Herramienta de monitorización de contenidos	[C], [I], [A], [D]	60%

Descripción:

H.AC Control de acceso lógico: La gobernación de Putumayo ha dispuesto de algunas medidas básicas para el control de acceso a los sistemas de información, servicios y la administración de algunos dispositivos como switches y firewall; a través de contraseñas y perfiles que solo permiten el ingreso a los funcionarios autorizados como ejemplo está el sistema de autenticación de cada uno de los equipos de cómputo del entidad que se encuentran ligados al Servidor de dominio; esta salvaguarda permite proteger los activos de software y servicios en los criterios de Autenticidad, Disponibilidad y Confidencialidad, se evalúa con un puntaje del 40% ya que pueden existir dichos métodos pero no son los suficientes requiriendo otros elementos como tarjetas y/o tokens que fortalezcan los controles de acceso lógico.

H.tools.TM Herramienta de monitorización de tráfico y DLP Herramienta de monitorización de contenidos: Existe en la Entidad un sistema para la gestión de tráfico y monitorización de contenidos denominada View Point fundamentada en plataforma web que complementa los servicios de seguridad de la herramienta firewall Sonic WALL la cual permite supervisar el uso de la red corporativa, las actividades y eventos que se desarrollan en la misma tales como amenazas a la seguridad, utilización de aplicaciones y de Internet por parte de los funcionarios o consumo de ancho de banda. Esta medida permite proteger los activos de comunicaciones, servicios y de software de la gobernación de

Putumayo en las dimensiones de Disponibilidad, Confidencialidad, Autenticidad, Integridad y Trazabilidad del servicio, con una efectividad del 60%, dicha valorización se realiza teniendo en cuenta que pueden existir la herramienta pero el personal encargado no cuentan con los procedimientos necesarios para tomar decisiones y actuar.

Salvaguardas de Protección de los Datos /Información.

Tabla 27. Protección de los Datos/Información

Salvaguardas		Dimensión	Evaluación
D.A	Copias de seguridad de los datos (backup)	[I], [D]	30%
D.DS	Uso de firmas electrónicas	[C], [T], [A], [I]	5%

Descripción:

D.A Copias de seguridad de los datos (backup): En la actualidad en la gobernación de Putumayo utilizan esta salvaguarda de las copias de seguridad aplicadas a los activos de datos e información las cuales se realizan dos veces al día de acuerdo al nivel de criticidad de las Bases de Datos, otras semanales y diarias según lo establecido al Procedimiento de Respaldo y Protección de la Información (CÓDIGO: PT-GTI-007), esta medida involucra todas las dimensiones(Integridad y Disponibilidad) y su valoración es del 30%, ya que el proceso no es completo y no se han definido claramente las actividades de restauración de las copias, además los lugares de almacenamiento no son los adecuados y tampoco se manejan métodos de encriptación de los medios que las almacenan.

D.DS Uso de firmas electrónicas: En la entidad se usa esta medida del dispositivo electrónico solo para los trámites que realiza la secretaria de Hacienda departamental a través de la DIAN (Dirección de Impuestos y Aduanas Nacionales) para la presentación de informes, proceso en los cuales la firma digital sustituye para todos los efectos la firma autógrafa, este mecanismo permite preservar la Autenticidad, Confidencialidad, Integridad y Trazabilidad de la información. Se califica con un valor bajo del (5%) ya que ningún otro tramite que genere documentos, certificación o constancias de la entidad usan la firma digital.

Salvaguardas de Protección de los Servicios

Tabla 28. Salvaguardas: Protección De Los Servicios

Salvaguardas		Dimensión	Evaluación
S.SC	Se aplican perfiles de seguridad	[A], [I], [D]	70%
S.www	Protección de servicios y aplicaciones web	[I],[D]	40%

Descripción:

S.SC Se aplican perfiles de seguridad: Existe en la entidad configurados perfiles de seguridad para los diferentes sistemas de información que se manejan definidos de acuerdo al grupo de usuarios y los permisos a los cuales tienen derecho, en algunas aplicaciones como el sistema financiero, banco de proyectos entro otros permiten la creación de perfiles de acuerdo a los roles y sus funciones asignadas. De igual forma a través del servidor de Dominio se configuran los perfiles y se controlan algunas funcionalidades de los equipos de cómputo de la Entidad tales como no ingresar dispositivos de almacenamiento (conector USB), instalación de aplicaciones, etc. y los cuales solo son habilitados para los perfiles administradores que corresponde a los funcionarios del área de sistemas; también estos perfiles son configurados a través de las políticas de firewall que se aplican dependiendo las zonas, los servicios, servidores, grupo de funcionarios, protocolos, etc.

Esta medida involucra las dimensiones de Autenticidad, Integridad y Disponibilidad de los datos y se evalúa con el 70% ya que a pesar de la falta de procedimientos y políticas en cuanto al tema de seguridad se han adoptado estas directivas a través de circulares que han emitido algunas dependencias y el área de Sistemas, pero hace falta incluir y robustecer algunos perfiles.

S.www Protección de servicios y aplicaciones web: Entre las medidas adoptadas por la Entidad relacionadas con esta salvaguarda están las validación de datos de entrada, limitar consultas a bases de datos, utilizar métodos de configuración que evitan bloqueos de cuentas de usuarios de forma malintencionada (bloquear el uso de una cuenta después de máximo 3 a 5 intentos fallidos de autenticación),etc. estas medidas de defensa comúnmente usadas para evitar el descubrimiento de contraseñas de usuarios por fuerza bruta; aunque se adopten estos métodos hacen faltan muchos más como el análisis frecuente de vulnerabilidades que permiten asegurar la Integridad y la

Disponibilidad de los servicios y aplicaciones; esta salvaguarda se evalúa en un 40 % ya que hace falta la aplicación de muchos más métodos que permitan garantizar la seguridad de estos activos que se pueden comprometer.

Salvaguardas de Protección de las aplicaciones (software)

Tabla 29. Protección de las aplicaciones (software)

Salvaguardas		Dimensión	Evaluación
SW.A	Copias de seguridad (backup)	[I], [D]	50%
SW.Cm	Cambios (actualizaciones y mantenimiento)	[I],[D], [A]	70%

Descripción:

SW.Cm Cambios (actualizaciones y mantenimiento): En la Entidad se mantiene el control permanente de algunas aplicaciones que son críticas para el normal funcionamiento de las actividades tales como los sistemas operativos, software financiero, nómina y antivirus, a este último también se aplica la actualización regular de las bases de datos. Es importante mencionar que en la organización también se regula el uso autorizado de aplicaciones y se controla la instalación de software y productos con licencia con el fin de mantener y garantizar sus dimensiones de Integridad Disponibilidad y Autenticidad. Estas medidas son aceptables ya que a pesar de no contar con políticas documentadas se realiza el proceso y se controla a través de circulares y el apoyo de la oficina de Control Interno de Gestión.

Salvaguardas de Protección de los equipos (hardware)

Tabla 30. Protección de los equipos (hardware)

Salvaguardas		Dimensión	Evaluación
HW.op	Operación	[D]	30%

Descripción:

HW.op Operación: Aunque en la entidad no se han definido políticas y procedimientos claros para el manejo de equipos, se han aplicado medidas como la aplicación de pautas y recomendaciones entregadas por parte de los profesionales expertos que han instalado los equipos, servidores, switches y central telefónica, además del asesoramiento a los funcionarios de la oficina de sistemas; dichas medidas permiten asegurar la Disponibilidad del activo y el criterio de evaluación es baja (30%) teniendo en cuenta que es necesario aplicar y fortalecer esta salvaguarda.

Salvaguardas de Protección de las comunicaciones

Tabla 31. Protección de las comunicaciones

Salvaguardas		Dimensión	Evaluación
COM.internet	Internet: uso de ? acceso a	[D], [C],[T]	70%
COM.wifi	Seguridad Wireless (WiFi)	[D], [C], [A]	80%

Descripción:

COM.internet Internet: uso de? acceso a: La aplicación de esta salvaguardad se realiza mediante la aplicación de filtros y la configuración de políticas de acuerdo a los perfiles definidos en el firewall físico que tiene la entidad, el cual a través de la herramienta Dashboard les proporciona instrumentos para el seguimiento del servicio de internet tales como informes de los sitios visitados, consumo de ancho de banda, monitoreo de tráfico y alertas de vulnerabilidades así como también a través del firewall se restringe el ancho de banda por zonas, filtro de contenidos y también horarios de navegación para sitios especiales; con dichas medidas de seguridad se logra garantizar en cierta forma la Disponibilidad, confidencialidad y trazabilidad del servicio, la evaluación de la salvaguarda se da con un 70% de efectividad teniendo en cuenta que a pesar de las directivas establecidas en el dispositivo firewall hace falta reforzar con políticas documentadas sobre este tema.

COM.wifi Seguridad Wireless (WiFi): Con respecto a esta medida la configuración de la red inalámbrica está separada por zonas en el firewall permitiendo la asignación de políticas propias para ese segmento de red (protocolos, ancho de banda, control de contenidos), además cuentan con una controladora de accesos de radio H3C que permite realizar métodos de autenticación (filtro de seguridad por MAC Address), configuración de servicios inalámbricos, y demás estándares usados para garantizar la seguridad de las

transmisiones inalámbricas y la efectividad de las dimensiones relacionadas la Disponibilidad, Confiabilidad y Autenticidad; se asigna una evaluación del 80% ya que existen buenos métodos de autenticación en la red pero se requiere reforzar las políticas.

Salvaguardas de Protección de los elementos auxiliares

Tabla 32. Protección de los elementos auxiliares

Salvaguardas		Dimensión	Evaluación
AUX.power	Suministro eléctrico	[D]	40%
AUX.AC	Climatización	[D]	20%

Descripción:

AUX.power Suministro eléctrico: A pesar de que la entidad cuenta con respaldo de tres UPS distribuidas de acuerdo a la carga de los sub-centros y una plata eléctrica, en muchas ocasiones han presentado fallas por estas razón se considera en los criterios de evaluación como baja y puede afectar la disponibilidad de los activos.

AUX.AC Climatización: Al evaluar esta medida de seguridad se evidencia que la entidad cuenta con un aire acondicionado que de acuerdo al tamaño del cuarto si permite lograr la temperatura adecuada, pero se requiere de otras medidas de refrigeración más técnicas y de precisión que permitan mantener el correcto funcionamiento de los sistemas así como también de otros elementos complementarios como son las puertas, piso y techo.

6.2.3.4 Evaluación del riesgo

La siguiente valoración se realiza con base a los datos obtenidos de las fuentes utilizadas como son las visitas de campo, observación directa y entrevista aplicada al profesional del área de Sistemas de la Gobernación de Putumayo. (Ver anexo N°6)

Este proceso de evaluación del estado del riesgo se realiza con el objetivo de analizar los datos obtenidos en las acciones anteriores y evaluar el estado de riesgo, incluyendo la estimación de impacto y riesgo.

Estimación Del Impacto

El objetivo de realizar este proceso es determinar el alcance del daño producido sobre los activos de información de la Entidad en caso de llegarse a materializar una amenaza; para lo cual se evalúa el grado de repercusión que pueda presentar cada activo, dentro de las dimensiones de valoración analizadas anteriormente como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Figura 16. Escala de valoración del impacto

Fuente: Herramienta PILAR

Impacto acumulado: Es el impacto potencial al que está expuesto el sistema tomando como base los valores obtenidos de los activos (degradación) y la valoración de las amenazas por cada dimensión al que está expuesto, sin tener en cuenta las salvaguardas actuales. El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. [29]

La siguiente tabla de valoracion es tomada de la herramienta Pilar propuesta por la metodologia por Magerit v.3.

Tabla 33. Criterios de valoración.

[29] MAGERIT – versión 3.0 Libro I - Método

Valor			Criterio
10	E	Extremo	Daño extremadamente grave
9	MA	Muy Alto	Daño muy grave
6-8	A	Alto	Daño grave
3-5	M	Medio	Daño importante
1-2	B	Bajo	Daño menor
0	D	Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit V.3 - Libro II - Catálogo de

En el Anexo 8. Impacto Acumulado herramienta PILAR, se incluye la evidencia del proyecto desarrollado en la herramienta PILAR.

- **Impacto Acumulado: [D] Datos / Información**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Actos administrativos	[6]	[4]			
Datos de gestión interna	[6]	[4]			
Documentos contractuales (contratos, convenios)	[8]	[7]		[7]	
Proyectos	[6]	[4]			
Credenciales (Contraseñas)	[3]	[9]			
Copias de respaldo	[8]	[9]	[7]		
Base de datos de los sistemas de información	[8]	[9]	[9]	[7]	
Archivo fotográfico y de video	[0]				
Información página web	[8]	[6]	[6]	[6]	

- **Impacto Acumulado: [S] Servicios**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Correo electrónico	[6]	[3]	[3]	[7]	
Mensajería interna (chat)	[6]	[3]		[7]	
Página web	[8]	[6]	[6]	[7]	
Liquidación de impuestos en línea	[4]	[6]	[6]	[7]	
Consulta de pagos en línea	[8]	[3]	[6]	[7]	
Internet	[9]				
Intranet	[6]	[6]	[6]	[9]	
Ingreso y consultas de PQRD	[3]	[3]	[3]	[4]	
Diferentes Trámites y servicios que se realiza	[6]				

Servicio VOZ/IP	[6]				
Ventanilla única	[6]				

Fuente: Autores

- **Impacto Acumulado: [SW] Software - Aplicaciones informáticas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
PCT	[9]	[7]	[7]	[7]	
SI Nomina	[7]	[7]	[9]	[7]	
Liquidador Rentas	[7]	[7]			
Gestión de PQRD	[4]				
Gestión Documental	[7]	[7]			
SIREBPID	[7]	[7]	[7]	[9]	
SISTRANP	[7]	[7]			
SIG	[5]	[7]			
ZIMBRA	[9]	[7]	[7]	[7]	
Aplicaciones web	[7]	[7]			
Gaceta Putumayo	[7]				
Mensajería interna Openfire y Spark.	[4]		[7]	[9]	
Sistema Integral de Información para la S.S.D	[9]	[7]			
Sistema operativo	[7]				
Ofimática	[7]				
Antivirus	[8]				
Gestor de máquinas virtuales	[7]		[4]	[4]	

Fuente: Autores

- **Impacto Acumulado: [HW] Equipamiento informático (hardware)**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	[10]	[8]	[10]		
SAN (Storage área Network)	[10]				
Equipo de cómputo (escritorio, portátil)	[7]				
Periféricos (medios de impresión, Impresora, escáneres, etc)	[0]				
FIREWALL Físico	[9]				

Fuente: Autores

- **Impacto Acumulado: [COM] Redes de comunicaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Router (proveedor internet)	[9]				
Switches	[9]				
Acces Point	[7]				
Swicth Consola KVM	[4]				
Controladora de red (inalámbrica)	[7]				
Radios de enlace y Antena omnidireccional para AMO-2G10	[6]				
Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	[9]				
Central telefónica	[8]				
Teléfonos IP	[4]				

Fuente: Autores

- **Impacto Acumulado: [AUX] Equipamiento auxiliar**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Regulador de voltaje automático	[10]				
Estabilizador	[9]				
UPS	[3]				
Planta eléctrica	[1]				
Aire acondicionado	[4]				
Cámaras IP	[0]				

Fuente: Autores

- **Impacto Acumulado: [L] Instalaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Gabinete Piso	[2]				
Patch Panel AMP cat 6.	[4]				
Puntos de cableado estructurado cat. 6	[7]				
Canaleta red de voz/datos	[9]				

Fuente: Autores

- **Impacto Acumulado: [P] Personas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Jefe departamento de sistemas	[6]	[7]	[9]		
Operador de Base datos y aplicaciones	[8]	[7]	[7]		
Web Máster	[7]	[7]	[7]		
Soporte técnico	[8]	[6]	[5]		
Funcionarios de la Entidad	[3]				
Usuarios /comunidad general	[0]				

Fuente: Autores

Impacto Residual: Es el resultado de combinar el valor de los activos, de las amenazas y la aplicación de la efectividad de las salvaguardas existentes identificadas anteriormente; los activos con resultado muy bajo o bajo (o casillas en blanco), son riesgos con los que se puede convivir pero que se tendrán en cuenta dentro de los controles, políticas de seguridad y recomendaciones.

El impacto residual repercutido se calcula sobre el valor propio, en el Anexo 9. Impacto residual herramienta PILAR, se incluye la evidencia del proyecto desarrollado en la herramienta PILAR.

- **Impacto Residual: [D] Datos / Información**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Actos administrativos	[4]	[2]			
Datos de gestión interna	[4]	[2]			
Documentos contractuales (contratos, convenios)	[6]	[5]		[6]	
Proyectos	[4]	[2]			
Credenciales (Contraseñas)	[1]	[7]			
Copias de respaldo	[6]	[7]	[5]		
Base de datos de los sistemas de información	[6]	[7]	[7]	[6]	
Archivo fotográfico y de video	[0]				
Información página web	[6]	[4]	[4]	[5]	

Fuente: Autores

- **Impacto Residual: [S] Servicios**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Correo electrónico	[5]	[1]	[1]	[6]	
Mensajería interna (chat)	[5]	[1]		[6]	
Página web	[7]	[5]	[5]	[6]	
Liquidación de impuestos en línea	[3]	[5]	[5]	[6]	
Consulta de pagos en línea	[7]	[1]	[5]	[6]	
Internet	[8]				
Intranet	[5]	[5]	[5]	[8]	
Ingreso y consultas de PQRD	[2]	[1]	[1]	[2]	
Diferentes Trámites y servicios que se realiza	[5]				
Servicio VOZ/IP	[5]				
Ventanilla única	[5]				

Fuente: Autores

- **Impacto Residual: [SW] Software - Aplicaciones informáticas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
PCT	[8]	[5]	[5]	[6]	
SI Nomina	[6]	[5]	[7]	[6]	
Liquidador Rentas	[6]	[5]			
Gestión de PQRD	[3]				
Gestión Documental	[6]	[5]			
SIREBPID	[6]	[5]	[5]	[8]	
SISTRANP	[6]	[5]			
SIG	[4]	[5]			
ZIMBRA	[8]	[5]	[5]	[6]	
Aplicaciones web	[6]	[5]			
Gaceta Putumayo	[6]				
Mensajería interna Openfire y Spark.	[3]		[5]	[8]	
Sistema Integral de Información para la S.S.D	[8]	[5]			
Sistema operativo	[6]				
Ofimática	[6]				
Antivirus	[7]				
Gestor de máquinas virtuales	[5]		[2]	[2]	

Fuente: Autores

- **Impacto Residual: [HW] Equipamiento informático (hardware)**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	[10]	[7]	[9]		
SAN (Storage área Network)	[10]				
Equipo de cómputo (escritorio, portátil)	[7]				
Periféricos (medios de impresión, Impresora, escáneres, etc)	[0]				
FIREWALL Físico	[9]				

Fuente: Autores

- **Impacto Residual: [COM] Redes de comunicaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Router (proveedor internet)	[9]				
Switches	[9]				
Acces Point	[7]				
Swicth Consola KVM	[4]				
Controladora de red (inalámbrica)	[7]				
Radios de enlace y Antena omnidireccional para AMO-2G10	[4]				
Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	[9]				
Central telefónica	[6]				
Teléfonos IP	[2]				

Fuente: Autores

- **Impacto Residual: [AUX] Equipamiento auxiliar**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Regulador de voltaje automático	[9]				
Estabilizador	[8]				
UPS	[2]				
Planta eléctrica	[0]				
Aire acondicionado	[3]				
Cámaras IP	[0]				

Fuente: Autores

- **Impacto Residual: [L] Instalaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Gabinete Piso	[1]				
Patch Panel AMP cat 6.	[3]				
Puntos de cableado estructurado cat. 6	[6]				
Canaleta red de voz/datos	[8]				

Fuente: Autores

- **Impacto Residual: [P] Personas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Jefe departamento de sistemas	[5]	[6]	[8]		
Operador de Base datos y aplicaciones	[7]	[6]	[6]		
Web Máster	[6]	[6]	[6]		
Soporte técnico	[8]	[6]	[4]		
Funcionarios de la Entidad	[3]				
Usuarios /comunidad general	[0]				

Fuente: Autores

Estimación del estado del riesgo

A continuación se procede a estimar el riesgo por amenaza, activo y dimensión tanto el riesgo potencial y los valores residuales, que brindan información importante para tomar decisiones en materia de seguridad, permiten identificar que activos se deben supervisar y son más críticos, que salvaguardas medidas se deben mejorar y la aceptación de riesgos.

El riesgo es un indicador de lo que probablemente suceda por causa de las amenazas, se identifican los dos tipos de riesgos de acuerdo a la herramienta PILAR: acumulado y residual repercutido.

Para realizar la estimación del riesgo se hace uso de la siguiente escala cualitativa, establecida por PILAR que contiene los siguientes valores:

Figura 17. Niveles criticidad de riesgo

Fuente: Herramienta PILAR

Riesgo Acumulado:

Se calcula sobre los activos teniendo en cuenta el impacto acumulado sobre cada activo y la frecuencia de la amenaza. En el Anexo 10. Riesgo acumulado herramienta PILAR., se incluye la evidencia del proyecto desarrollado en la herramienta PILAR.

- **Riesgo Acumulado: [D] Datos / Información**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Actos administrativos	{5,4}	{4,2}			
Datos de gestión interna	{5,4}	{4,2}			
Documentos contractuales (contratos, convenios)	{6,6}	{5,9}		[5,9]	
Proyectos	{5,4}	{4,2}			
Credenciales (Contraseñas)	{3,7}	{7,1}			
Copias de respaldo	{6,6}	{7,1}	{6,3}		
Base de datos de los sistemas de información	{6,6}	{7,1}	{7,5}	{5,9}	
Archivo fotográfico y de video	{1,9}				
Información página web	{6,6}	{5,4}	{5,7}	{5,4}	

Fuente: Autores

- **Riesgo Acumulado: [S] Servicios**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Correo electrónico	{5,4]	{3,7}	{2,8}	{5,1}	
Mensajería interna (chat)	{5,4}	{3,7}		{5,1}	
Página web	{6,6}	{5,4}	{4,5}	{5,1}	
Liquidación de impuestos en línea	{4,2}	{5,4}	{4,5}	{5,1}	
Consulta de pagos en línea	{6,6}	{3,7}	{4,5}	{5,1}	
Internet	{6,2}				
Intranet	{5,4}	{5,4}	{4,5}	{6,2}	
Ingreso y consultas de PQRD	{3,7}	{3,7}	{2,8}	{3,3}	
Diferentes Trámites y servicios que se realiza	{5,4}				
Servicio VOZ/IP	{5,4}				
Ventanilla única	{5,4}				

Fuente: Autores

- **Riesgo Acumulado: [SW] Software - Aplicaciones informáticas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
PCT	{6,2}	{5,1}	{5,1}	{5,1}	
SI Nomina	{5,1}	{5,1}	{6,2}	{5,1}	
Liquidador Rentas	{5,1}	{5,1}			
Gestión de PQRD	{3,3}				
Gestión Documental	{5,1}	{5,1}			
SIREBPID	{5,1}	{5,1}	{5,1}	{6,2}	
SISTRANP	{5,1}	{5,1}			
SIG	{3,9}	{5,1}			
ZIMBRA	{6,2}	{5,1}	{5,1}	{5,1}	
Aplicaciones web	{5,1}	{5,1}			
Gaceta Putumayo	{5,1}				
Mensajería interna Openfire y Spark.	{3,3}		{5,1}	{6,2}	
Sistema Integral de Información para la S.S.D	{6,2}	{5,1}			
Sistema operativo	{5,1}				
Ofimática	{5,1}				
Antivirus	{5,7}				

Fuente: Autores

- **Riesgo Acumulado: [HW] Equipamiento informático (hardware)**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	{7,2}	{5,6}	{6,3}		
SAN (Storage área Network)	{7,2}				
Equipo de cómputo (escritorio, portátil)	{5,4}				
Periféricos (medios de impresión, Impresora, escáneres, etc)	{1.3}				
FIREWALL Físico	{6.6}				

Fuente: Autores

- **Riesgo Acumulado: [COM] Redes de comunicaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Router (proveedor internet)	{6,6}				
Switches	{6,6}				
Acces Point	{5,4}				
Swicth Consola KVM	{3,7}				
Controladora de red (inalámbrica)	{5,4}				
Radios de enlace y Antena omnidireccional para AMO-2G10	{5,4}				
Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	{6,6}				
Central telefónica	{6,6}				
Teléfonos IP	{4,2}				

Fuente: Autores

- **Riesgo Acumulado: [AUX] Equipamiento auxiliar**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Regulador de voltaje automático	{6,8}				
Estabilizador	{6,2}				
UPS	{2,7}				
Planta eléctrica	{1,5}				
Aire acondicionado	{3,3}				
Cámaras IP	{0,9}				

Fuente: Autores

- **Riesgo Acumulado: [L] Instalaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Gabinete Piso	{2,1}				
Patch Panel AMP cat 6.	{3,3}				
Puntos de cableado estructurado cat. 6	{5,4}				
Canaleta red de voz/datos	{6,6}				

Fuente: Autores

- **Riesgo Acumulado: [P] Personas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Jefe departamento de sistemas	{4,5}	{5,0}	{6,6}		
Operador de Base datos y aplicaciones	{5,7}	{5,0}	{5,4}		
Web Máster	{4,7}	{5,0}	{5,4}		
Soporte técnico	{5,4}	{4,5}	{4,7}		
Funcionarios de la entidad	{2,5}				
Usuarios / comunidad general	{0,6}				

Fuente: Autores

Riesgo Residual:

Es el riesgo obtenido posterior a la valoración y aplicación de salvaguardas que permitirían reducir la probabilidad de que una amenaza ocurra. Para su evaluación se utiliza los valores residuales para la probabilidad y la degradación, es decir, los valores originales reducidos por la eficacia de las salvaguardas.[30]

En el Anexo 11. Riesgo residual herramienta PILAR., se incluye la evidencia del proyecto desarrollado en la herramienta PILAR.

- **Riesgo Residual: [D] Datos / Información**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Actos administrativos	{3,8}	{2,4}			
Datos de gestión interna	{3,8}	{2,4}			
Documentos contractuales (contratos, convenios)	{5,0}	{4,1}		[4,8]	
Proyectos	{3,8}	{2,4}			
Credenciales (Contraseñas)	{2,1}	{5,4}			
Copias de respaldo	{5,0}	{5,3}	{4,3}		
Base de datos de los sistemas de información	{5,0}	{5,4}	{5,5}	{4,8}	
Archivo fotográfico y de video	{0,8}				
Información página web	{5,0}	{3,6}	{3,7}	{4,2}	

Fuente: Autores

- **Riesgo Residual: [S] Servicios**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Correo electrónico	{4,6]	{2,0}	{1,1}	{3,9}	
Mensajería interna (chat)	{4,6}	{2,0}		{3,9}	
Página web	{5,8}	{3,8}	{3,3}	{3,9}	
Liquidación de impuestos en línea	{3,5}	{3,8}	{3,3}	{3,9}	
Consulta de pagos en línea	{5,8}	{2,1}	{3,3}	{3,9}	
Internet	{5,7}				
Intranet	{4,6}	{3,8}	{3,3}	{5,2}	

[30] http://www.ar-tools.com/es/glossary/index.html

Ingreso y consultas de PQRD	{2,9}	{2,1}	{1,2}	{1,7}	
Diferentes Trámites y servicios que se realiza	{4,6}				
Servicio VOZ/IP	{4,6}				
Ventanilla única	{4,6}				

Fuente: Autores

- **Riesgo Residual: [SW] Software - Aplicaciones informáticas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
PCT	{5,3}	{3,3}	{3,3}	{3,9}	
SI Nomina	{4,1}	{3,3}	{4,6}	{3,9}	
Liquidador Rentas	{4,1}	{3,3}			
Gestión de PQRD	{2,3}				
Gestión Documental	{4,1}	{3,3}			
SIREBPID	{4,1}	{3,3}	{3,3}	{5,2}	
SISTRANP	{4,1}	{3,3}			
SIG	{2,9}	{3,3}			
ZIMBRA	{5,3}	{3,3}	{3,3}	{3,9}	
Aplicaciones web	{4,1}	{3,3}			
Gaceta Putumayo	{4,1}				
Mensajería interna Openfire y Spark.	{2,3}		{3,3}	{5,2}	
Sistema Integral de Información para la S.S.D	{5,3}	{3,3}			
Sistema operativo	{4,1}				
Ofimática	{4,1}				
Antivirus	{4,7}				

Fuente: Autores

- **Riesgo Residual: [HW] Equipamiento informático (hardware)**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	{6,6}	{5,2}	{5,8}		
SAN (Storage área Network)	{6,6}				
Equipo de cómputo (escritorio, portátil)	{4,9}				
Periféricos (medios de impresión, Impresora, escáneres, etc)	{0.9}				
FIREWALL Físico	{6.1}				

Fuente: Autores

- **Riesgo Residual: [COM] Redes de comunicaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Router (proveedor internet)	{6,1}				
Switches	{6,1}				
Acces Point	{4,9}				
Swicth Consola KVM	{3,1}				
Controladora de red (inalámbrica)	{4,9}				
Radios de enlace y Antena omnidireccional para AMO-2G10	{3,4}				
Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	{5,8}				
Central telefónica	{4,6}				
Teléfonos IP	{2,3}				

Fuente: Autores

- **Riesgo Residual: [AUX] Equipamiento auxiliar**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Regulador de voltaje automático	{6,3}				
Estabilizador	{5,7}				
UPS	{2,2}				
Planta eléctrica	{1,0}				
Aire acondicionado	{2,8}				
Cámaras IP	{1,7}				

Fuente: Autores

- **Riesgo Residual: [L] Instalaciones**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Gabinete Piso	{1,7}				
Patch Panel AMP cat 6.	{2,9}				
Puntos de cableado estructurado cat. 6	{4,6}				
Canaleta red de voz/datos	{5,8}				

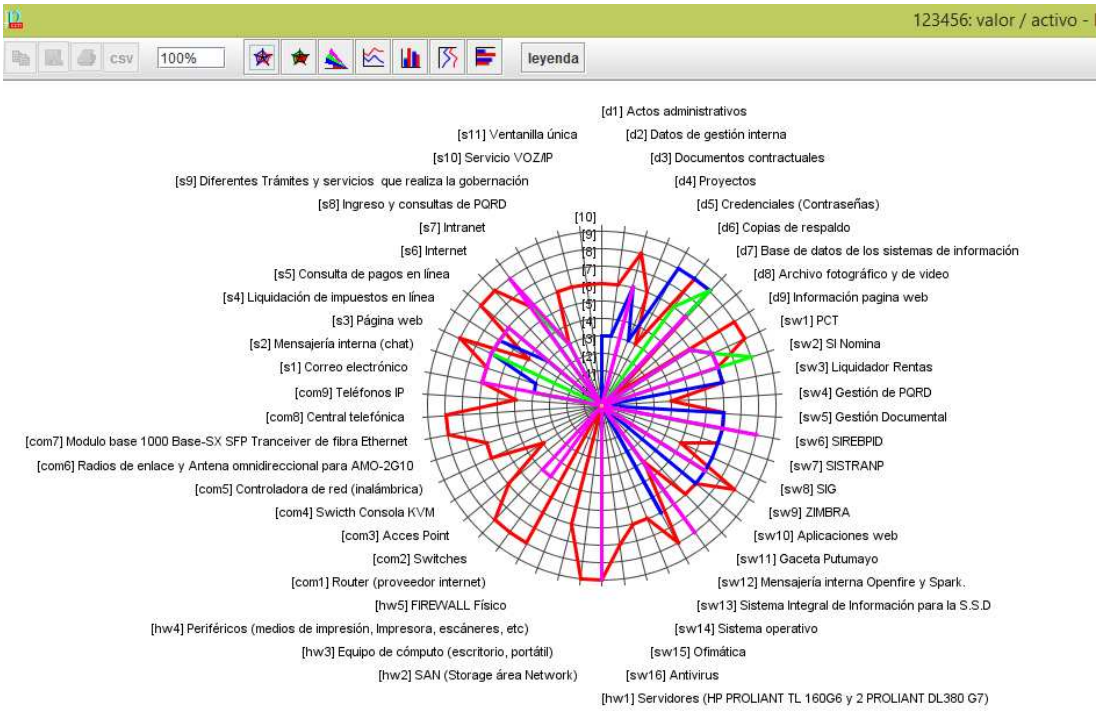
Fuente: Autores

- **Riesgo Residual: [P] Personas**

Activo	DIMENSIONES				
Nombre	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Jefe departamento de sistemas	{3,9}	{4,4}	{6,2}		
Operador de Base datos y aplicaciones	{5,1}	{4,4}	{5,0}		
Web Máster	{4,3}	{4,4}	{5,0}		
Soporte técnico	{5,0}	{4,1}	{4,3}		
Funcionarios de la entidad	{2,0}				
Usuarios / comunidad general	{0,5}				

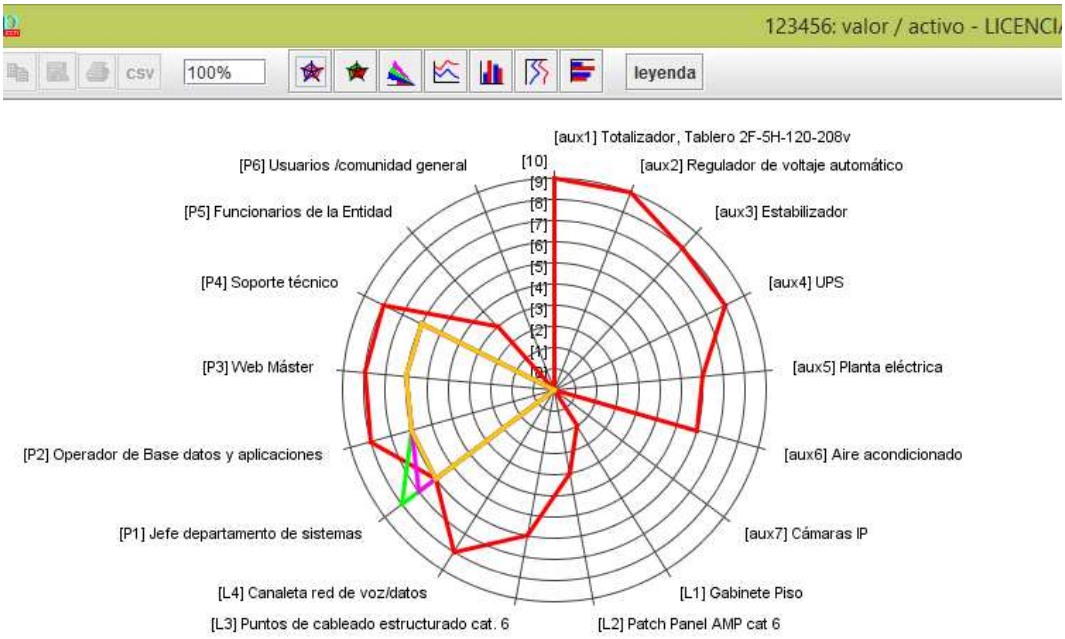
Análisis de Riesgos:

Figura 18. Identificación de los riesgos fuente PILAR



Fuente: Proyecto Herramienta PILAR

Figura 19. Identificación de los riesgos fuente pilar



Fuente: Proyecto Herramienta PILAR

Como se puede evidenciar en las figuras anteriores estas son el resultado de todo el proceso del análisis de los riesgos, en ella se puede evidenciar con facilidad cuales son los activos de información de la Gobernación de Putumayo que tienen un alto nivel de riesgos, estos riesgos serán mitigados en la siguiente fase, es decir, se establecerán las políticas de seguridad de la información buscando reducir la materialización de alguno de estos incidentes.

Dentro del análisis de riesgo realizado se puede apreciar con mayor claridad los impactos y los riesgos a los cuales está sometida la entidad, estos riesgos fueron calificados y basándose en esta calificación se determina lo siguiente:

1. Riesgo crítico: Estos riesgos requieren atención urgente
2. Riesgo Grave: Estos requieren atención.
3. Riesgo normal: Este riesgo puede ser estudiado para manejar su tratamiento.
4. Riesgo asumible: Este tipo de riesgos son aceptados por la organización y no se tomaran medidas para su control.

Los análisis de los activos, amenazas y riesgos en la gobernación del Putumayo representan una base sólida para que los funcionarios encargados de la implementación de las políticas de seguridad pueda tomar decisiones, de acuerdo a los activos más críticos de la entidad y se tiene claro cuáles son los que se deben proteger de las amenazas y la determinación de las medidas de salvaguardas que se han establecido para ser protegidos.

Cabe destacar que dentro de las organizaciones los activos están expuestos a un número muy amplio de riesgos, pero la tarea de identificar cuáles son los activos que poseen un nivel más avanzado de materializar un riesgo está definida con el proceso de levantamiento de riesgos, con esto se puede hacer el análisis para la implementación de políticas de seguridad para mitigarlos al máximo.

A continuación se presentara las politicas para la gestión de los activos con los riesgos más críticos:

Datos / Información

Dentro de los activos de Datos Informaticos se establecerán politicas para mitigar las amenazas que puedan afectar la disponibilidad, integridad, confidencialidad de estos, el unico riesgo que se acepta es el de archivos fotografico o multimedia, el cual no representan un activo critico a tener en cuenta en las politicas de seguridad para la entidad.

Servicios

Los activos relacionados en la categoria servicios fueron identificados como muy importantes para la gobernacion del Putumayo, es por esto que al aplicar el proceso de análisis de las amenazas y los riesgos sobre estos activos, las calificaciones para su riesgo son altas, lo que contempla que se deben aplicar politicas para controlar estos riesgos, en especial proteger los activos de la página web de la entidad, el servicio de internet y el sistema de pagos en linea, los cuales son muy criticos y afectaria a la entidad en gran escala si uno de estos servicios dejara de funcionar corectamente, se deben aplicar políticas de segurida en menor medida que las anteriores para los activos de Correo electrónico, mensajeria interna y la intranet, siendo servicios muy importantes para la entidad pero su afectacion no representa un grado de daño severo como los anteiores.

Software - Aplicaciones informáticas

Dentro de los activos que pertenecen a la capa de las aplicaciones encontramos los sistemas informáticos de la gobernación del Putumayo, una vez evaluado sus amenazas y analizado las salvaguardas existentetes se define que se deben aplicar politicas a su conjunto, estableciendo más importancia a los activos del Sistema de Nómina, Liquidador de Rentas, PCT y el sistema integral de información para la SSD, estos tienen un valor muy alto para la entidad y pueden ser sujetos de varias amenazas y su materialización afectaría en gran medida a la gobernación del Putumayo. Por otro lado, los demás activos también tienen un nivel muy alto en cuanto al riesgo para lo cual también se consideraran las políticas correspondientes para mitigar su afectación de las propiedades de cada uno, se debe elegir las mejores políticas para optimizar y prevenir los riesgos sobre estos activos.

Equipamiento informático (hardware)

En este grupo de activos se identifica uno de los grupos con la más alta calificación en cuanto a los riesgos, amenazas y el valor del activo para la gobernación del Putumayo, por este motivo los resultados obtenidos establecen que se deben aplicar políticas muy bien establecidas y de manera inmediata para mitigar la materialización de las amenazas sobre este grupo, en especial sobre los activos de Servidores, SAN, Firewall físico, estos activos representan la información más preciada para la organización y su materialización dejaría sin funcionar ninguno de los otros procesos importantes de la entidad. Las politicas a aplicar serán evaluadas con el fin de reducir al máximo o mitigar por completo la materialización de amenazas, para el activo de periféricos se aceptara el riesgo, esto puede afectar levemente un proceso pero no representa perdida grave de información o perdida de las propiedades de disponibilidad de la información.

Redes de comunicaciones

Dentro de los activos que conforman el grupo de las redes de comunicaciones se puede identificar claramente los más propensos a materializar una amenaza, dentro de estos se encuentra el Router, Switch y el módulo de fibra Ethernet; principalmente estos se encargaran de brindar la conectividad de todos los dispositivos para crear la intranet y además permite la conectividad de estos dispositivos al internet, por esta razón dentro del analisis del levantamiento de riesgos estos aparecen con un grado muy alto de criticidad, por lo tanto, se deben evaluar las políticas para mitigar la materialización de las amenazas sobre estos

activos, en caso de presentarse seria muy grave y la entidad no podría prestar el servico con normalidad.

También podemos identificar otro grupo de activos los cuales son los accces point, switch, red inalámbrica, los radios de enlace y la telefonía IP, este grupo de activos aunque representan un valor alto para la entidad, sufren en menor escala el analisis de los riesgos, en caso de afectarse alguno de esto afectaría a la gobernación del Putumayo pero se podrá seguir prestando el servicio mientras se da una solución, no obstante, se crearan las políticas correspondientes para mitigar y reducir al máximo la materialización de estas amenazas.

Equipamiento auxiliar

El análisis de riesgos realizado para este grupo de activos nos permite identificar que se debe prestar atención urgente al activo denominado Regulador de voltaje automatico el cual representa el sistema de protección contra problemas eléctricos los cuales son muy comunes en la región, la materialización de una amenaza sobre esta activo dejaría desprotegida a la entidad y causar daños en cualquiera de los otros dispositivos, otro de los activos importantes son las UPS y la planta eléctrica la cual protege de las suspensiones de electricidad y picos eléctricos los cuales puede dañar los otros dispositivos, este activo también será sujeto para aplicar las políticas para su protección, así como los activos de los aires acondicionados, aunque no tiene un grado alto en el analisis de riesgos sé establecerán las políticas correspondientes para evitar las fallas.

Instalaciones

En este grupo de activos corresponde la infraestructura de la entidad, en si los lugares estratégicos que albergan otros activos como servidores y los sistemas de comunicaciones, dentro del analisis de riesgos se puede identificar que existe relación de los activos de infraestructura con los otros tipos de activos como hardware y comunicaciones y su relación es directa a la importancia de estos activos, en el análisis se puede apreciar que los activos denominados canaletas presentan una alta valoración de riesgo, si llegara a afectarse este elemento generaría daños en sistemas de cableados y electricos, por esa razón se presentaran políticas para mitigar los riesgos sobre estos.

En menor medida el activo de puntos de cableado también presenta un grado alto de evaluación de riesgos por lo tanto se establecerán políticas para prevenir la materialización de las amenazas, el sistema de gabinete del primero piso plantea que puede ser manejado o aceptado, por lo tanto, se considerara en aceptar el riesgo ya que este presenta un grado bajo de evaluación del análisis de riesgo y no afectaría de manera grave a la entidad.

Personas

Dentro del grupo de activos de personas podemos identificar que la valoración del análisis de riesgos establece las calificaciones de acuerdo con la importancia del grupo de personal, es decir, entre mayor sea el cargo y la importancia de los procesos a su cargo mayor será la valoración del riesgo para ese activo, en ese orden de ideas podemos identificar los activos de operador de base de datos, jefe de sistemas y soporte técnico como los más críticos, a estos activos se debe aplicar políticas de controles para prevenir el riesgo.

Por otro lado, los activos de web máster y funcionaros de la entidad también representan un riesgo aceptable para la entidad, y por lo tanto también deben ser objeto de análisis para la implementación de políticas de seguridad.

El activo de usuarios está catalogado por el análisis de riesgos como despreciable, por lo tanto, no se tendrán en cuenta politicas de seguridad para este activo, aunque pueden estar sujetos a otras políticas para proteger otros activos diferentes a este grupo como por ejemplo el control de acceso para proteger la perdida de harware en la entidad.

6.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Con la definición de las políticas de seguridad de la información, la GOBERNACIÓN DE PUTUMAYO busca preservar sus activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software) y permitir un adecuado proceso de gestión de la información garantizando la integridad, confidencialidad y disponibilidad así como también la continuidad de los servicios de la Entidad.

Con el fortalecimiento del procedimiento de la seguridad de la información de la Entidad se busca establecer al interior de la entidad cultura por parte de los funcionarios, concientización y uso de buenas prácticas permitiendo apoyar el proceso de Gestión de Tecnología de Información de la Administración departamental.

Además de convertirse en un compromiso por parte del Mandatario y los secretarios despacho de cada una de las dependencias, los cuales deben promover su difusión, consolidación y cumplimiento.

6.3.1 Objetivos

LA GOBERNACIÓN DEL PUTUMAYO, para el cumplimiento de su misión, visión, política de calidad y enmarcado dentro de los valores y principios institucionales, establece las políticas de seguridad de la información, con el objetivo de:

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Proteger los activos tecnológicos de la gobernación de Putumayo de las vulnerabilidades y amenazas internas o externas que puedan afectar la seguridad informática de sus recursos.
- Minimizar el riesgo de los servicios y sistemas más importantes de la entidad.
- Garantizar la prestación oportuna de los servicios que ofrece la Entidad enmarcados dentro de las dimensiones de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información indispensable para

la gestión institucional y la toma de decisiones por parte de los cargos directivos.

- Conservar las políticas de seguridad de la información de la Entidad actualizadas, con el fin de mantener su vigencia y nivel de validez.

- Concientizar a los funcionarios, contratistas y terceros de la GOBERNACIÓN DEL PUTUMAYO sobre los temas de seguridad de la información.

- Garantizar la continuidad de la Entidad frente a incidentes.

6.3.2 Alcance

La política aplica a toda la entidad enmarcada dentro del proceso de Tecnología de Información, a sus funcionarios, contratistas, terceros, y proveedores de GOBERNACIÓN DEL PUTUMAYO dentro de sus áreas de responsabilidad.

6.3.3 Nivel de Cumplimiento

Todas las personas incluidas dentro del alcance deben darle aplicabilidad a la política, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción. La oficina de Sistemas suscrita a la secretaría de Servicios Administrativos departamental liderará el Comité de Seguridad de la Información y se encargara de la revisión constante de las políticas de seguridad informática, con el fin de realizar los cambios o ajustes de acuerdo a la actualización de infraestructura tecnológica o el impacto de los incidentes de seguridad informática, etc.

6.3.4 Sanciones previstas por Incumplimiento

El incumplimiento de las instrucciones establecidas en las políticas de seguridad de la información, serán sancionadas de acuerdo al grado y característica del aspecto no cumplido establecida por el jefe de personal de recursos humanos.

El documento establece una guía procedimental, dichas políticas son desplegadas y soportadas por estándares de seguridad informática, mejores prácticas, procedimientos y guías basados en los lineamientos de las normas ISO 27001

6.3.5 Políticas de Seguridad Relacionada al Personal

ORGANIZACIÓN INTERNA RELACIONADA CON LA SEGURIDAD DE LA INFORMACIÓN.	
Activos relacionados:	Inventario de Activos
El documento de la política de seguridad de la información, debe ser aprobado por el Secretario de despacho de Servicios Administrativos, publicado y comunicado a todos los funcionarios. La política de seguridad de la información debe ser revisada mínimo cada seis (6) meses, o si ocurren cambios significativos para garantizar la continuidad, sostenibilidad, efectividad y su actualización. El Gobernador y las Secretarias de Despacho deben apoyar activamente el proceso y las actividades relacionadas con la seguridad dentro de la entidad con compromiso demostrado, y la asignación de responsabilidades u/o recursos necesarios para su implementación. Las actividades de seguridad de la información deben ser lideradas por la oficina de Sistemas y coordinadas por los Secretarios de despacho y los jefes de oficina de la entidad con roles y funciones pertinentes, según lo definido en el organigrama. Se debe programar actividades de auditoría de seguridad con personal experto, que se encarguen de realizar la verificación de los sistemas con el fin de minimizar el riesgo de interrupciones de los procesos de la entidad. Se debe hacer seguimiento y ajustes del uso de los recursos tecnológicos, así como proyecciones de los requisitos de la capacidad tecnológica futura que permitan asegurar el desempeño requerido de los sistemas de la Gobernación.	

FUNCIONARIOS Y CAPACITACIONES	
Activos relacionados:	Personas
Como parte de su obligación contractual, los empleados, contratistas y usuarios	

de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, en el cual se deben establecer sus responsabilidades y las de la entidad con relación a la seguridad de la información.

Todos los empleados de la entidad y cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir capacitación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la entidad, según sea pertinente para sus funciones laborales.

Todos los empleados y contratistas deben devolver todos los activos pertenecientes a la entidad que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.

INCIDENTES Y ATENCIÓN A USUARIOS	
Activos relacionados:	Personas

Todo incidente u ocurrencia relacionada con la seguridad informática que se presente en la entidad debe ser reportada oficialmente a la oficina de sistemas encargada del proceso de Gestión de Tecnología e información.

Las solicitudes de atención a usuarios serán gestionadas a través del personal encargado del proceso del Área de Sistemas.

6.3.6 Políticas de Seguridad Lógica

DEFINICIÓN DE USUARIOS Y GRUPOS DE TRABAJO	
Activos relacionados:	Aplicaciones Informáticas
	Servicios
	Datos

Las cuentas de usuario y las contraseñas respectivas deben ser asignadas a todos los funcionarios de la Entidad únicamente por personal autorizado del área de Sistemas.

Los usuarios deben ser incluidos en su grupo de trabajo correspondiente, dicho grupo deben tener sus debidas restricciones de acuerdo a los permisos y accesos a los recursos de la red.

Se debe fortalecer una cultura de la aplicación de buenas prácticas y el uso adecuado de las cuentas de usuario así como también concientizar a los funcionarios de la Administración Departamental sobre la importancia y las responsabilidades individuales que tienen con la información a su cargo. Por lo cual no es permito que de un funcionario a otro se intercambien roles y/o cuentas de usuario para accesos al sistema.

En el caso de que se requieran cuentas públicas o compartidas, se deben proporcionar los mecanismos para su identificación.

ADMINISTRACIÓN DE ACCESO DE USUARIOS Y PRIVILEGIOS	
Activos relacionados:	Aplicaciones Informáticas
	Servicios
	Datos

La oficina de recursos humanos debe notificar las novedades de los funcionarios (retiro, ingreso, licencias, vacaciones) a la oficina de Sistemas para asignarle los permisos correspondientes, creación de usuario para la red y anulación en caso de retiro. Es importarte definir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

Es necesario tener documentados y actualizados los privilegios de los grupos de usuarios, no se debe otorgar más privilegios de los que se requiera.

En caso de que se necesiten privilegios temporales, estos deben ser retirados en el momento que ya no se requieran.

La Oficina de Sistemas debe establecer procedimiento para la revisión periódica de los derechos de acceso de los usuarios de la Entidad.

USO DE CONTRASEÑAS	
Activos relacionados:	Aplicaciones Informáticas
	Servicios
	Datos

Los diferentes sistemas de información que conforman la plataforma tecnológica de la gobernación de Putumayo, incluyen características de restricción de contraseñas, que se aplican a la duración, la sintaxis y repetición. Se deben activar dichas restricciones y mantener una documentación de las características para las mismas. El Comité de Seguridad de la Información del área de sistema de información de la Gobernación, ha definido los valores de los parámetros de configuración de contraseñas:

- ✓ Características de la clave: Las Contraseñas no deben contener datos como el nombre ni apellidos de los usuarios, y debe contener números letras y algún carácter especial.
- ✓ Bloqueo por intentos incorrectos: SI
- ✓ Mínimo 8 caracteres de longitud para estaciones de trabajo.
- ✓ Mínimo 12 caracteres de longitud para servidores, equipos activos de red, dominios.
- ✓ Duración del conteo de intentos incorrectos: 5 Veces
- ✓ Historial de claves empleadas: ACTIVADO, es decir no se podrán utilizar las últimas tres contraseñas empleadas con anterioridad.
- ✓ Se deben cambiar cada treinta (30) días para estaciones de trabajo.
- ✓ Se deben cambiar cada dos (2) meses para servidores, equipos activos de red, dominios, etc.

Se debe concientizar y exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.

RESPONSABILIDADES DE LOS USUARIOS	
Activos relacionados:	Aplicaciones Informáticas
	Servicios
	Datos
	Personas

Si un funcionario se ausenta por cualquier motivo o razón no está permitido ingresar al sistema sin su autorización a excepción de que el jefe inmediato lo permita.

Cada funcionario es responsable del contenido y uso del correo institucional.

Es importante que los funcionarios eviten malas prácticas para el manejo de contraseñas ya que la responsabilidad recae sobre cada usuario.

No se debe almacenar las contraseñas en lugares como hojas de papel, agendas, cuadernos de notas o lugares de fácil acceso.

Los equipos de cómputo de la entidad deben tener configurado la opción de cierre de sesión después de un tiempo de inactividad, bloqueando la cuenta con contraseña al momento que requiera ausentarse.

Los funcionarios son responsables de proteger su información personal, la Entidad no se hace responsable por la pérdida de esta.

Los usuarios deben reportar al profesional universitario del área de Sistemas o al personal de apoyo del área cualquier daño, vulnerabilidad, riesgo o amenaza detectada.

COPIAS DE SEGURIDAD	
Políticas relacionadas:	Política de Registro y Auditoria
	Política de Aplicación General

Se deben realizar y mantener copias de seguridad de la información de la entidad, que lo amerite de acuerdo con su clasificación. Dichas copias deben seguir un estándar en cuanto a número, antigüedad, rotulación y lugar de almacenamiento, ya sea interno o externo de acuerdo al procedimiento establecido por el Sistema Integrado de Gestión de la Administración Departamental PT-GTI-007 PROCEDIMIENTO DE RESPALDO Y PROTECCIÓN DE LA INFORMACIÓN.

El personal del área de Sistemas encargado de este proceso debe diligenciar el formato FT-GTI-004 FORMATO DE CONTROL DE BACKUP y cumplir el procedimiento establecido.

RESTAURACIÓN DE LA INFORMACIÓN	
Activos relacionados:	Datos
Todos los sistemas de información que componen la plataforma de la entidad, deberán incluir la documentación necesaria para garantizar la ejecución de tareas de recuperación de la información. Cada procedimiento de restauración de información deberá incluir las funciones y responsabilidades del personal participante en la restauración de la misma.	

SOFTWARE DE LOS EQUIPOS DE CÓMPUTO	
Activos relacionados:	Aplicaciones informáticas
	Personas
Mientras el sistema operativo lo permita, la cuenta administrador debe ser renombrada y el nuevo nombre no debe hacer referencia a las características de la cuenta. Las estaciones de trabajo de los funcionarios deben estar configuradas y vinculadas al sistema de dominio de la Entidad, en el cual se han configurado directivas como: No está permitido la instalación de aplicaciones, ingreso de dispositivos de almacenamiento USB, cambiar la página de inicio del navegador predeterminado, entre otras. Es responsabilidad de los funcionarios almacenar su información únicamente en la partición del disco duro destinada para tal fin. Todos los equipos de cómputo de la entidad deben tener instalado y debidamente actualizado el Antivirus. El personal encargado del área de Sistemas periódicamente debe realizar el seguimiento de los equipos de cómputo conectados a la red de la entidad y realizar la actualización de las base de datos de firmas del antivirus de acuerdo al fabricante.	

El área de sistemas debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

CAMBIOS A LOS PAQUETES DE SOFTWARE	
Activos relacionados:	Aplicaciones informáticas

Se deben controlar todos los cambios o modificaciones a los paquetes de software, y limitarlos a los cambios necesarios, los paquetes de software suministrados por terceras partes, se deben usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deben tener en cuenta los siguientes puntos: El riesgo de que los procesos de integridad y de control incorporados se vean comprometidos y si es necesario, obtener el consentimiento del vendedor.

Cuando se cambian los sistemas operativos o las aplicaciones críticas para la entidad se deben revisar y realzar las pruebas necesarias para garantizar las operaciones y la seguridad de la organización.

El área de Sistemas no se responsabiliza por el software (aplicaciones) instalado en equipos ajenos a la administración departamental, tampoco de realizar la configuraciones o instalaciones en aquellos equipos.

SERVIDORES	
Activos relacionados:	Equipos informáticos

Los servidores que proporcionan los servicios a la entidad deberán:

- ✓ Funcionar las todos los días con el fin de garantizar la disponibilidad del servicio (A excepciones programadas).
- ✓ Ser monitoreados por el personal asignado en el área de Sistemas.
- ✓ Recibir mantenimiento preventivo mínimo dos veces al año y recibir mantenimiento semestral que incluya depuración de logs (de acuerdo al plan de mantenimiento)
- ✓ Recibir mantenimiento anual que incluya la revisión de su configuración.

Los Servidores de la entidad no deben ser empleados como estaciones de trabajo, ni tener instaladas aplicaciones de usuario final, tales como

navegadores y clientes de correo electrónico, así como tampoco software de escritorio.

Las excepciones a esta recomendación deben estar documentadas y aprobadas por el profesional universitario del área de Sistemas, en el caso de que algunos servidores requieran la instalación de software de usuario final para el funcionamiento de aplicaciones.

Los usuarios con derechos de administrador deben tener dos cuentas distintas, una de uso administrativo y otra para tareas generales. Se debe usar la cuenta con privilegios de administrador sólo cuando se tenga que realizar en el servidor trabajos que requieran de estos privilegios.

CORREO ELECTRÓNICO	
Activos relacionados:	Servicios
	Personas

La oficina de Sistemas se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra y la información contenida en la mensajería electrónica debe tener la protección adecuada.

La gestión de contraseñas será suministrada por el servidor de dominio de la entidad de acuerdo a las directivas configuradas ya que cada cuenta se autenticara con el mismo usuario asignado a cada host.

Los mensajes enviados a través del sistema de correo electrónico de la entidad no podrán incluir contenidos ofensivos (lenguaje/imágenes vulgares u ofensivas).

Para la creación, modificación y desbloqueo de una cuenta de correo se debe dar cumplimiento al PT-GTI-002 PROCEDIMIENTO PARA LA ADMINISTRACIÓN Y SOPORTE DE CORREOS INSTITUCIONALES, así como también el diligenciamiento del FT-GTI-006 FORMATO DE SOLICITUD DE CREACION, MODIFICACIÓN O ELIMINACIÓN DE CUENTA CORREO CORPORATIVO.

La oficina de recursos humanos debe reportar las novedades de ingreso y retiro de los funcionarios a la oficina de sistemas con el fin de cerrar u proceder habilitar la cuenta.

Los funcionarios del servicio de correo electrónico deben conocer la importancia

del buen uso del mismo y concientizarse de los peligros la entidad se expone por su mal uso como ataque de virus, spam, intercepción, descargar archivos adjuntos infectados, etc. El servicio de correo electrónico, tanto interno como externo deberá ser usado única y exclusivamente para intercambio de información de interés institucional, quedando prohibido la suscripción a cualquier sitio web con el mail corporativo.

DE ACCESO A TERCEROS	
Activos relacionados:	Personas
	Aplicaciones informáticas
	Servicios
Los usuarios considerados como terceros son los proveedores, personal externo o personal que tenga algún tipo de relación con la entidad. Para garantizar el acceso de terceros a los sistemas de la entidad se deben identificar en el área de Sistemas previa autorización del jefe de área o funcionario responsable del proceso. La asignación de privilegios será limitada de acuerdo a tiempo y las actividades a realizarse. Los usuarios terceros deben aceptar los acuerdos y políticas de seguridad dispuestas internamente en la entidad además de las exigidas puntualmente dentro del documento del contrato (Si aplica). La red inalámbrica (LIBREGOB) es un servicio que permite conectarse a personal externo de la entidad (usuarios, proveedores) a internet sin la necesidad de algún tipo de autenticación, esta red de invitados permitirá utilizar los servicios de Internet, en las zonas de cobertura de Gobernación; los usuarios invitados no tendrán acceso a la Red de la entidad ni a ningún recurso de uso privado.	

6.3.7 Políticas de redes y comunicaciones

ACCESO A LA RED DE DATOS DE LA ENTIDAD	
Activos relacionados:	Servicios
	Aplicaciones informáticos
Todos los equipos que no hagan parte del inventario tecnológico de la Gobernación de Putumayo, sean de propiedad de funcionarios o contratistas de la entidad; deben tener instalado y actualizado un ANTIVIRUS para poder ser ingresados a la red de la Gobernación y de esta manera tener los servicios de Impresora, Mensajería interna, e Internet. No se permitirá el ingreso a la red de datos de equipos de cómputo que tengan el antivirus vencido o versión de prueba. Cada equipo que se requiera ingresar a la red de datos de la Gobernación y obtener los servicios ya mencionados anteriormente debe ser revisado y registrado en el formato FT-GTI-005 LISTADO DE DIRECCIONES MAC DE EQUIPOS CONECTADOS A LA RED (Sistema Integrado de Gestión) por el personal encargado del área de Sistemas, para determinar que estos no se encuentran infectados y disponen del ANTIVIRUS actualizado.	

EQUIPOS DE REDES Y CONFIGURACIÓN	
Activos relacionados:	Redes de comunicaciones
	Equipos informáticos
Todos los puertos y protocolos de los dispositivos utilizados en la red, que no estén en uso deberán ser bloqueados adecuadamente. Al momento de diseñar o realizar cambios en la red se deberá considerar todas las medidas de seguridad y ventajas que los equipos de red estén en capacidad de proveer en lo posible utilizando equipos de alta tecnología. Todos los dispositivos de red deberán estar correctamente salvaguardados, tomando en cuenta aspectos como ubicación, protección física y suministro eléctrico. El personal que realiza trabajos de configuración de los dispositivos de red deberá prestar debidamente capacitado o tener una certificación o título que	

respalde sus capacidades y conocimientos.

Se debe definir un proceso de reemplazo de equipos, ya sea a través de acuerdos con proveedores (precios, tiempo de reposición, disponibilidad) o si es posible mantener respaldo en Almacén.

La oficina de Sistemas es la responsable de proporcionar el servicio de acceso remoto y las políticas de acceso y autenticación a los recursos informáticos disponibles en la entidad.

CONTROL DE CONTENIDOS Y USO DE INTERNET	
Activos relacionados:	Datos
	Redes de comunicaciones

El acceso a Internet será restringido, este será suministrado solamente para los funcionarios de la entidad que necesiten el servicio para realizar labores propias de la administración de departamental.

Los funcionarios de la entidad deben utilizar el servicio de internet de forma responsable y eficiente, este solo se debe limitar a las actividades relacionadas con las funciones del cargo.

Todos los sitios y descargas serán susceptibles de supervisión y/o bloqueo por parte de entidad, si se consideran perjudiciales y/o improductivos para la administración departamental.

La infraestructura tecnológica, los equipos y los servicios utilizados para acceder a internet pertenecen a la gobernación de Putumayo y la entidad se reserva el derecho a supervisar el tráfico de internet y a acceder a los datos de sitios visitados, y servicios utilizados.

Queda prohibida la instalación de aplicaciones de mensajería instantánea, solo el autorizado por la entidad (Openfire – Spark).

Si un funcionario no está seguro de qué un servicio o portal visitado constituye un uso aceptable de internet, deberá consultar con el personal del área de Sistemas y solicitar más información y asesoramiento al respecto.

6.3.7 Políticas de manejo de hardware y seguridad física

CONTROL DE ACCESO FÍSICO	
Activos relacionados:	Equipos informáticos
	Instalaciones
	Equipamiento auxiliar

Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

Todos los funcionarios y contratistas deben portar su carnet para el ingreso a las instalaciones de la Gobernación de Putumayo, así como también realizar su registro en la entrada en los medios que disponga la Entidad.

Únicamente el personal del área de Sistemas puede ingresar al centro de datos, cuando un funcionario no autorizado o visitante requiera ingresar al cuarto del centro de datos, debe solicitar autorización mediante comunicación interna a la oficina de Sistemas encargada del proceso de Gestión de Tecnología e información o a la Secretaria de Servicios Administrativos Departamental.

MANTENIMIENTO Y SEGURIDAD FÍSICA	
Activos relacionados:	Equipos informáticos
	Instalaciones
	Redes de comunicaciones

Se debe mantener actualizado el inventario de todos los equipos y dispositivos que formen parte de la infraestructura tecnológica de la Entidad, debe incluir características como: fecha de adquisición, proveedor, modelo, responsable, garantía, y demás aspectos que la oficina responsable estime conveniente, además de contener la hoja de vida del estado actual del equipo y las configuraciones o mantenimientos realizados.

La oficina de sistemas adscrita a la Secretaria de Servicios Administrados debe realizar el mantenimiento periódico preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física en informática, y su acondicionamiento específico, de acuerdo con el procedimiento establecido en la entidad: PT-GTI-004 PROCEDIMIENTO DE MANTENIMIENTO PREVENTIVO DE EQUIPOS DE SISTEMAS y PT-GTI-005 PROCEDIMIENTO DE MANTENIMIENTO CORRECTIVO DE HARDWARE.

Es responsabilidad del Profesional Universitario de la oficina de Sistemas planear adecuadamente los horarios de mantenimiento de los equipos en jornadas que no afecten el normal funcionamiento de las actividades de la Administración Departamental.

Otro aspecto importante cuando se vaya a realizar mantenimiento en alguno de los equipos, se debe dar aviso con anticipación al usuario.

El cambio de lugar de un equipo de cómputo se debe realizar con la autorización de personal de la oficina de Sistemas, los cuales dispondrán de las condiciones adecuadas para su traslado tales como: puntos de red, eléctrico y demás aspectos; así como también se debe actualizar en el inventario las razones de cambio, y el nombre del nuevo responsable si lo hay.

Los equipos de cómputo, cables, UPS, planta eléctrica, aires acondicionados, dispositivos de almacenamiento y de comunicación inalámbrica, deben estar amparados en pólizas contra robo, pérdida, daño o acceso no autorizado.

No está permitido el consumo de líquidos, alimentos, ni humo dentro de los centros de datos o lugares donde se encuentren los equipos.

DOTACIÓN Y PROTECCIÓN DEL CENTRO DE CÓMPUTO	
Activos relacionados:	Equipamiento auxiliar
	Instalaciones

Se deben implementar mecanismos de seguridad física como detectores de humo, medidores de temperatura, sensores de movimiento, aire acondicionado, cableado debidamente instalado, puertas blindadas y demás elementos en las áreas donde se encuentran los equipos de comunicación y de computo propiedad de la entidad con el fin de protegerlos .

Las instalaciones de comunicaciones y eléctricas, deben estar protegidas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

El área de sistemas debe contar con un plano actualizado de las instalaciones de red de comunicaciones y eléctricas de la Entidad.

CONTROL DE MEDIOS DE ALMACENAMIENTO	
Activos relacionados:	Datos

Deben existir procedimientos para la gestión de medios Removibles.

Los medios deben ser eliminados de manera segura y sin peligros (técnica, ambiental e industrialmente), usando procedimientos formales.

Todo medio ya sea documentos en papel, CD y DVD que contenga datos confidenciales de la entidad y se requieran destruir se deben realizar a través de la destructora de Papel ubicada en el área de Sistemas de la Entidad.

Los procedimientos para la manipulación y almacenamiento de información deben ser establecidos para proteger la información de la divulgación no autorizada, o un mal uso.

Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer las copias de seguridad y el personal encargado de su protección.

6.3.8 Políticas de Seguridad Legal

LICENCIAMIENTO DE SOFTWARE	
Activos relacionados:	Aplicaciones informáticas

Se prohíbe en la gobernación de Putumayo software y aplicaciones no autorizadas y sin licenciamiento en los sistemas de la Entidad.

El área de Sistemas de la gobernación es la única que autoriza la instalación de software el cual debe contar con licencias de propiedad de la entidad.

Se debe mantener actualizado el inventario de licencias y revisar cada vez que se vaya a instalar software en uno de los equipos de la entidad.

De igual forma, los terceros o contratistas que tengan equipos propios dentro de las instalaciones de la Gobernación deberán hacerse responsables por las licencias del software instalado en dichos equipos.

Se considera una falta grave que los usuarios, instalen cualquier tipo de

programa en sus computadores, servidores, estación de trabajo u otros equipos conectados a la red de a entidad que no esté autorizado por la oficina de Sistemas.

La Oficina Sistemas debe establecer un cronograma para realizar las revisiones periódicas que permita asegurar el cumplimiento de los requisitos legales y reglamentarios sobre la propiedad intelectual en la Entidad.

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Activos relacionados:	Inventario de activos

La oficina de Sistemas encargada del proceso de gestión de Tecnología e Información con el apoyo de la alta dirección (Gobernador y Secretarias) deben crear un plan de contingencias informáticas que contenga al menos los siguientes puntos:

- ✓ Identificar los sucesos que pueden ocasionar interrupciones en los procesos de la entidad así como también identificar los riesgos, y las consecuencias para la seguridad de la información.

- ✓ Contar con procedimientos informáticos alternos que permitan continuar con la operación de la Entidad.

- ✓ Tener los respaldos de información en un lugar seguro, fuera del perímetro físico donde se encuentran los equipos.

- ✓ Tener el apoyo de medios magnéticos o en forma física (documentos), de los proceso necesarios para reconstruir los archivos dañados.

- ✓ Se debe disponer de los planes necesarios para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempos requeridos, después de la interrupción o la falla de los procesos críticos para la entidad; para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.

- ✓ Es importante tener un directorio actualizado del personal interno o externo de soporte, a los cuales se pueda llamar en el momento que se presente las fallas.

- ✓ Ejecutar pruebas de la funcionalidad y revisiones periódicas del plan de acuerdo a la identificación de prioridades para asegurar su actualización y su eficacia.

6.3.9 Restricciones

Las políticas definidas anteriormente se establecen como un firme compromiso por parte de todos los funcionarios de la **GOBERNACIÓN DE PUTUMAYO** y así mismo deben ser divulgarlas a través de toda la organización siendo implementados de forma que genere confianza y garantice la funcionalidad de los sistemas de Entidad:

- Sé prohíbe intentar evadir o violar la seguridad o autentificación de usuario de cualquier host, red o cuenta.

- Sé prohíbe a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma.

- Sé prohíbe el almacenamiento, instalación, configuración, o uso de software ilegal o no autorizado o de datos no autorizados en los equipos informáticos de la **Gobernación Putumayo**.

- Sé prohíbe el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.

- Sé prohíbe el hurto, robo, sustracción ó uso no autorizado de: datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos de la **Gobernación de Putumayo**.

- Sé prohíbe el acceso, modificación o alteración no autorizada de componentes, datos o información de los activos informáticos de la **Gobernación de Putumayo.**

- Sé prohíbe el uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes

de fuentes no certificadas o de terceros, sin la previa revisión y autorización del área de Sistemas.

- Sé prohíbe el almacenamiento y reproducción de aplicaciones, programas o archivos de audio o video que no están relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.

- El software y hardware, se debe verificar para asegurar que son compatibles con otros componentes del sistema.

- Sé prohíbe la instalación de juegos y/o software diferente al instalado y autorizado por el profesional responsable de la Oficina de Sistemas de la **Gobernación de Putumayo.**

6.3.10 Excepciones

- Cuando se realicen eventos, capacitaciones, talleres, conferencias o visitas de personal externo que requieran hacer uso de los servicios de la red de datos de la Gobernación, se podrán habilitar equipos de manera temporal por el tiempo necesario, previa solicitud del jefe área interesado.

- En el caso de ser necesario habilitar servicios restringidos (redes sociales, YouTube u otros portales), también se deberá realizar la solicitud justificada por parte del jefe de área responsable del proceso.

- Entre las directivas de seguridad dispuestas por la entidad se encuentra configurado el firewall para restringir algunas palabras y sitios de Internet; por lo tanto pueden existir portales que a pesar de ser inofensivos están restringidos su acceso, en este caso, los funcionarios pueden notificar al área de Sistemas para habilitarlos.

7. CONCLUSIONES

En la actualidad de la era digital, el uso de las tecnologías de información es un aspecto importante que requieren las entidades u organizaciones para cumplir efectivamente su misión u objetivos propuestos; por tal razón la gestión correcta de los riesgos representa un papel fundamental en la protección de los diferentes activos de información.

La información es el activo más valioso de cualquier entidad o empresa, por lo cual se debe diseñar las estrategias más efectivas que conlleve a mitigar el impacto de los posibles riesgos cerrando las brechas de los mismos, para lograrlo se puede determinar a partir de un buen análisis y evaluación de los riesgos.

Al realizar el proceso de análisis de riesgos de la gobernación de Putumayo se evaluó las vulnerabilidades, amenazas y el impacto que se podría generar si estas se materializan así como también la criticidad de los riesgos por cada grupo de activos identificados en la entidad, dicho diagnóstico nos permite conocer el estado actual de la seguridad de la información y facilitar la toma decisiones para la mejora de la seguridad en la información.

El factor humano representa un alto nivel de riesgo de seguridad, porque a pesar de tener un buen sistema de seguridad resulta inútil resguardar los activos informáticos si los funcionarios no hacen uso de las buenas prácticas y de las políticas de Seguridad de la entidad.

Las políticas de seguridad permiten proteger y salvaguardar la información de la entidad y sus activos de la gran cantidad de amenazas a las cuales pueden estar expuestos a fin de garantizar la continuidad de los sistemas de información, disminuir los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de las entidades del Estado.

Finalizado el proyecto se obtiene el resultado de todos los objetivos propuestos y a través del documento de las políticas de la seguridad de la información permitirá optimizar y fortalecer los procesos de la Administración Departamental.

La gobernación de Putumayo actualmente presenta un nivel de riesgo informático considerable, que necesita atención y la aplicación inmediata de las políticas y

controles así como también el apoyo de los cargos de dirección (Gobernador y Secretarias de despacho) y de los jefes de área.

8. RECOMENDACIONES

Se recomienda realizar la socialización del proyecto “DISEÑO DE LAS POLÍTICAS DE CONTROL DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SEDE CENTRAL DE LA GOBERNACIÓN DEL PUTUMAYO (MOCOA)” con el fin de dar a conocer el resultado a los funcionarios de la entidad y de esta manera adoptar las mejoras o actualización que se puedan plantear al documento de las políticas de seguridad de la información de la Gobernación de Putumayo.

Es importante que todos los funcionarios y contratistas de la entidad se capaciten en cada uno de los temas de las políticas de seguridad de la información y se concienticen en la aplicación de buenas prácticas para lograr un óptimo resultado en todo el proceso de implementación.

Para lograr una estabilidad y buena aplicación de actividades en pro de fortalecer el sistema de seguridad de la Entidad se recomienda también capacitar al personal del área de sistemas e invertir los recursos necesarios para fortalecer esta área.

Es necesario se priorice la elaboración de un plan de continuidad de negocios que permita identificar las acciones que se deben llevar a cabo y los procedimientos a seguir en el caso de la presencia de un daño o siniestro que afecte la disponibilidad de los sistemas de información de la Entidad.

Se recomienda fortalecer y rediseñar los temas de Auditorías, que permitan incluir temas de seguridad informática con el fin de realizar el análisis, gestión y seguimiento de los sistemas de información y la verificación de las políticas de seguridad con personal especializado en el tema.

BIBLIOGRAFÍA

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (12 diciembre 2014). *Decreto Nacional N° 2573, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.",* PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA año 2014.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Compendio, tesis y otros trabajos de grado. NTC 1486. Sexta actualización. Bogotá, ICONTEC, 2008.

CASTAÑO, Wilson. Material de Apoyo curso PROYECTO DE SEGURIDAD INFORMATICA II: 233013ª, Universidad Nacional Abierta y a Distancia UNAD. Enero 2015.

DÍAZ BURBANO, Jimmy Harold Gobernador de Putumayo. PLAN DE DESARROLLO DEPARTAMENTAL DEL PUTUMAYO 2012 – 2015 "PUTUMAYO SOLIDARIO Y COMPETITIVO", 2012-2015.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Manual 3.1 para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia. 2014.

RAMIREZ G, E. (2010). Diseño metodológico preliminar. Recuperado de: http://metodologiaparainvestigacion.blogspot.com/2010/06/esquema-tematico-del-marco-teorico.html

Universidad del Atlántico (s.f). 6. Diseño Metodológico Preliminar. Disponible en Internet: http://www.uniatlantico.edu.co/uatlantico/sites/default/files/docencia/facultades/pdf/ciencias-juridicas/guia%20_monografia_diseno_metodologico.pdf

PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA

CORPORATIVA, PROPOLSINECOR. Disponible en: http://hdl.handle.net/10596/2742

ANÁLISIS, EVALUACIÓN DE RIESGOS Y ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DE PAMPLONA - NORTE DE SANTANDER. Disponible en Internet: http://hdl.handle.net/10596/3415

ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA. Disponible en Internet: http://hdl.handle.net/10596/2655

ANÁLISIS Y GESTIÓN DEL RIESGO DE LA INFORMACIÓN EN LOS SISTEMAS DE INFORMACIÓN MISIONALES DE UNA ENTIDAD DEL ESTADO, ENFOCADO EN UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN. Disponible en Internet: http://repository.unad.edu.co/handle/10596/3423

GOBIERNO Y MODELADO DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES. Disponible en Internet: http://e-archivo.uc3m.es/handle/10016/11898

Aislamiento y sellado adecuado del centro de proceso de datos CPD. Disponible en Internet: http://www.cliatec.com/blog/aislamiento-y-sellado-adecuado-del-centro-de-proceso-de-datos-cpd

Guía de referencia de Nmap, Disponible en Internet: https://nmap.org/zenmap/

Portal web del departamento de Putumayo, Disponible en Internet: www.putumayo.gov.co

EAR / PILAR Entorno de análisis de riesgos. Disponible en Internet: http://www.ar-tools.com/es/index.html

Lección 12: Metodología MAGERIT. Disponible en Internet:: http://datateca.unad.edu.co

Estrategia de Gobierno en Línea. Disponible en Internet: http://estrategia.gobiernoenlinea.gov.co

ANEXOS

Anexo A. Oficios de Solicitud de Viabilidad a la Entidad y respuesta.

UNAD Universidad Nacional Abierta y a Distancia

Especialización en seguridad Informática
Propuesta de trabajo de Grado

Mocoa Putumayo, 18 de Mayo del 2015

Doctora
PILAR ANDREA MARÍN ARTEAGA
Secretaria de Servicios Administrativos
Gobernación de Putumayo

REF: Solicitud de viabilidad propuesta de Trabajo de Grado, Especialización en seguridad Informática – UNAD.

Cordial saludo,

Como estudiantes de la Universidad ABIERTA y a Distancia - UNAD de la Escuela de Ciencias Básicas, Tecnología e Ingeniería, Especialización en Seguridad INFORMÁTICA se requiere como requisito de grado la elaboración de un proyecto de investigación, para lo cual hemos tomado como referente la Administración departamental, con el fin de contribuir con nuestro conocimiento y fortalecer el proceso de Gestión de Tecnología e información de la administración departamental específicamente en el tema de seguridad de la información.

Por lo anterior comedidamente solicitamos la autorización de esta propuesta para el desarrollo y aplicación del trabajo de grado denominado: DISEÑO DE LAS POLÍTICAS DE CONTROL DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SEDE CENTRAL DE LA GOBERNACIÓN DEL PUTUMAYO (MOCOA).

Agradecemos su atención y esperamos contar con su apoyo.

Cordialmente,

LEYDA LILIANA CORDOBA ARAUJO
Código: 1124848759

WILSON CAMILO DELGADO TRUJILLO
Código: 18130014

Anexo. Anteproyecto

Anexo A. Oficios de Solicitud de Viabilidad a la Entidad y respuesta.

PUTUMAYO

REPUBLICA DE COLOMBIA
GOBERNACIÓN DEL PUTUMAYO
"Marca la diferencia"

Secretaria de Servicios Administrativos

Putumayo
Solidario y Competitivo

Mocoa Putumayo, 25 de Mayo del 2015

Ingenieros
LEYDA LILIANA CORDOBA ARAUJO
WILSON CAMILO DELGADO TRUJILLO
Estudiantes UNAD

REF: Autorización elaboración del Anteproyecto de Grado en La Entidad

Cordial saludo,

Por medio de la presente se comunica la autorización a los estudiantes de la Universidad ABIERTA y a Distancia - UNAD, Especialización en Seguridad INFORMÁTICA la elaboración de un proyecto de grado denominado: DISEÑO DE LAS POLÍTICAS DE CONTROL DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SEDE CENTRAL DE LA GOBERNACIÓN DEL PUTUMAYO (MOCOA), el cual se desarrolladora en la Administración departamental y contara con el apoyo necesario en cuanto a información y disposición del personal de las áreas que se requiera.

La coordinación y dirección del proyecto estará a cargo del profesional universitario del Área de Sistemas, suscrita a la Secretaría de Servicios Administrativos Departamental.

Cordialmente,

PILAR ANDREA MARÍN ARTEAGA
Secretaria de Servicios Administrativos
Gobernación de Putumayo

Reviso, Andrés Trejo
Profesional U. Área de Sistemas

Palacio Departamental Mocoa Calle 8 No. 7–40, Código Postal: 860001
Conmutador (57+8) 4206600 - Fax: 4295196 - Pagina web: www.putumayo.gov.co

Anexo B. Encuesta

REPUBLICA DE COLOMBIA
GOBERNACIÓN DEL PUTUMAYO
"Marca la diferencia"

Secretaria de Servicios Administrativos

4. SEGURIDAD DE LA INFORMACIÓN:

¿Conoce la importancia y la necesidad de proteger la información? si su respuesta es afirmativa explique por qué?

SI X NO ___
la información hace parte del patrimonio de la entidad.

¿Conoce las políticas de seguridad de la información que deben ponerse en práctica para proteger la información de la Entidad?

SI ___ NO X

¿Ha perdido alguna vez información importante en su quipo de cómputo?

SI X NO ___

Si es afirmativa responda la siguiente información: ¿Según usted por qué sucedió?

- ☐ Virus informático
- ☒ Falla Física del equipo de cómputo
- ☐ Sin querer borro Información
- ☐ Otras razones. _____

El Almacenamiento en la Nube, es el modelo de servicio en el cual los datos se almacenan, se administran, y se respaldan de forma remota, en servidores que están en internet y que son administrados por un proveedor del servicio). **En qué casos considera usted necesario hacer uso de este servicio:**

- ☒ Para compartir la información con otras personas.
- ☒ Para almacenar información sensible (DNI, contraseñas, datos personales en general), ya sea propia o ajena, de tipo personal o corporativo.
- ☐ Para guardar archivos a modo de copia de seguridad.

¿Usted hace uso de las redes sociales?

SI X NO ___

Si es afirmativa responda la siguiente información: **Las redes sociales son un servicio que te permiten estar en contacto con otras personas, por eso: (Elija una respuesta):**

- ○ Compartes todo lo que haces con todos tus contactos, para eso es una red social.
- ⊘ Eres cuidadoso con la información que compartes y tienes bien configurados los niveles de privacidad.
- ○ Aceptas todas las solicitudes de amistad que recibes, te gusta tener muchos amigos, así tus publicaciones tienen más éxito (más "me gustas", compartidos, etc.).

Conoce algún tipo de estos ataques o vulnerabilidades que se pueden presentar en la actualidad:

1. Ciberacoso	SI ___	NO X
2. Ingeniería social	SI ___	NO X
3. Ciberdependencia	SI ___	NO X
4. Virus informático (Malware, Troyano, etc)	SI ___	NO X
5. Sexting y grooming	SI ___	NO X

Anexo C. Resultados Encuesta aplicada a los funcionarios

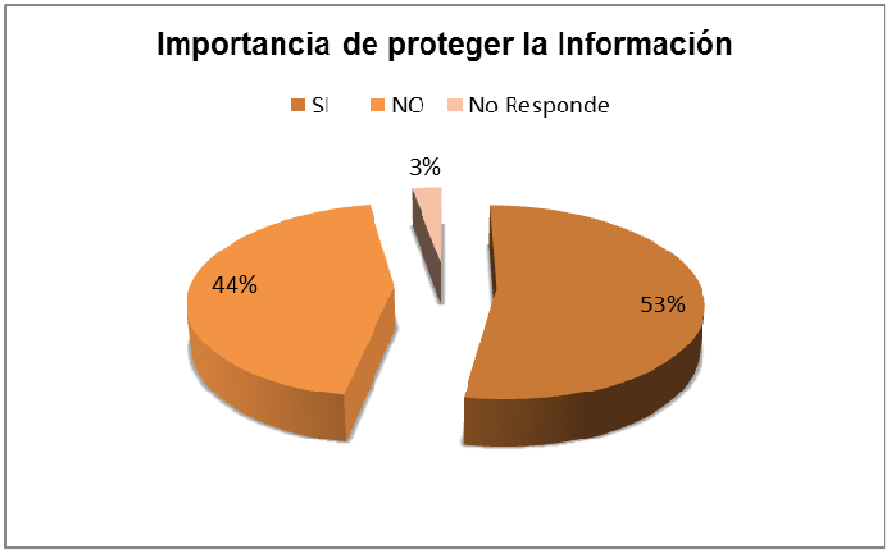
La información recolectada a través de la encuesta fue interpretada en forma cualitativa y cuantitativa, por medio del registro unificado de las respuestas, la tabulación y la deducción de la respectiva ponderación dada a cada uno de los aspectos considerados.

- ¿Conoce la importancia y la necesidad de proteger la información? Si su respuesta es afirmativa explique por qué?

Tabla 34. Importancia de Proteger la Información

Opciones de Respuesta	*Frecuencia*	*%*
SI	38	53
NO	32	44
No Responde	2	3
Total	**72**	100

Figura 20. Importancia de Proteger la Información



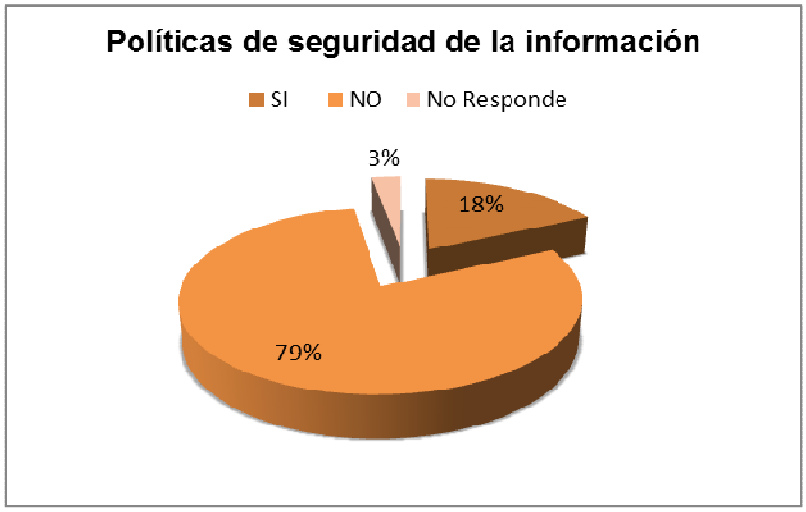
Fuente: Autores

¿Conoce las políticas de seguridad de la información que deben ponerse en práctica para proteger la información de la Entidad?

Tabla 35. Políticas de Seguridad de la Información

Opciones de Respuesta	*Frecuencia*	*%*
SI	13	18
NO	57	79
No Responde	2	3
Total	**72**	100

Figura 21. Políticas de Seguridad de la Información



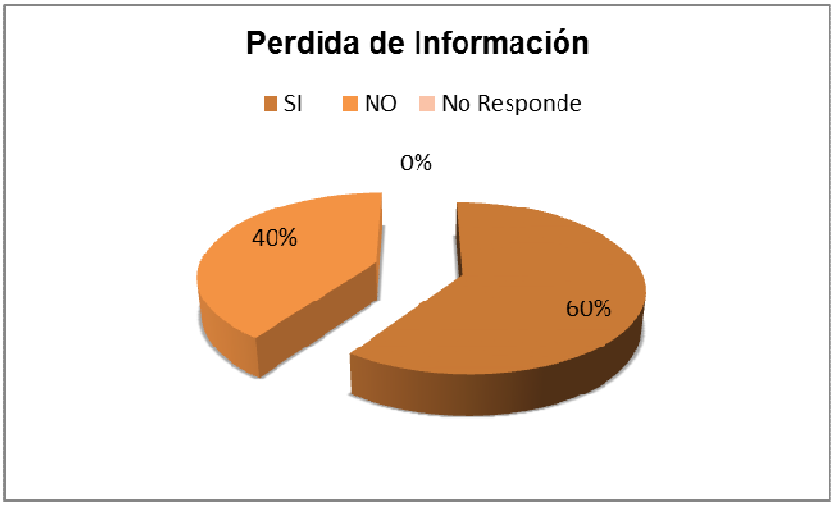
Fuente: Autores

- ¿Ha perdido alguna vez información importante en su equipo de cómputo?

Tabla 36. Pérdida de Información

Opciones de Respuesta	*Frecuencia*	*%*
SI	43	60
NO	29	40
No Responde	0	0
Total	**72**	100

Figura 22. Pérdida de Información



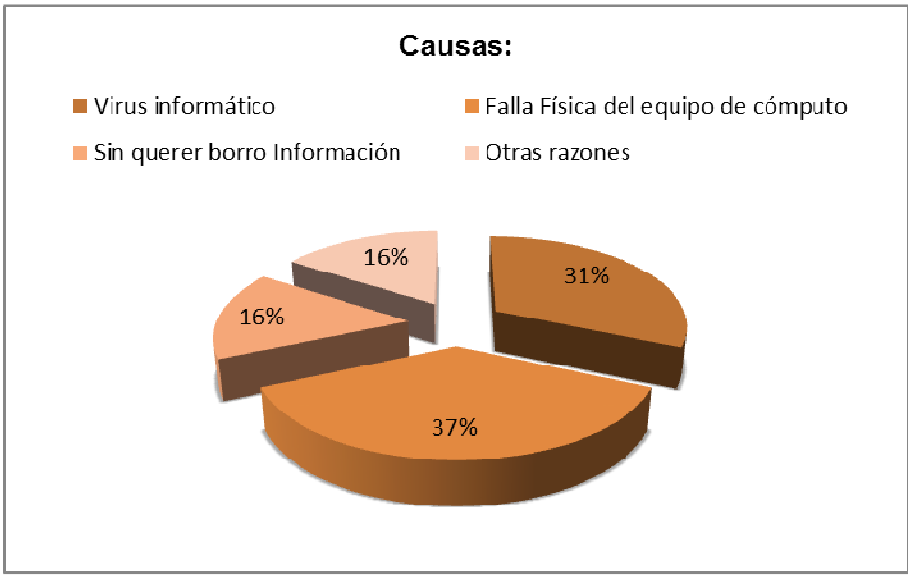
Fuente: Autores

- ¿Según usted por qué sucedió?

Tabla 37. Causas de la pérdida

Opciones de Respuesta	*Frecuencia*	*%*
Virus informático	18	31
Falla Física del equipo de cómputo	21	37
Sin querer borro Información	9	16
Otras razones	9	16
Total	57	100

Figura 23. Causas de la pérdida



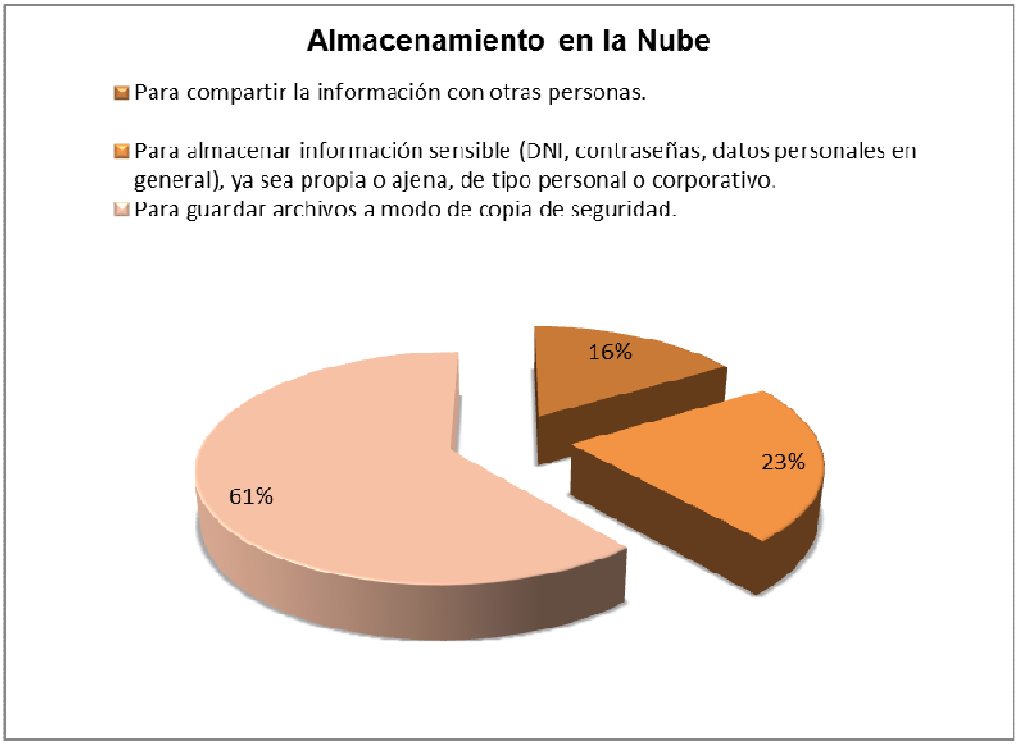
Fuente: Autores

- El Almacenamiento en la Nube, es el modelo de servicio en el cual los datos se almacenan, se administran, y se respaldan de forma remota, en servidores que están en internet y que son administrados por un proveedor del servicio). En qué casos considera usted necesario hacer uso de este servicio:

Tabla 38. Almacenamiento en la Nube

Opciones de Respuesta	*Frecuencia*	*%*
Para compartir la información con otras personas.	13	16
Para almacenar información sensible (DNI, contraseñas, datos personales en general), ya sea propia o ajena, de tipo personal o corporativo.	18	23
Para guardar archivos a modo de copia de seguridad.	49	61
Total	80	100

Figura 24. Almacenamiento en la Nube



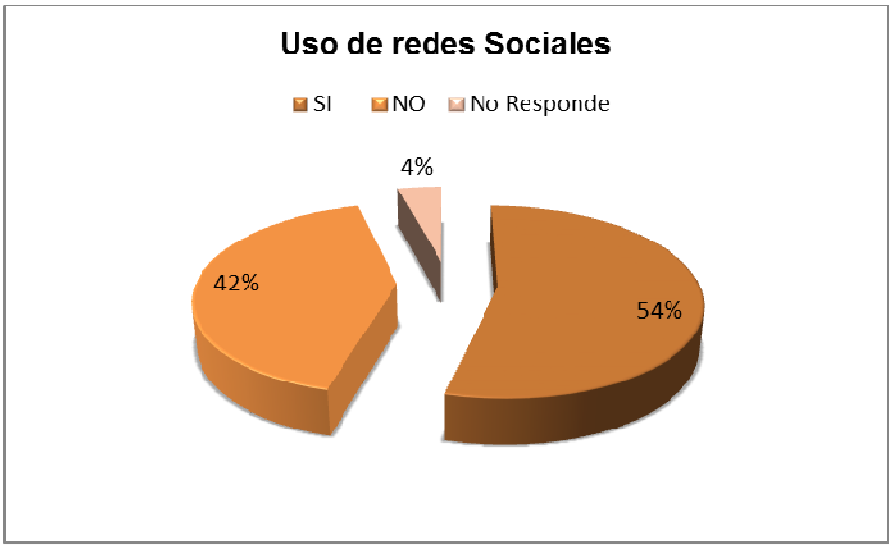
Fuente: Autores

- ¿Usted hace uso de las redes sociales?

Tabla 39. Uso de redes Sociales

Opciones de Respuesta	*Frecuencia*	*%*
SI	39	54
NO	30	42
No Responde	3	4
Total	72	100

Figura 25. Uso de redes Sociales



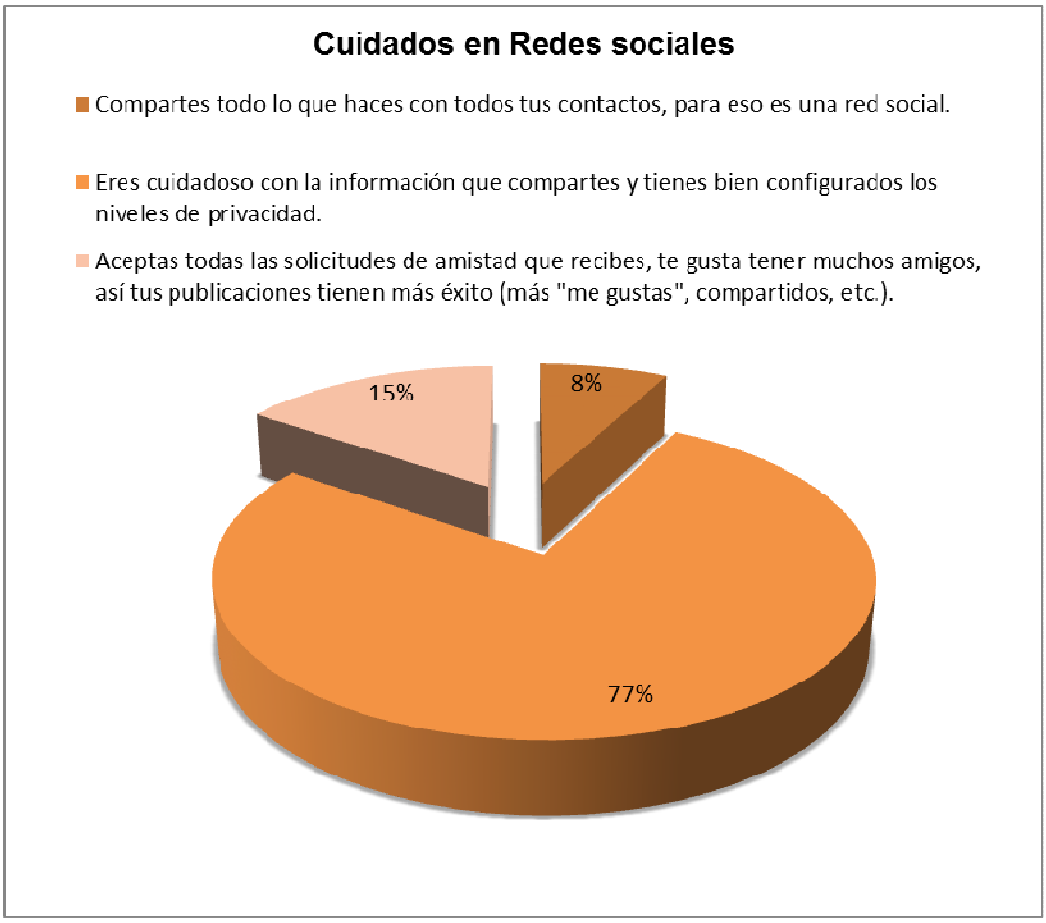
Fuente: Autores.

- Si es afirmativa responda la siguiente información: Las redes sociales son un servicio que te permiten estar en contacto con otras personas, por eso: (Elija una respuesta):

Tabla 40. Cuidados en Redes sociales

Opciones de Respuesta	*Frecuencia*	*%*
Compartes todo lo que haces con todos tus contactos, para eso es una red social.	3	8
Eres cuidadoso con la información que compartes y tienes bien configurados los niveles de privacidad.	30	77
Aceptas todas las solicitudes de amistad que recibes, te gusta tener muchos amigos, así tus publicaciones tienen más éxito (más "me gustas", compartidos, etc.).	6	15
Total	**39**	100

Figura 26. Cuidados en Redes sociales



Fuente: Autores.

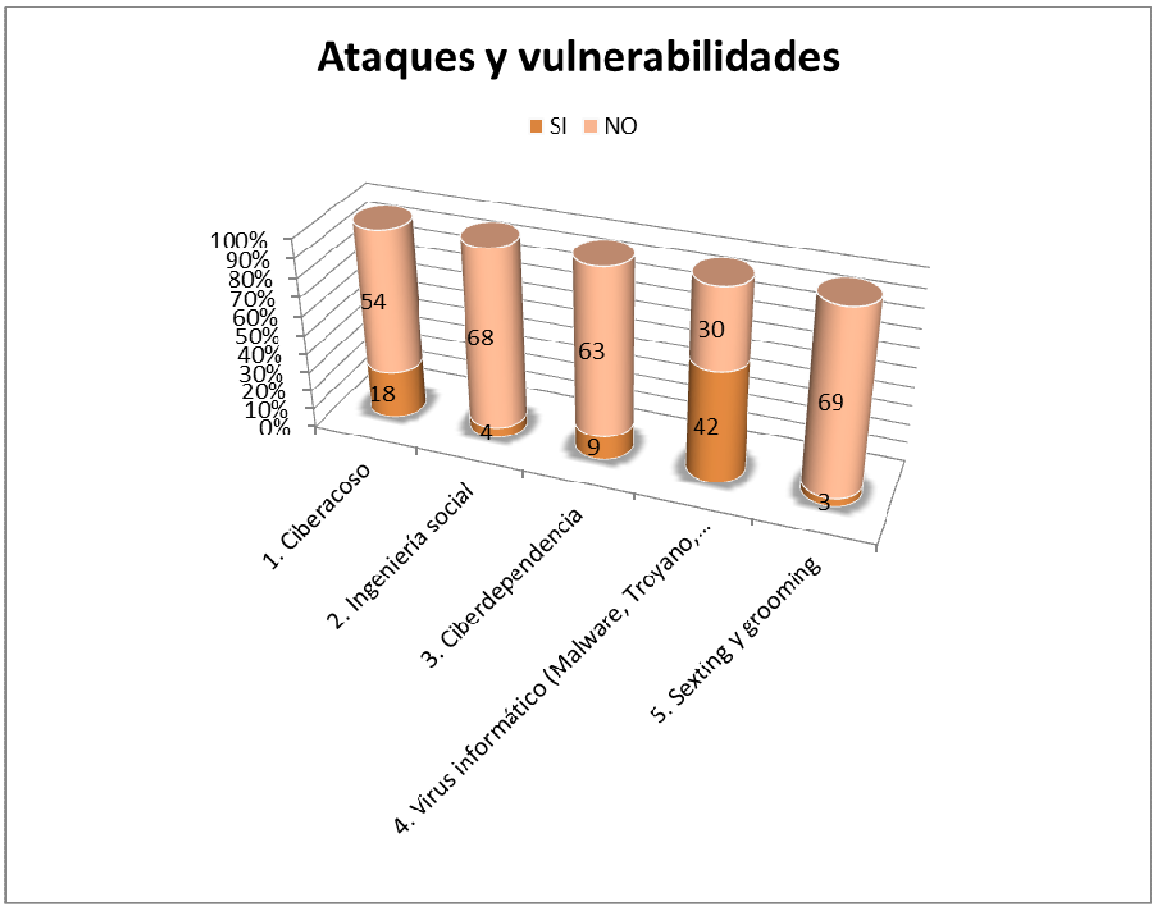
- Conoce algún tipo de estos ataques o vulnerabilidades que se pueden presentar en la actualidad:

Tabla 41. Ataques y vulnerabilidades.

Opciones de Respuesta	*SI*	*NO*	*Total*
1. Ciberacoso	18	54	72
2. Ingeniería social	4	68	72
3. Ciberdependencia	9	63	72
4. Virus informático (Malware, Troyano, etc)	42	30	72

5. Sexting y grooming	3	69	72

Figura 27. Ataques y vulnerabilidades.



Fuente: Autores.

Anexo D. Ficha técnica de encuestas

Tabla 42. Ficha Técnica

Tipo:	Muestral
Objetivo:	Criterio principal conocer y analizar la el nivel de conocimiento en cuanto al tema de seguridad de la información y analizar algunas prácticas y situaciones que han presentado en la Gobernación de Putumayo.
Periodo de trabajo de campo:	Tercera y cuarta semana de Junio 2015.
Población:	Encuesta aplicad a la muestra de los funcionarios de nómina de la parte central de la Entidad.
Universo presentado:	158 funcionarios de nómina.
Diseño de muestra:	Instrumento estructurado y con selección de encuestados por Muestreo aleatorio simple.
Tamaño de la muestra:	72 Encuestas
Preguntas formuladas	8 Preguntas
Técnica:	Presencial.
El nivel de confianza	75%
Error de estimación:	5%
Dirección:	LEYDA CÓRDOBA ARAUJO WILSON CAMILO DELGADO.

Fuente: Autores.

Anexo E. Análisis de los resultados de las encuestas

Pregunta 1. ¿Conoce la importancia y la necesidad de proteger la información? Si su respuesta es afirmativa explique por qué?:
Según las respuesta obtenidas con esta pregunta se concluyó que más del 50% de los encuestados dice conocer la importancia y la necesidad de proteger sus datos, pero si se realiza un análisis de sus explicaciones se evidencia una falta de conocimiento del tema ya que pueden tener un vana idea de la pregunta pero sus explicaciones no corresponden con su definición; también se encontró unas explicaciones muy coherentes como: "*La información hace parte del patrimonio de nuestra entidad*"; además es importante analizar que el 44% de los encuestado no conoce dicha importancia, lo que evidencia una falta de concientización del tema.

Pregunta 2. ¿Conoce las políticas de seguridad de la información que deben ponerse en práctica para proteger la información de la Entidad?:
A partir de los resultados obtenidos mediante esta pregunta se evidencio que un gran número (79%) de funcionarios no conoce las políticas de seguridad para ser adoptadas en la Entidad; razón por la cual se amplió el tema con el profesional universitario de la oficina de sistemas (entrevista) y se observó que la entidad no cuenta con una políticas claras y bien definidas que les permitan aplicarlas.

Pregunta 3. ¿Ha perdido alguna vez información importante en su equipo de cómputo?:
Mediante la respuesta obtenida en esta pregunta se puede concluir que aproximadamente la mitad de los funcionarios encuestados (43 %) han perdido información importante de sus equipos de cómputo, este resultado deja en claro que existe la necesidad de crear unas políticas y controles a riesgos tan inminentes como la perdida de información.

Pregunta 4. ¿Según usted por qué sucedió?:
Esta pregunta se respondió teniendo en cuenta la respuesta afirmativa de la anterior pregunta, de la cual se evidencio que la perdida de información fue por fallas Físicas de los equipos de cómputo (37%), seguida en un menor porcentaje por Virus informático (31%) y en otras ocasiones por malos manejos así como también por deficiente servicio técnico prestado por parte del personal encargado.

Pregunta 5. El Almacenamiento en la Nube, es el modelo de servicio en el cual los datos se almacenan, se administran, y se respaldan de forma remota, en servidores que están en internet y que son administrados por un proveedor del servicio). En qué casos considera usted necesario hacer uso de este servicio:

En esta pregunta consideramos necesario dar a conocer un término muy mencionado actualmente (almacenamiento en la nube, con el fin de que los funcionarios nos den a conocer su punto de vista y como ellos perciben la necesidad de aplicar este servicio en la entidad, se pudo decir que más de la mitad de los funcionarios consideran necesario este servicios para *Guardar archivos a modo de copia de seguridad*, esta respuesta puede estar relacionada con los inconvenientes que se han presentado en cuento a la perdida de datos.

Pregunta 6 y 7. ¿Usted hace uso de las redes sociales?

De acuerdo con los resultados obtenidos se observa que más del 50% de los funcionarios hace uso de las redes sociales, el objetivo de esta pregunta es indagar qué tan confiados pueden ser los funcionarios al momento de compartir información y cuidar sus datos. Para lo cual se formula la siguiente parte de la pregunta en la cual se presenta 3 opciones de los posibles comportamientos y de cual se pudo evidenciar que de las personas que usan estos servicios la mayoría son cuidadoso con la información que comparten y tienes bien configurados los niveles de privacidad; aunque también se puede evidenciar que el 42% no hace uso de estos servicios la mayoría por desconocimiento y el temor de exponer sus datos.

Pregunta 7. Conoce algún tipo de estos ataques o vulnerabilidades que se pueden presentar en la actualidad:

Al presentarles unas opciones de ataques o vulnerabilidades que se pueden presentar en la actualidad con respecto a la seguridad de la información; se concluyó lo siguiente, más de mitad de los funcionarios (55%) solo reconoce a los virus informático (Malware, Troyano, etc) como las vulnerabilidad a las que estamos expuestos y es muy poco el conocimiento que tiene con respectos a otra técnicas que son muy comunes en la actualidad.

Anexo F. Documento de la entrevista diligenciado (Hoja 1)

REPUBLICA DE COLOMBIA
GOBERNACIÓN DEL PUTUMAYO
"Marca la diferencia"

Secretaria de Servicios Administrativos

Entrevista dirigida al Profesional Universitario encargado del proceso de Gestión de tecnología e información de la Gobernación de Putumayo.

Objetivo:	Formular un conjunto de preguntas a la Entidad que permitan levantar la información de la infraestructura física, lógica y metodológica de seguridad, como parte del estudio de la situación actual de la administración departamental.
Categoría:	Documento técnico
Autor (es):	Leyda Liliana Córdoba Araujo Wilson Camilo delgado Trujillo Estudiantes Especialización en Seguridad Informática Universidad UNAD
Aprobó:	Secretaria de Servicios administrativos Departamental

- **Información General**

Nombre de la persona encargada: Andres Fernando Trejo Gaviria
Formación Académica: profesional X Especialista ____ Magister ____
Antigüedad Laboral: Menos de 2 años ___ De 2 a 5 años X Mas de 5 años ___
Cargo: Profesional Universitario. - oficina Sistemas

- **Infraestructura física, acceso y medio ambiente.**

a. Centro de Datos.

Existe en la entidad un centro de datos: SI X NO__

b. Control de Acceso.

En la Entidad se utiliza sistemas de control de acceso: SI X NO__

Cuales:
Los equipos (80%) estan suscritos al Dominio, configurado algunas Directivas de control de Acceso, de igual forma para el acceso a los diferente Sistemas de Información de acuerdo a los Roles asignados. en el tema de Accesos Físicos existen los barreras pero no hay suficiente Seguridad.

c. Barreras.

Existen barreras físicas que aíslen las áreas coyunturales de la entidad. SI X NO___

d. Cableado y Canaletas

- Eléctrico:
  Existencia y estado del cableado eléctrico

El sistema electrico esta instalado desde el año 2011. y esta en buen Estado. Puntos certificado, cada subcentro cuenta con una caja de control electrico Independiente

Continuación Anexo F. (Hoja 2)

PUTUMAYO

REPUBLICA DE COLOMBIA
GOBERNACIÓN DEL PUTUMAYO
"Marca la diferencia"

Secretaria de Servicios Administrativos

Putumayo
Solidario y Competitivo

- Datos.
  Existencia y estado del cableado de datos.

La Red de Datos con cableado estructurado Cat. 6., aprox 210 Puntos certificados, se dispone de 3 subcentros ubicados en áreas estrategicas. (Incluyendo Centro Datos)

f. Seguridad.

¿Existe un Firewall en la entidad? : SI X NO___
¿Se entiende para qué debe existir? La Entidad tiene un firewall Fisico que nos Permite gestionar y controlar la totalidad de trafico entrante y saliente de la Red.

g. Switches.

Cuál es el tipo de red de área local que existe en la entidad: Topologia Estrella.
Descripción de cómo está construida la red de área local en cuanto a equipos activos:
→En el centro de Datos se Dispone de 2 switches de 48 Puertos, una controladora de Red, un rack de Piso, el Router del Proveedor de Internet (Movistar), 1 transceiver, 5 access Point para la Zona wifi.

Tambien se dispone de 1 central telefonica Hibrida Conectada a 1 linea E1.

h. Equipos en el Piso

¿En la entidad hay equipos en el piso? SI X NO___

i. Aire Acondicionado.

¿La entidad utiliza aire acondiciona en el centro de Datos? SI X NO___

Descripción 18000 btu 220v.

j. Reguladores y UPS.

¿La entidad cuenta con reguladores y UPS? SI X NO___

Descripción 3. UPS de 6KVA.

Continuación Anexo F. (Hoja 3)

REPUBLICA DE COLOMBIA
GOBERNACIÓN DEL PUTUMAYO
"Marca la diferencia"

Secretaria de Servicios Administrativos

k. Planta de Emergencia.

¿La entidad cuenta con una planta de generación de emergencia? SI X NO___
Descripción A presentado algunas fallas.

- **Lógico**

l. Actualización de Servidores.

¿Se actualizan y parchan con regularidad los servidores? SI X NO___

Periocidad: Cuando se generan las alertas.

¿Cuál de los métodos siguientes utilizan?
- ☐ YUM
- ☐ WSUS
- ☒ Manual

m. Pruebas de Intrusión.

Se han aplicado Pruebas de intrusión en la entidad, cuales se han hecho o se hacen con regularidad en la Entidad?.
- ☐ Hacking Ético
- ☐ Ingeniería Social
- ☒ Ninguna

- **Metodológico.**

Cuál de los siguientes puntos metodológicos existe y se utilizan en la entidad.

a) Políticas. ¿Hay un manual como tal? SI___ NO X

b) Procedimientos. ¿Para qué labores?
La entidad esta en Proceso de Certificacion de SIG. NTCGP 1000-2009 para lacual la entidad atraves del Proceso de GESTION DE TECNOLOGIA e Informacion maneja 8 Procedimientos

c) Normas. ¿Cuáles?
Decreto 2573 del 2014.
Ley 1712 del 2014
NTCP GP 1000-2009
Decreto 943 del 2014

Continuación Anexo F. (Hoja 4)

d) Estándares. ¿Aplicados a qué?

NTCGP 1000-2009. (en Proceso)

e) Concientización.

¿Hacen regularmente procesos de concienciación en lo referente a seguridad de la información? SI___ NO_X_

¿Se hace inducción a los empleados nuevos? SI___ NO_X_

f) Acuerdos de Confidencialidad.

¿Los hay como tal o están embebidos en el contrato laboral? SI_X_ NO___

g) Renuncia de Propiedad de Información.

¿Se ha firmado aparte o existe dentro del contrato laboral? SI___ NO_X_

h) Código de Buena Conducta.

¿Existe? SI_X_ NO___

Entrevistado: _____

Anexo G. Resultados entrevista

De acuerdo a la entrevista realizada al Profesional Universitario encargado del Área de Sistemas, se indago y se obtuvo información importante a cerca de la Infraestructura física, tecnológica, de acceso y algunos temas relacionados con el medio ambiente del centro de datos y los sistemas de información de la Entidad.

Según datos suministrados la entidad tiene un centro de datos, ubicado alado de la oficina de Sistemas; cuenta con un rack de piso con tres (3) servidores físicos, un servidor web y dos más en los cuales se encuentran virtualizados servicios como: servidor de dominio, de Bases de datos, de archivos y el servidor del Sistema de Georeferenciación – SIG. Para el acceso al centro de datos se realiza a través de la oficina de sistemas que comparte una puerta; el 80% de los equipos de cómputo con los que cuenta la entidad están ligados al servidor de dominio el cual controla su acceso a través de la contraseña y la aplicación de algunas directivas configuradas (bloqueo de Puerto USB, restricciones para la instalación de aplicaciones, etc).

La entidad posee una red de datos instalada aproximadamente desde el año 2011, con un sistema de cableado estructurado categoría 6 con aproximadamente 210 puntos de red datos y electricidad, los cuales están distribuidos por2 sub-centros ubicados en lugares estratégicos de la entidad, cada uno de los cuales tiene un Switch administrable de 48 puestos y el respaldo eléctrico con una UPS de 6 KVA.

En el centro de datos cuentan con dos Switches administrables de 48 puertos, un Firewall físico, y una central telefónica Hibrida IP Análoga/Digital ya que la entidad cuenta con telefonía voz/IP, par el tema de ventilación el cuarto está equipado con un aire acondicionado de pared de 18000 btu220v. Existe una planta de respaldo eléctrico pero en ocasiones mencionan que ha presentado fallas.

Los equipos de cómputo cuentan con la licencia de kaspersky end point security que se ha venido renovándose desde el año 2010, las actualizaciones de los servidores se realizan de forma manual y en la mayoría de veces ha sido necesaria la contratación de servicios de los expertos en tema.

Con respecto a la pregunta si se han aplicado alguna vez Pruebas de Intrusión, la respuesta es negativa, también se indaga sobre la existencia de un manual de las políticas de seguridad de la información, para lo cual el profesional del área

menciona que existen algunas políticas que se han establecido a través de circulares internas, oficios o practicas internas pero no existe en sí, un documento que consolide y tenga a disposición todas las políticas para el control de los riesgos que se puedan presentar.

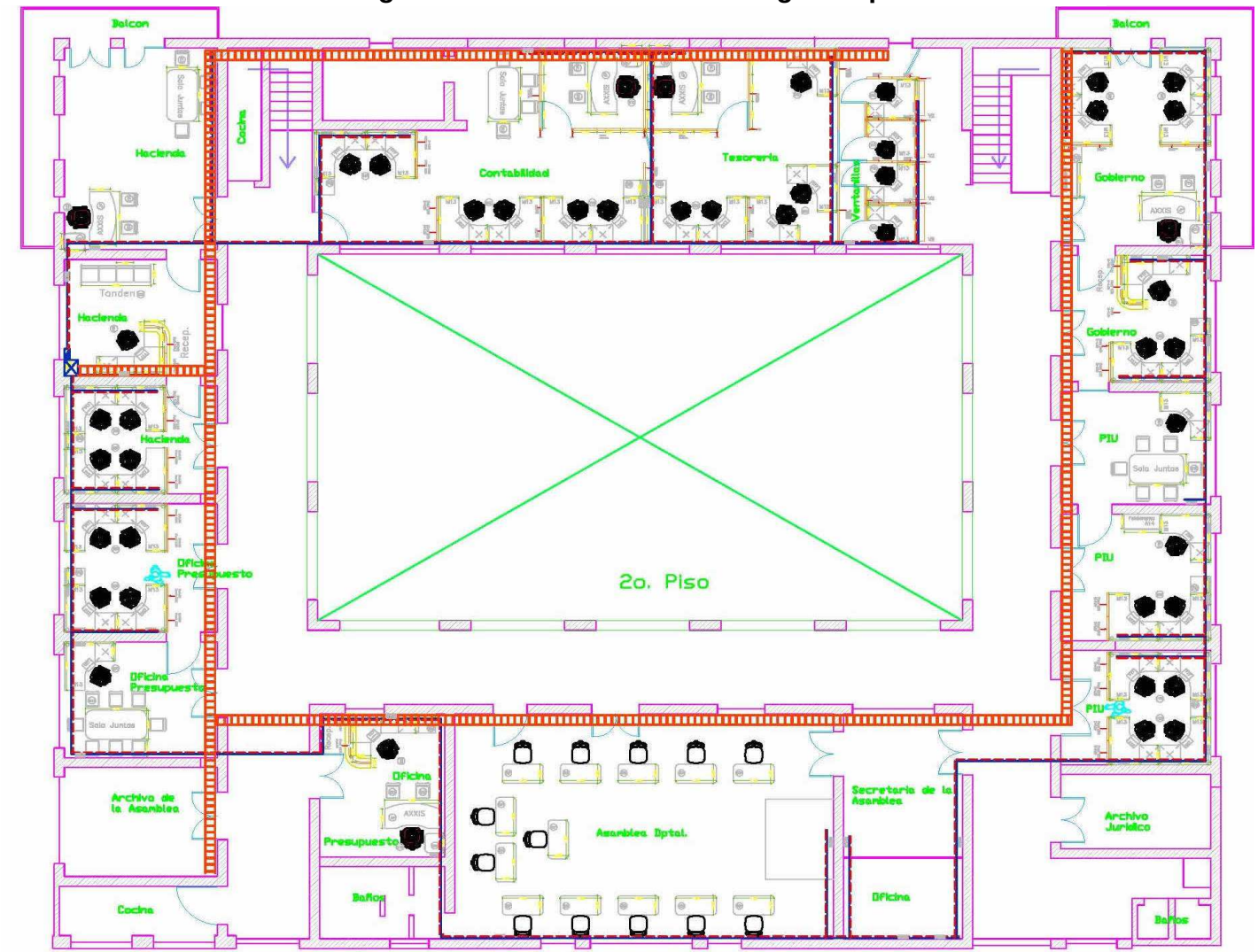
También menciona que la entidad está en un proceso de certificación del sistema integrado de gestión NTCGP 1000:2009—MECI 2014, para lo cual se han levantado unos procedimientos y un proceso que está a cargo de la oficina de sistemas llamado: Proceso de Gestión de Tecnología e Información; así como también un mapa de riesgos generalizado para toda la entidad donde se han incluido algunos riesgos del área pero de manera generalizada. De acuerdo a la pregunta si se ha realizado en la entidad procesos de concienciación en lo referente a seguridad de la información, la respuesta es negativa, así como tampoco se firman Acuerdos de Confidencialidad solo las cláusulas que están inmersas en están embebidos en los contrato laborales del personal vinculados con contrato de prestación de servicios.

Anexo H. Planos de la Red de datos (1°y 2 do piso parte central de la Gobernación de Putumayo.

Figura 28. Plano red de datos primer piso.

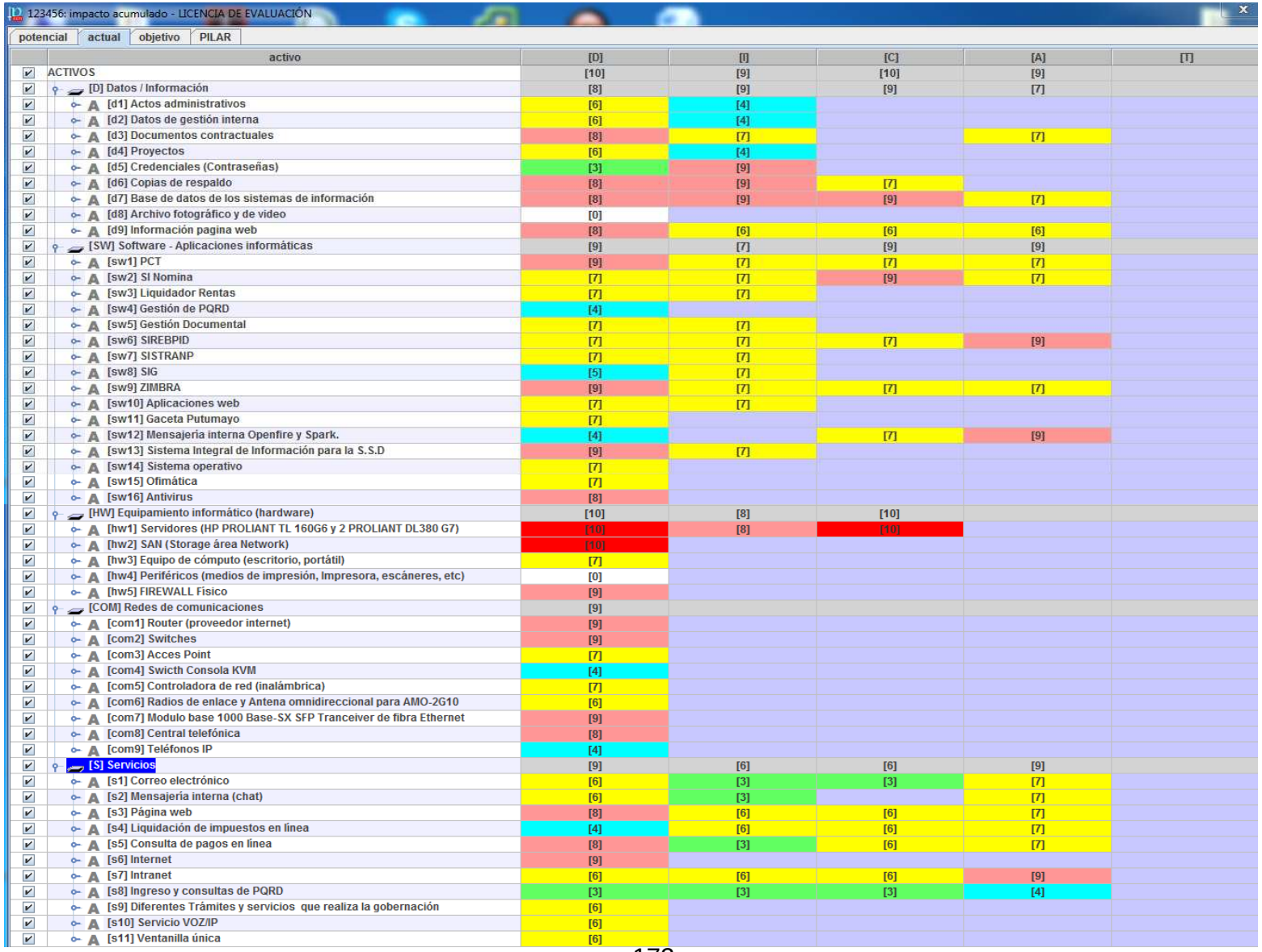
Fuente: Documentación Entidad

Figura 29. Plano red de datos segundo piso.



Fuente: Documentación Entidad

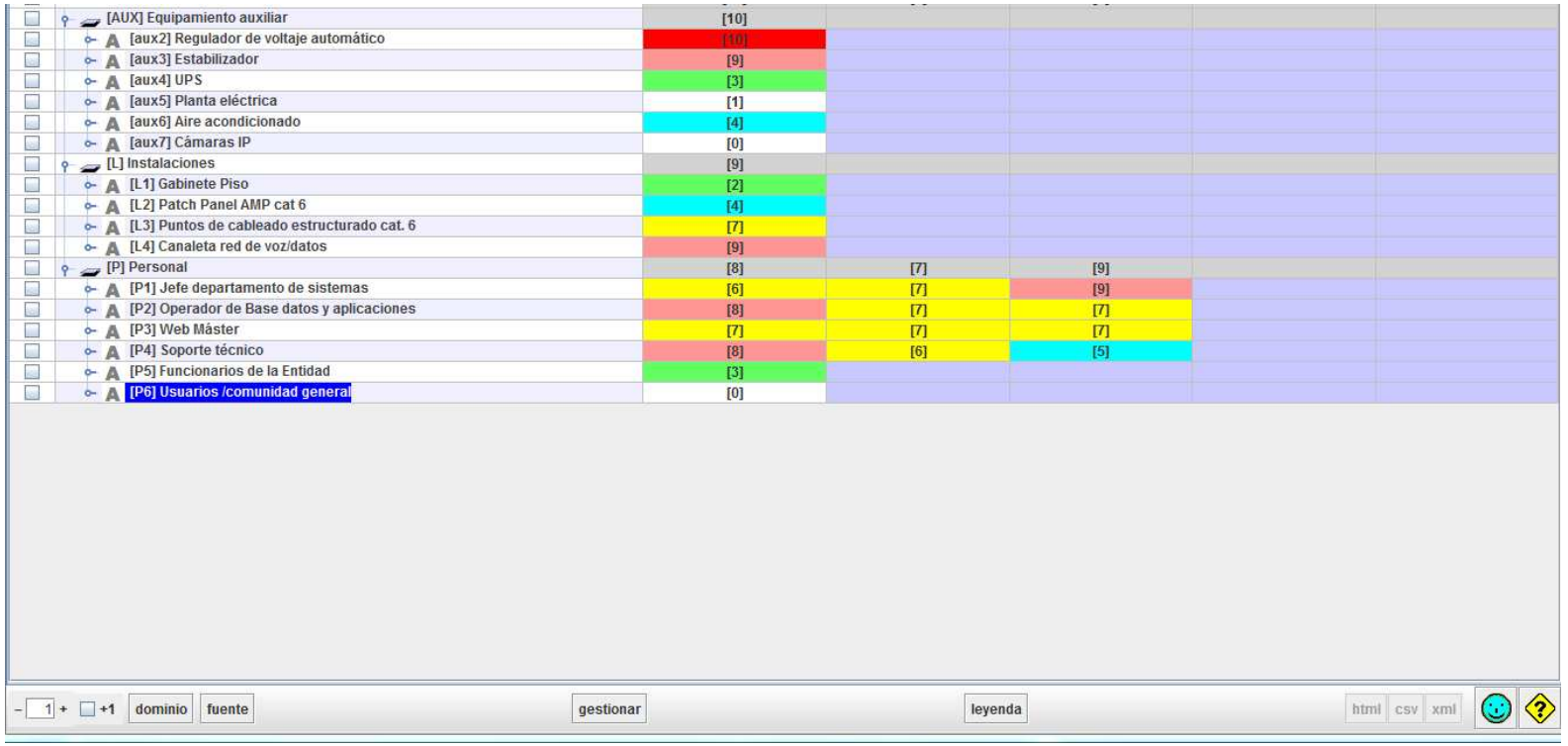
Anexo I. Impacto acumulado herramienta PILAR.



123456: impacto acumulado - LICENCIA DE EVALUACIÓN

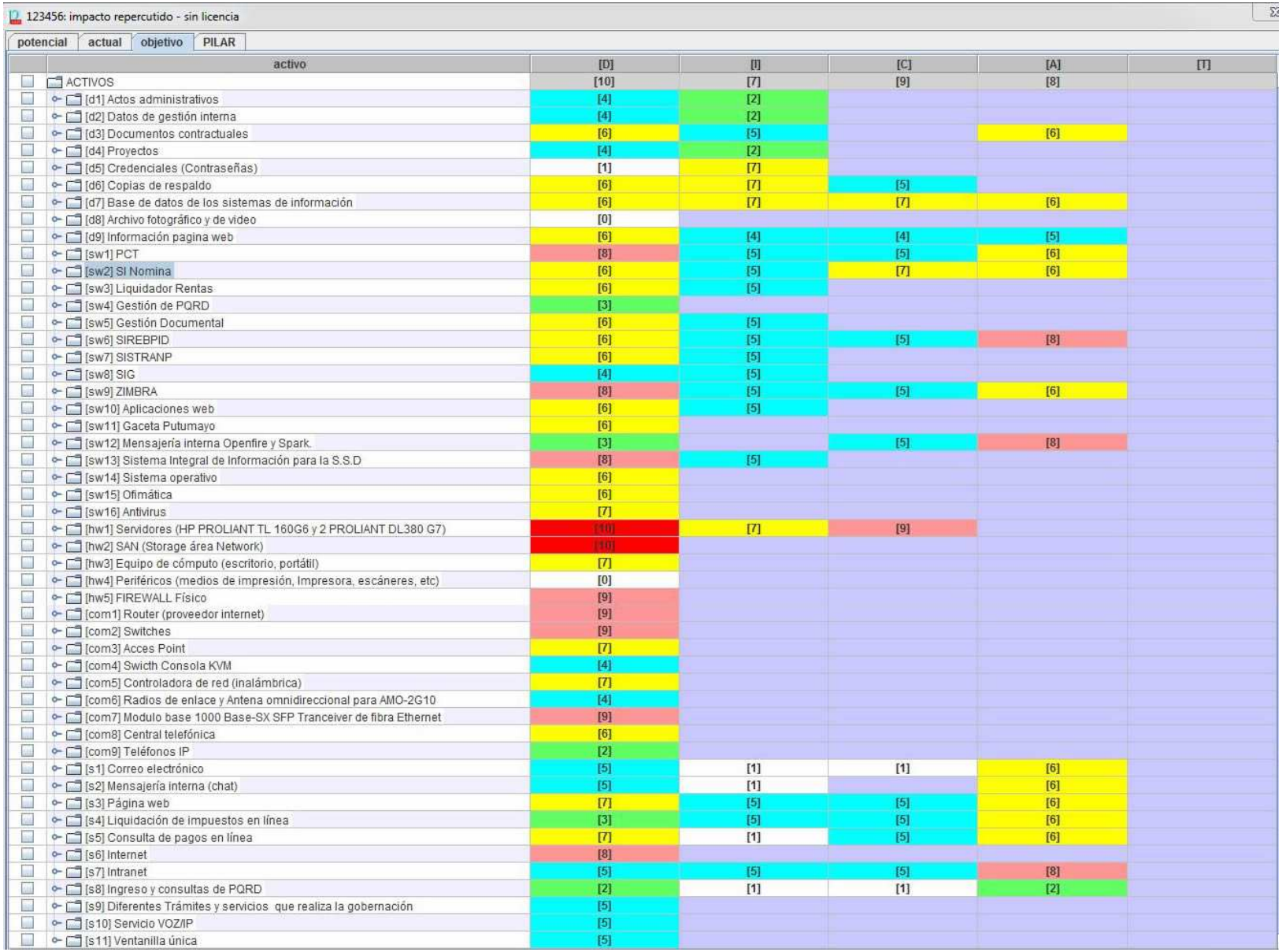
potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[10]	[9]	[10]	[9]	
[D] Datos / Información	[8]	[9]	[9]	[7]	
[d1] Actos administrativos	[6]	[4]			
[d2] Datos de gestión interna	[6]	[4]			
[d3] Documentos contractuales	[8]	[7]		[7]	
[d4] Proyectos	[6]	[4]			
[d5] Credenciales (Contraseñas)	[3]	[9]			
[d6] Copias de respaldo	[8]	[9]	[7]		
[d7] Base de datos de los sistemas de información	[8]	[9]	[9]	[7]	
[d8] Archivo fotográfico y de video	[0]				
[d9] Información pagina web	[8]	[6]	[6]	[6]	
[SW] Software - Aplicaciones informáticas	[9]	[7]	[9]	[9]	
[sw1] PCT	[9]	[7]	[7]	[7]	
[sw2] SI Nomina	[7]	[7]	[9]	[7]	
[sw3] Liquidador Rentas	[7]	[7]			
[sw4] Gestión de PQRD	[4]				
[sw5] Gestión Documental	[7]	[7]			
[sw6] SIREBPID	[7]	[7]	[7]	[9]	
[sw7] SISTRANP	[7]	[7]			
[sw8] SIG	[5]	[7]			
[sw9] ZIMBRA	[9]	[7]	[7]	[7]	
[sw10] Aplicaciones web	[7]	[7]			
[sw11] Gaceta Putumayo	[7]				
[sw12] Mensajeria interna Openfire y Spark.	[4]		[7]	[9]	
[sw13] Sistema Integral de Información para la S.S.D	[9]	[7]			
[sw14] Sistema operativo	[7]				
[sw15] Ofimática	[7]				
[sw16] Antivirus	[8]				
[HW] Equipamiento informático (hardware)	[10]	[8]	[10]		
[hw1] Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	[10]	[8]	[10]		
[hw2] SAN (Storage área Network)	[10]				
[hw3] Equipo de cómputo (escritorio, portátil)	[7]				
[hw4] Periféricos (medios de impresión, Impresora, escáneres, etc)	[0]				
[hw5] FIREWALL Fisico	[9]				
[COM] Redes de comunicaciones	[9]				
[com1] Router (proveedor internet)	[9]				
[com2] Switches	[9]				
[com3] Acces Point	[7]				
[com4] Swicth Consola KVM	[4]				
[com5] Controladora de red (inalámbrica)	[7]				
[com6] Radios de enlace y Antena omnidireccional para AMO-2G10	[6]				
[com7] Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	[9]				
[com8] Central telefónica	[8]				
[com9] Teléfonos IP	[4]				
[S] Servicios	[9]	[6]	[6]	[9]	
[s1] Correo electrónico	[6]	[3]	[3]	[7]	
[s2] Mensajería interna (chat)	[6]	[3]		[7]	
[s3] Página web	[8]	[6]	[6]	[7]	
[s4] Liquidación de impuestos en línea	[4]	[6]	[6]	[7]	
[s5] Consulta de pagos en línea	[8]	[3]	[6]	[7]	
[s6] Internet	[9]				
[s7] Intranet	[6]	[6]	[6]	[9]	
[s8] Ingreso y consultas de PQRD	[3]	[3]	[3]	[4]	
[s9] Diferentes Trámites y servicios que realiza la gobernación	[6]				
[s10] Servicio VOZ/IP	[6]				
[s11] Ventanilla única	[6]				



Fuente. Proyecto Herramienta Pilar

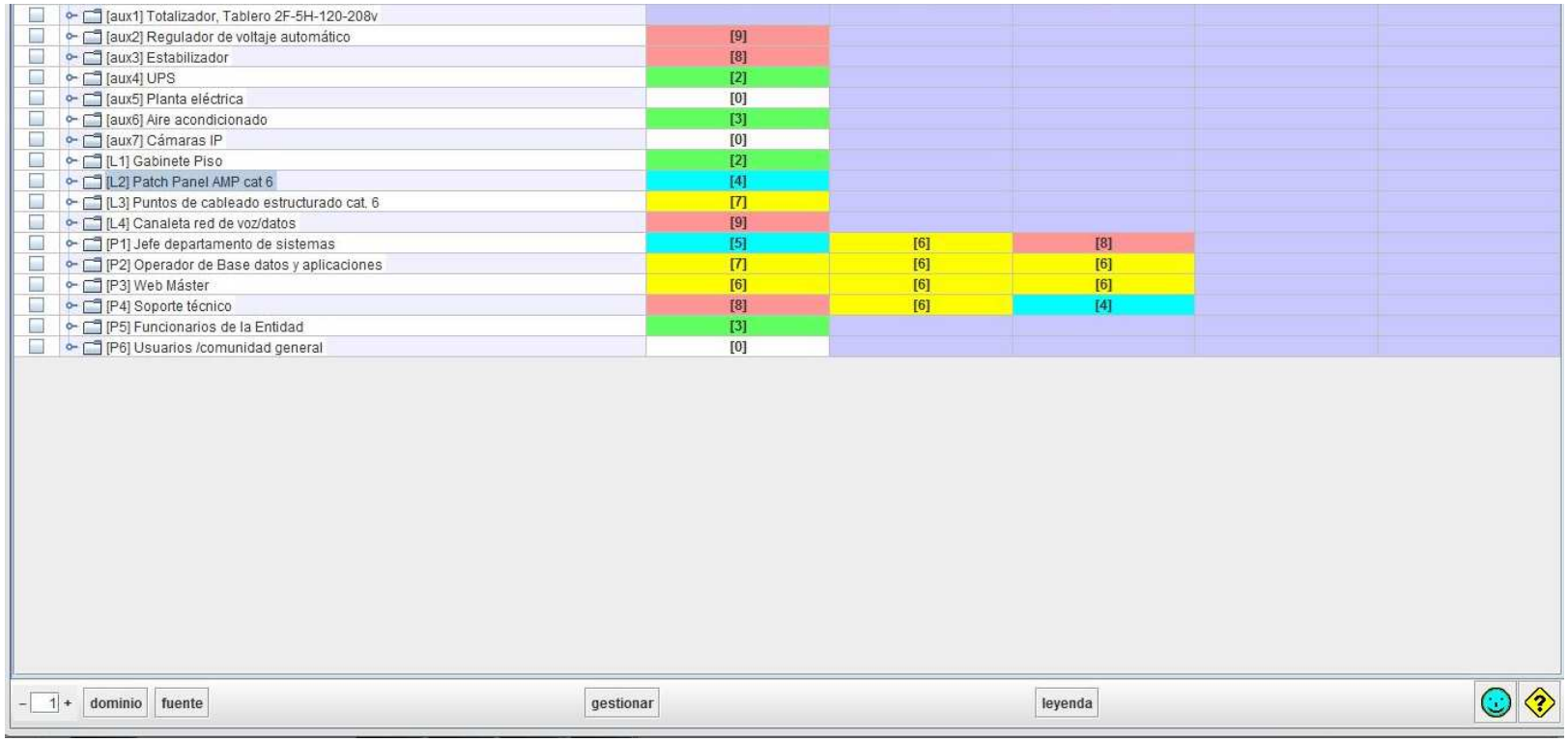
Anexo J. Impacto residual herramienta PILAR.



123456: impacto repercutido - sin licencia

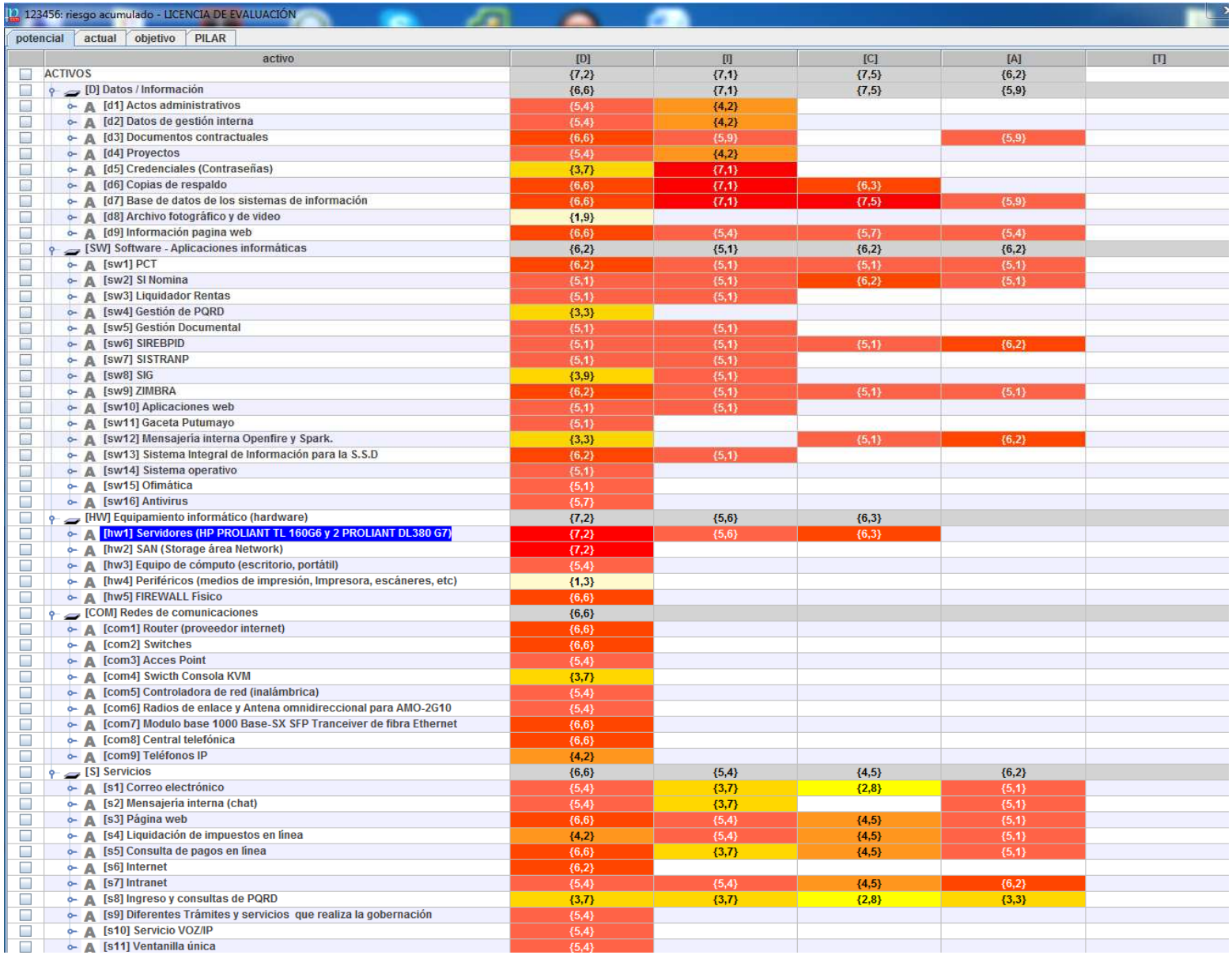
potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[10]	[7]	[9]	[8]	
[d1] Actos administrativos	[4]	[2]			
[d2] Datos de gestión interna	[4]	[2]			
[d3] Documentos contractuales	[6]	[5]		[6]	
[d4] Proyectos	[4]	[2]			
[d5] Credenciales (Contraseñas)	[1]	[7]			
[d6] Copias de respaldo	[6]	[7]	[5]		
[d7] Base de datos de los sistemas de información	[6]	[7]	[7]	[6]	
[d8] Archivo fotográfico y de video	[0]				
[d9] Información pagina web	[6]	[4]	[4]	[5]	
[sw1] PCT	[8]	[5]	[5]	[6]	
[sw2] SI Nomina	[6]	[5]	[7]	[6]	
[sw3] Liquidador Rentas	[6]	[5]			
[sw4] Gestión de PQRD	[3]				
[sw5] Gestión Documental	[6]	[5]			
[sw6] SIREBPID	[6]	[5]	[5]	[8]	
[sw7] SISTRANP	[6]	[5]			
[sw8] SIG	[4]	[5]			
[sw9] ZIMBRA	[8]	[5]	[5]	[6]	
[sw10] Aplicaciones web	[6]	[5]			
[sw11] Gaceta Putumayo	[6]				
[sw12] Mensajería interna Openfire y Spark.	[3]		[5]	[8]	
[sw13] Sistema Integral de Información para la S.S.D	[8]	[5]			
[sw14] Sistema operativo	[6]				
[sw15] Ofimática	[6]				
[sw16] Antivirus	[7]				
[hw1] Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	[10]	[7]	[9]		
[hw2] SAN (Storage área Network)	[10]				
[hw3] Equipo de cómputo (escritorio, portátil)	[7]				
[hw4] Periféricos (medios de impresión, Impresora, escáneres, etc)	[0]				
[hw5] FIREWALL Físico	[9]				
[com1] Router (proveedor internet)	[9]				
[com2] Switches	[9]				
[com3] Acces Point	[7]				
[com4] Swicth Consola KVM	[4]				
[com5] Controladora de red (inalámbrica)	[7]				
[com6] Radios de enlace y Antena omnidireccional para AMO-2G10	[4]				
[com7] Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	[9]				
[com8] Central telefónica	[6]				
[com9] Teléfonos IP	[2]				
[s1] Correo electrónico	[5]	[1]	[1]	[6]	
[s2] Mensajería interna (chat)	[5]	[1]		[6]	
[s3] Página web	[7]	[5]	[5]	[6]	
[s4] Liquidación de impuestos en línea	[3]	[5]	[5]	[6]	
[s5] Consulta de pagos en línea	[7]	[1]	[5]	[6]	
[s6] Internet	[8]				
[s7] Intranet	[5]	[5]	[5]	[8]	
[s8] Ingreso y consultas de PQRD	[2]	[1]	[1]	[2]	
[s9] Diferentes Trámites y servicios que realiza la gobernación	[5]				
[s10] Servicio VOZ/IP	[5]				
[s11] Ventanilla única	[5]				



Fuente. Proyecto Herramienta Pilar

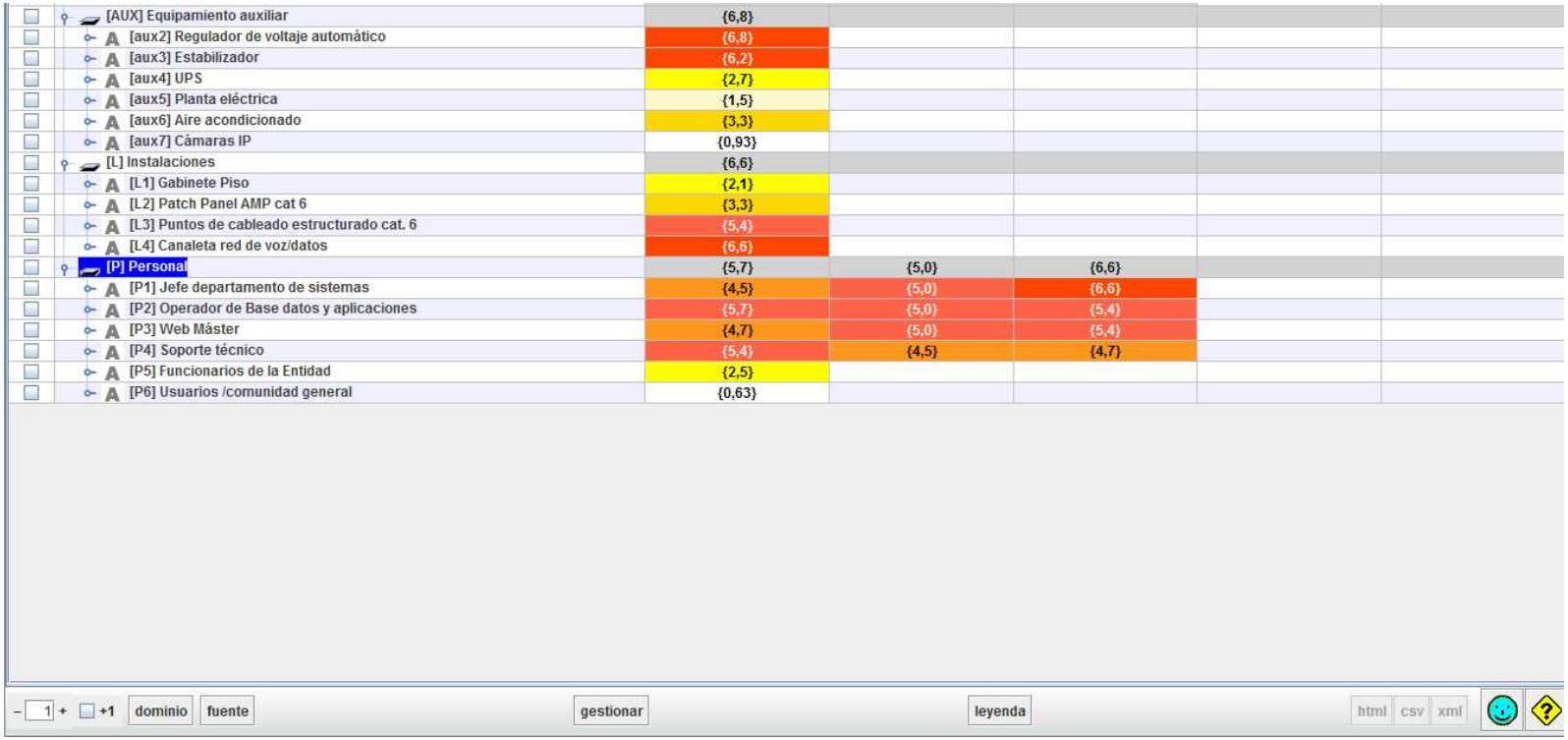
Anexo K. Riesgo acumulado herramienta PILAR.



123456: riesgo acumulado - LICENCIA DE EVALUACIÓN

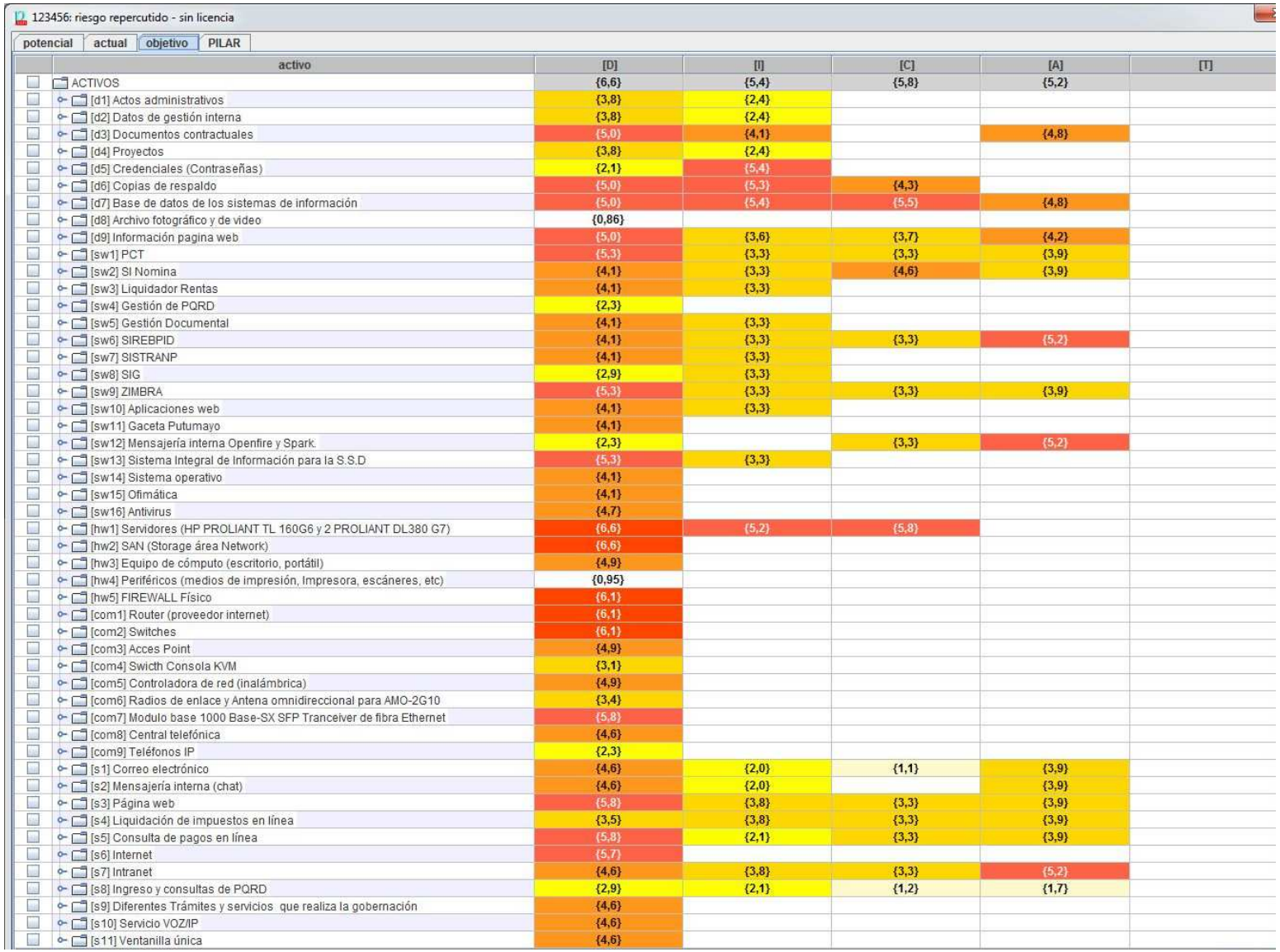
potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{7,2}	{7,1}	{7,5}	{6,2}	
[D] Datos / Información	{6,6}	{7,1}	{7,5}	{5,9}	
[d1] Actos administrativos	{5,4}	{4,2}			
[d2] Datos de gestión interna	{5,4}	{4,2}			
[d3] Documentos contractuales	{6,6}	{5,9}		{5,9}	
[d4] Proyectos	{5,4}	{4,2}			
[d5] Credenciales (Contraseñas)	{3,7}	{7,1}			
[d6] Copias de respaldo	{6,6}	{7,1}	{6,3}		
[d7] Base de datos de los sistemas de información	{6,6}	{7,1}	{7,5}	{5,9}	
[d8] Archivo fotográfico y de video	{1,9}				
[d9] Información pagina web	{6,6}	{5,4}	{5,7}	{5,4}	
[SW] Software - Aplicaciones informáticas	{6,2}	{5,1}	{6,2}	{6,2}	
[sw1] PCT	{6,2}	{5,1}	{5,1}	{5,1}	
[sw2] SI Nomina	{5,1}	{5,1}	{6,2}	{5,1}	
[sw3] Liquidador Rentas	{5,1}	{5,1}			
[sw4] Gestión de PQRD	{3,3}				
[sw5] Gestión Documental	{5,1}	{5,1}			
[sw6] SIREBPID	{5,1}	{5,1}	{5,1}	{6,2}	
[sw7] SISTRANP	{5,1}	{5,1}			
[sw8] SIG	{3,9}	{5,1}			
[sw9] ZIMBRA	{6,2}	{5,1}	{5,1}	{5,1}	
[sw10] Aplicaciones web	{5,1}	{5,1}			
[sw11] Gaceta Putumayo	{5,1}				
[sw12] Mensajería interna Openfire y Spark.	{3,3}		{5,1}	{6,2}	
[sw13] Sistema Integral de Información para la S.S.D	{6,2}	{5,1}			
[sw14] Sistema operativo	{5,1}				
[sw15] Ofimática	{5,1}				
[sw16] Antivirus	{5,7}				
[HW] Equipamiento informático (hardware)	{7,2}	{5,6}	{6,3}		
[hw1] Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	{7,2}	{5,6}	{6,3}		
[hw2] SAN (Storage área Network)	{7,2}				
[hw3] Equipo de cómputo (escritorio, portátil)	{5,4}				
[hw4] Periféricos (medios de impresión, Impresora, escáneres, etc)	{1,3}				
[hw5] FIREWALL Físico	{6,6}				
[COM] Redes de comunicaciones	{6,6}				
[com1] Router (proveedor internet)	{6,6}				
[com2] Switches	{6,6}				
[com3] Acces Point	{5,4}				
[com4] Swicth Consola KVM	{3,7}				
[com5] Controladora de red (inalámbrica)	{5,4}				
[com6] Radios de enlace y Antena omnidireccional para AMO-2G10	{5,4}				
[com7] Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	{6,6}				
[com8] Central telefónica	{6,6}				
[com9] Teléfonos IP	{4,2}				
[S] Servicios	{6,6}	{5,4}	{4,5}	{6,2}	
[s1] Correo electrónico	{5,4}	{3,7}	{2,8}	{5,1}	
[s2] Mensajería interna (chat)	{5,4}	{3,7}		{5,1}	
[s3] Página web	{6,6}	{5,4}	{4,5}	{5,1}	
[s4] Liquidación de impuestos en línea	{4,2}	{5,4}	{4,5}	{5,1}	
[s5] Consulta de pagos en línea	{6,6}	{3,7}	{4,5}	{5,1}	
[s6] Internet	{6,2}				
[s7] Intranet	{5,4}	{5,4}	{4,5}	{6,2}	
[s8] Ingreso y consultas de PQRD	{3,7}	{3,7}	{2,8}	{3,3}	
[s9] Diferentes Trámites y servicios que realiza la gobernación	{5,4}				
[s10] Servicio VOZ/IP	{5,4}				
[s11] Ventanilla única	{5,4}				



Fuente. Proyecto Herramienta Pilar

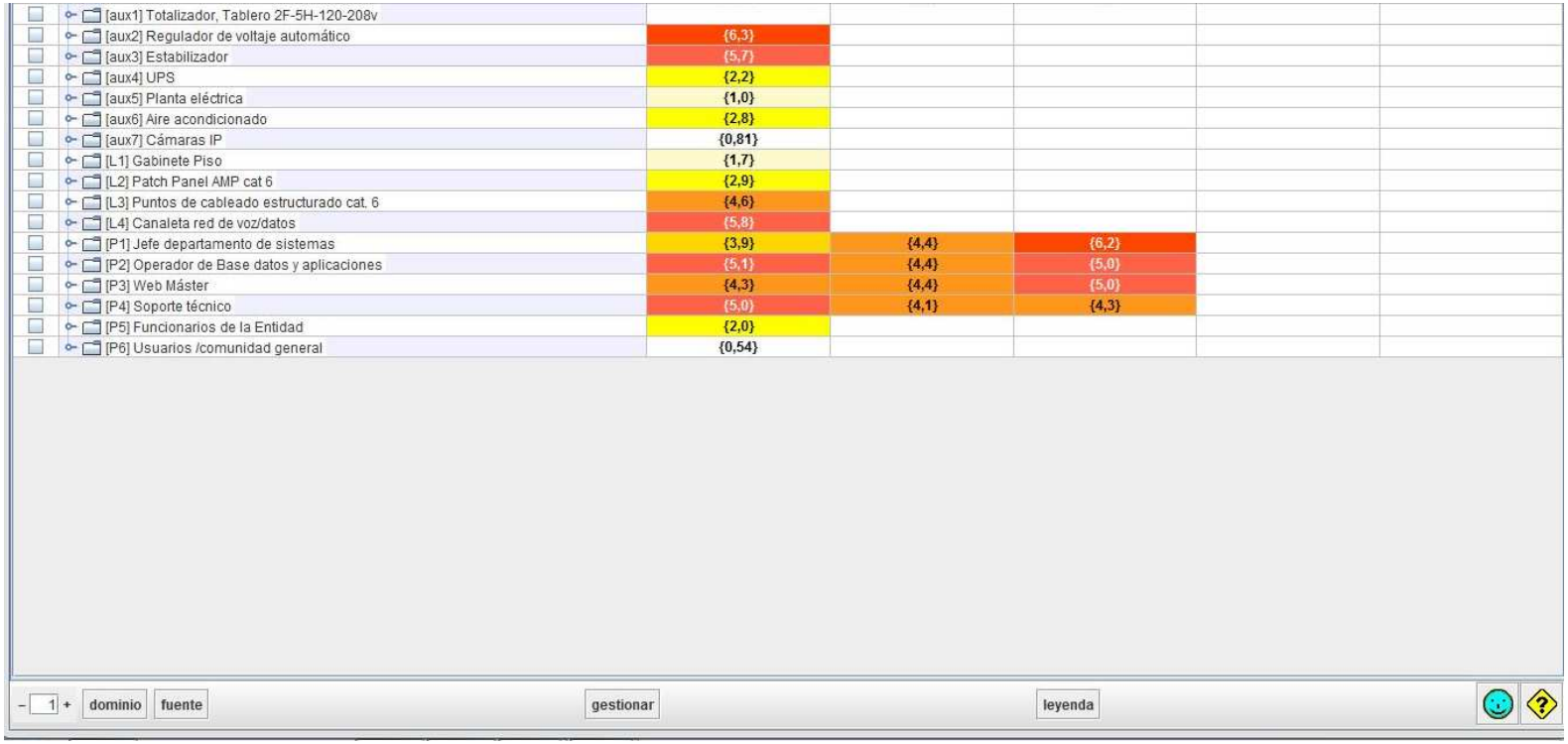
Anexo L. Riesgo residual herramienta PILAR.



123456: riesgo repercutido - sin licencia

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{6,6}	{5,4}	{5,8}	{5,2}	
[d1] Actos administrativos	{3,8}	{2,4}			
[d2] Datos de gestión interna	{3,8}	{2,4}			
[d3] Documentos contractuales	{5,0}	{4,1}		{4,8}	
[d4] Proyectos	{3,8}	{2,4}			
[d5] Credenciales (Contraseñas)	{2,1}	{5,4}			
[d6] Copias de respaldo	{5,0}	{5,3}	{4,3}		
[d7] Base de datos de los sistemas de información	{5,0}	{5,4}	{5,5}	{4,8}	
[d8] Archivo fotográfico y de video	{0,86}				
[d9] Información pagina web	{5,0}	{3,6}	{3,7}	{4,2}	
[sw1] PCT	{5,3}	{3,3}	{3,3}	{3,9}	
[sw2] SI Nomina	{4,1}	{3,3}	{4,6}	{3,9}	
[sw3] Liquidador Rentas	{4,1}	{3,3}			
[sw4] Gestión de PQRD	{2,3}				
[sw5] Gestión Documental	{4,1}	{3,3}			
[sw6] SIREBPID	{4,1}	{3,3}	{3,3}	{5,2}	
[sw7] SISTRANP	{4,1}	{3,3}			
[sw8] SIG	{2,9}	{3,3}			
[sw9] ZIMBRA	{5,3}	{3,3}	{3,3}	{3,9}	
[sw10] Aplicaciones web	{4,1}	{3,3}			
[sw11] Gaceta Putumayo	{4,1}				
[sw12] Mensajería interna Openfire y Spark	{2,3}		{3,3}	{5,2}	
[sw13] Sistema Integral de Información para la S.S.D	{5,3}	{3,3}			
[sw14] Sistema operativo	{4,1}				
[sw15] Ofimática	{4,1}				
[sw16] Antivirus	{4,7}				
[hw1] Servidores (HP PROLIANT TL 160G6 y 2 PROLIANT DL380 G7)	{6,6}	{5,2}	{5,8}		
[hw2] SAN (Storage área Network)	{6,6}				
[hw3] Equipo de cómputo (escritorio, portátil)	{4,9}				
[hw4] Periféricos (medios de impresión, Impresora, escáneres, etc)	{0,95}				
[hw5] FIREWALL Físico	{6,1}				
[com1] Router (proveedor internet)	{6,1}				
[com2] Switches	{6,1}				
[com3] Acces Point	{4,9}				
[com4] Swicth Consola KVM	{3,1}				
[com5] Controladora de red (inalámbrica)	{4,9}				
[com6] Radios de enlace y Antena omnidireccional para AMO-2G10	{3,4}				
[com7] Modulo base 1000 Base-SX SFP Tranceiver de fibra Ethernet	{5,8}				
[com8] Central telefónica	{4,6}				
[com9] Teléfonos IP	{2,3}				
[s1] Correo electrónico	{4,6}	{2,0}	{1,1}	{3,9}	
[s2] Mensajería interna (chat)	{4,6}	{2,0}		{3,9}	
[s3] Página web	{5,8}	{3,8}	{3,3}	{3,9}	
[s4] Liquidación de impuestos en línea	{3,5}	{3,8}	{3,3}	{3,9}	
[s5] Consulta de pagos en línea	{5,8}	{2,1}	{3,3}	{3,9}	
[s6] Internet	{5,7}				
[s7] Intranet	{4,6}	{3,8}	{3,3}	{5,2}	
[s8] Ingreso y consultas de PQRD	{2,9}	{2,1}	{1,2}	{1,7}	
[s9] Diferentes Trámites y servicios que realiza la gobernación	{4,6}				
[s10] Servicio VOZ/IP	{4,6}				
[s11] Ventanilla única	{4,6}				



Fuente. Proyecto Herramienta Pilar