PROPUESTA PARA EL MANEJO DE LA SEGURIDAD INFORMATÍCA EN LA ALCALDÍA DE POPAYÁN UTILIZANDO COMO BASE LA NORMA ISO 27002:2013

FABIÁN MAURICIO OCHOA BONILLA

CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA
FACULTAD DE INGENIERÍAS
PROGRAMA INGENIERÍA DE SISTEMAS INFORMÁTICOS
GESTIÓN ORGANIZACIONAL
POPAYÁN, ABRIL 7 DE 2017

PROPUESTA PARA EL MANEJO DE LA SEGURIDAD INFORMATÍCA EN LA ALCALDÍA DE POPAYÁN UTILIZANDO COMO BASE LA NORMA ISO 27002:2013

FABIÁN MAURICIO OCHOA BONILLA

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS INFORMÁTICOS

DIRECTOR

Dra (c) ELIZABETH GRANADOS PEMBERTY

CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA
FACULTAD DE INGENIERÍAS
PROGRAMA INGENIERÍA DE SISTEMAS
GESTIÓN ORGANIZACIONAL
POPAYÁN, ABRIL 7 DE 2017

NOTA DE ACEPTACIÓN

El trabajo de grado modalidad pasantía, denominado **PROPUESTA PARA EL MANEJO DE LA SEGURIDAD INFORMATÍCA EN LA ALCALDÍA DE POPAYÁN UTILIZANDO COMO BASE LA NORMA ISO 27002:2013** EN POPAYÁN – CAUCA, elaborado por FABIAN MAURICIO OCHOA BONILLA, identificado con cédula de ciudadanía número 1.061.750.843 de Popayán Cauca y cumpliendo con los requisitos establecidos en la RESOLUCIÓN Nº 0047 del 9 de Abril de 2012 de la CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA, cumple con los requisitos para optar por el título de Ingeniero de Sistemas Informáticos. Aceptan y firman para los fines pertinentes.

_____
Directora trabajo de grado

_____
Jurado Nº1

_____
Jurado Nº2

Popayán, Julio 27 de 2017

DEDICATORIA

Inicialmente quiero dedicarle este proyecto a Dios, por ser siempre la guía de mi camino y por darme la inteligencia, sabiduría, paciencia, entendimiento y capacidad de ejercer este proyecto.

Dedicar a mis padres, Mamá (Amparo Bonilla Suarez), Papa (Lorenzo Ochoa Lemus) y familiares que siempre creyeron en mi capacidad, que me apoyaron y brindaron confianza y comprensión para culminar este trabajo. Me siento afortunado de tenerlos conmigo, son el tesoro más valioso, al igual que los valores y enseñanzas que me han inculcado.

También quiero dedicarle este proyecto de grado, a todas las personas que creyeron en mí y que me dieron su apoyo constante, durante todo este proceso.

Por último Ingeniera Elizabeth Granados Pemberty, Dios le pague por su dedicación y esfuerzo, supo cómo guiarme en tan arduo trabajo, deseo expresar mi gratitud hacia usted deseándole éxitos y el mayor de los augurios en su trayectoria profesional.

“Nunca pongas en duda si una meta es o no posible
Solo preocúpate de adquirir los conocimientos necesarios y desarrollar las
Habilidades precisas para conseguirlas.”
Anonimo.

AGRADECIMIENTOS

Agradezco primero a Dios quién es el que ha puesto constantemente bendiciones en mi vida y es el que me está acompañando y guiando en mi camino, ya que sin él, nada de lo que hay en mi vida existiría.

Agradezco a mis padres, por el amor, el apoyo, la colaboración y la paciencia que han tenido conmigo a lo largo de este proceso de formación y desarrollo académico.

Agradezco a mi Directora de trabajo de grado, la Ingeniera Elizabeth Granados Pemberty por acompañarme, guiarme, aconsejarme, apoyarme y colaborarme en esta parte de mi vida, que es tan importante para mí.

Agradezco también a todos mis compañeros, amigos y personas que de alguna manera u otra, me han colaborado para llegar hasta esta etapa de mi vida y para culminar este proyecto.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

Página

ÍNDICE DE FIGURAS

Página

ÍNDICE DE ILUSTRACIONES

CAPÍTULO 1. INTRODUCCIÓN

CAPÍTULO 1. PROBLEMA

1.1 RESUMEN

En la pasantía realizada en la Oficina de Sistemas de la Alcaldía de Popayán, se desarrolló una propuesta para el control de acceso a los sistemas de información utilizando como base la norma ISO/IEC 27002:2013 [1].

Hoy, la Alcaldía de Popayán no cuenta con una política de control de acceso definida para sus sistemas de información, por consiguiente, se propone la definición de los cuatro objetivos del dominio de control de acceso para sus sistemas, los cuales se basan en: garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios; hacer que los usuarios sean responsables de la protección de la información para su identificación; impedir el acceso no autorizado a la información compilada por los sistemas y aplicaciones y, hacer que los usuarios sean responsables de la protección de la información para su identificación [1] [2].

Para ello, es necesario que la Oficina de defina una política de acceso incluyendo los catorce controles del dominio de control de acceso, a través de estrategias para impedir el acceso no autorizado a los sistemas de información y controlando la asignación de derechos de acceso a los funcionarios, contratistas y terceros, a los sistemas de información, bases de datos y servicios de información mediante la aplicación de los catorce controles como son [1] [3]: políticas de control de accesos, control de acceso a las redes, gestión de registros de usuarios, gestión de derechos de usuarios, gestión de privilegios de acceso, gestión de información confidencial, revisión de los derechos de acceso de los usuarios, retirar o adaptar los derechos de acceso, uso de información confidencial para la autenticación, restricción del acceso a la información, procedimientos seguros de inicio de sesión, gestión de contraseñas de usuario, uso de herramientas de administración de sistemas y control de acceso al código fuente [1].

Estos controles se documentaron y fueron comunicados y especificados en cuanto a su cumplimiento, para que estén debidamente sustentados y puedan ser adoptados por la Oficina de Sistemas de la Alcaldía de Popayán, permitiendo con ello mejorar su plan de mejoramiento en cuanto al control de acceso a los sistemas de información.

1.2 PALABRAS CLAVES

Seguridad informática, ISO 27002:2013, control de acceso, Alcaldía

1.3 ABSTRACT

It is presents an proposal for managing informatic security in the mayoralty of Popayan using as a base the ISO 27002:2013.

Today, the Mayoralty of Popayán does not have a defined access control policy for its information systems, therefore, it is proposed to define the four objectives of the access control domain for its systems, which are based on: guarantee Access to authorized users and prevent unauthorized access to information systems and services; Make users responsible for the protection of information for identification; Prevent unauthorized access to information compiled by systems and applications, and make users responsible for the protection of information for identification [1] [2].

To do this, it is necessary for the Office to define an access policy including the fourteen controls of the access control domain, through strategies to prevent unauthorized access to information systems and controlling the allocation of access rights to the Information systems, databases and information services through the application of the fourteen controls such as [1] [3]: access control policies, access control to networks, management of User registration, user rights management, access privilege management, management of confidential information, review of user access rights, withdrawal or adaptation of access rights, use of confidential information for authentication, access restriction To information, secure login procedures, user password management, use of administration tools Of systems and control of access to the source code [1].

These controls were documented and communicated and specified in terms of their compliance, so that they were adequately supported and could be adopted by the Mayor's Office of Systems in Popayan, thereby improving their improvement plan in terms of access control to Information systems.

1.4 KEYWORDS

Informatic security, ISO 27002:2013, access control, information system, Mayoralty

1.5 INTRODUCCIÓN

Hoy en día, la información es el activo más importante de una empresa al ser el eje principal de apoyo a la toma de decisiones, en especial de los altos directivos organizacionales; por ello, es de vital importancia establecer una política de control de acceso a los sistemas de información de una organización teniendo

claras las necesidades y objetivos de seguridad en los diferentes procesos definidos en la organización [1][2].

Por lo anterior, surge esta propuesta de seguridad en la cual se definen los requerimientos para el control de acceso a los sistemas de información de la Alcaldía de Popayán, utilizando como base la norma ISO 27002:2013. Esto lleva a proponer una política de control de acceso que pueda entre otras cosas, registrar el ingreso de manera correcta de los funcionarios, contratistas y terceros a los sistemas de información de la Alcaldía.

La Alcaldía de Popayán al ser un ente gubernamental, maneja gran cantidad de información confidencial; sin embargo, no se tiene manejo del grado de seguridad que manejan los sistemas de información, lo que puede generar problemas al presentar informes sobre las actividades que realizan dentro de ella. Esto implica que es necesario identificar cómo se encuentra la Alcaldía actualmente frente a la seguridad informática, cómo se encuentran otras alcaldías frente a dicha seguridad y qué proponen las normas para el control de acceso a la información [2].

Esta propuesta, brinda orientación y recomendaciones acerca de cómo mejorar los procesos de protección de la información de accesos no autorizados [3] y para su ejecución, es necesario contar con la cooperación de los funcionarios, contratistas y terceros, adoptando las medidas aquí definidas, siendo conscientes de su responsabilidad frente a la subsistencia de controles de acceso tales como los relacionados con el uso de contraseñas y la seguridad del equipamiento [1][2].

En esta propuesta se presenta una identificación del estado actual de la Alcaldía de Popayán frente al tema de seguridad informática, una definición del estado actual de algunas Alcaldías en Colombia con respecto a la seguridad informática, las características básicas con las que debe contar un sistema de control de accesos a los sistemas de información en una organización, para establecer los lineamientos a seguir por la Alcaldía de Popayán y las sugerencias de las estrategias necesarias para realizar el control de acceso a los sistemas computarizados de la Alcaldía de Popayán, que sirvan como base a la Alcaldía para la definición de una política de control de acceso a los sistemas de información.

1.6 PLANTEAMIENTO DEL PROBLEMA

Desde la perspectiva empresarial, la información se ve afectada por muchos factores, entre los que se encuentran la confidencialidad, la integridad y la disponibilidad de la misma, siendo éstos los principales problemas a los que se enfrenta el manejo de la información [4]. Ocurriendo casos como en el que una persona no autorizada altera la información, usurpa datos, filtra información, clasifica y desclasifica datos, observa información clasificada y/o confidencial, etcétera.

La medida de seguridad que deben adoptar las organizaciones para mitigar el riesgo en el manejo de la información es la política de seguridad [5], la cual brinda el mecanismo para regular el uso de la información y algunos aspectos del tratamiento de la información, como el alta y baja de usuarios y el acceso de los mismos a los sistemas de la Organización. Sin embargo, la Alcaldía de Popayán no ha dado la importancia necesaria a mantener segura la información, poniendo en riesgo sus operaciones informáticas [7].

Cabe anotar que tampoco analiza las vulnerabilidades a los que está expuesta, llevando un funcionamiento inadecuado y de alto riesgo en lo referente a los sistemas de información, teniendo en cuenta que el manejo de ésta es responsabilidad de todos los funcionarios que hacen parte de la organización.

De lo anterior se deriva que actualmente la Alcaldía de Popayán no cuenta con una política de control de acceso a la información, lo que genera una mala imagen institucional y un manejo poco confiable de la información [7]. El personal que trabaja en la Oficina de Sistemas constata el riesgo que sufren por no tener políticas de seguridad, por eso mismo han venido trabajando únicamente aspectos genéricos y básicos de dicho tema, lo cual propicia el planteamiento de la siguiente pregunta:

¿Es posible hacer una propuesta para el manejo del control de acceso a los sistemas de información computarizados de la Alcaldía de Popayán, basada en la Norma ISO 27002:2013?

1.7 JUSTIFICACIÓN

Actualmente, la implementación de una política de control de acceso en una organización es una temática útil y necesaria, obligando a que todos los funcionarios organizacionales, desde el nivel estratégico hasta el operativo de las empresas, sean los responsables de ella. La Alcaldía de Popayán y, en especial, la Oficina de Sistemas, son conscientes de ello, por lo tanto, se quiere definir una

política de control de acceso partiendo de la conceptualización de los controles de acceso a los sistemas de información por parte de los empleados de la Alcaldía.

1.8 OBJETIVOS

1.8.1 General

Definir una propuesta para el manejo de los controles de acceso a los sistemas de información computarizados en la Alcaldía de Popayán, con el fin de comenzar a establecer una política de seguridad informática en la organización.

1.8.2 Específicos

1. Identificar el estado actual de la Alcaldía de Popayán frente al tema de seguridad informática, con el fin de establecer un punto de partida inicial de la propuesta.
2. Definir el estado actual de algunas Alcaldías en Colombia con respecto a la seguridad informática, con el fin de tener un referente para las estrategias que se planteen para la Alcaldía de Popayán.
3. Especificar las características básicas con las que debe contar un sistema de control de acceso a los sistemas de información en una organización, para establecer los lineamientos a seguir por la Alcaldía de Popayán.
4. Sugerir las estrategias necesarias para realizar el control de acceso a los sistemas computarizados de la Alcaldía de Popayán, que sirva como base a la Alcaldía para la definición de una política de control de acceso a los sistemas de información.

CAPÍTULO 2. MARCO TEÓRICO

CAPÍTULO 2. MARCO TEÓRICO

2.1 MARCO CONCEPTUAL

2.1.1 Información

Es el conjunto de datos organizados y procesados que constituyen mensajes dando un significado a las cosas, objetos y entidades del mundo a través de códigos y modelos. Para la informática constituyen instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador [8].

2.1.2 Activo de información

Cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros), que tiene un valor para la institución y sea un riesgo su perdida, su alteración y la llegada a manos equivocadas [4].

2.1.3 Credenciales de acceso

Privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten el acceso a los sistemas de información manuales y/o computarizados [9].

2.1.4 Seguridad en la información

Son todas aquellas medidas preventivas y reactivas dispuestas que permiten resguardar y proteger la información [4].

2.1.5 Proceso

Se define como "conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados" [5].

2.1.6 Procedimiento

Describe detalladamente una serie de acciones establecidas con el fin de realizar actividades para lograr un objetivo [10].

2.1.7 ISO/IEC 27001:2013

Esta norma es orientada a los aspectos netamente organizacionales, es decir, “Organizar la seguridad de la información”, por tal motivo tiene una secuencia de acciones tendientes al establecimiento, implementación, operación,

monitorización, revisión, mantenimiento y mejora del Sistema de la Seguridad de la Información (SGSI) [11].

Con respecto al control de acceso, se tiene dentro de la norma: "**A9:** El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho".

2.2 ISO/IEC 27002:2013

Esta norma busca describir con un máximo detalle cada uno de los controles y objetivos de control que se deben considerar a la hora de implanta un SGSI correcto [1].

2.2.1 Seguridad

La seguridad tiene como fin la protección de la información y de los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada de la información [9].

2.2.2 Informática

La informática hace parte de la ingeniería, la cual se encarga de administrar grandes volúmenes de información a registrar o a contabilizar para futuras consultas o para llevar el record o control de alguna oficina o empresa, utilizando herramientas de hardware y el software que las automaticen [12].

2.2.3 Seguridad Informática

Hace referencia a las herramientas desarrolladas para proteger la información de una organización desde los equipos informáticos. Su principal objetivo es proteger el activo más importante que tiene la empresa, la información, ya que sus estrategias de negocio dependerán del almacenamiento, procesamiento y presentación para garantizar la seguridad de los sistemas de información deben cumplir los tres fundamentos básicos de seguridad que son [10]:

- Disponibilidad. Es la capacidad de poder acceder a información [2].
- Integridad. Se establece como la necesidad de garantizar que la información no haya sido manipulada [2].
- Confidencialidad. Es la capacidad de proteger la información mediante un acceso a usuarios autorizados y la negación a los no autorizados[2].

2.2.4 Riesgos

Es una medida que consiste en la posibilidad del incumplimiento de un objetivo. La Organización Internacional de Normalización (ISO) define riesgo como la probabilidad de que una amenaza se materialice generando pérdidas o daños de información [7].

2.2.5 Análisis de riesgos

Consiste en identificar los riesgos de seguridad en la organización, determinar su magnitud e identificar las áreas que requieren implantar controles [3].

2.2.6 Amenaza

Consiste en identificar los riesgos de seguridad en la organización, determinar su magnitud e identificar las áreas que requieren implantar controles [2].

Son los eventos que pueden desencadenar un incidente produciendo daño en la información [4].

Tipos de Amenaza. Se deben considerar las diversas amenazas que puede afectar la información como se muestra en la siguiente ilustración [13].

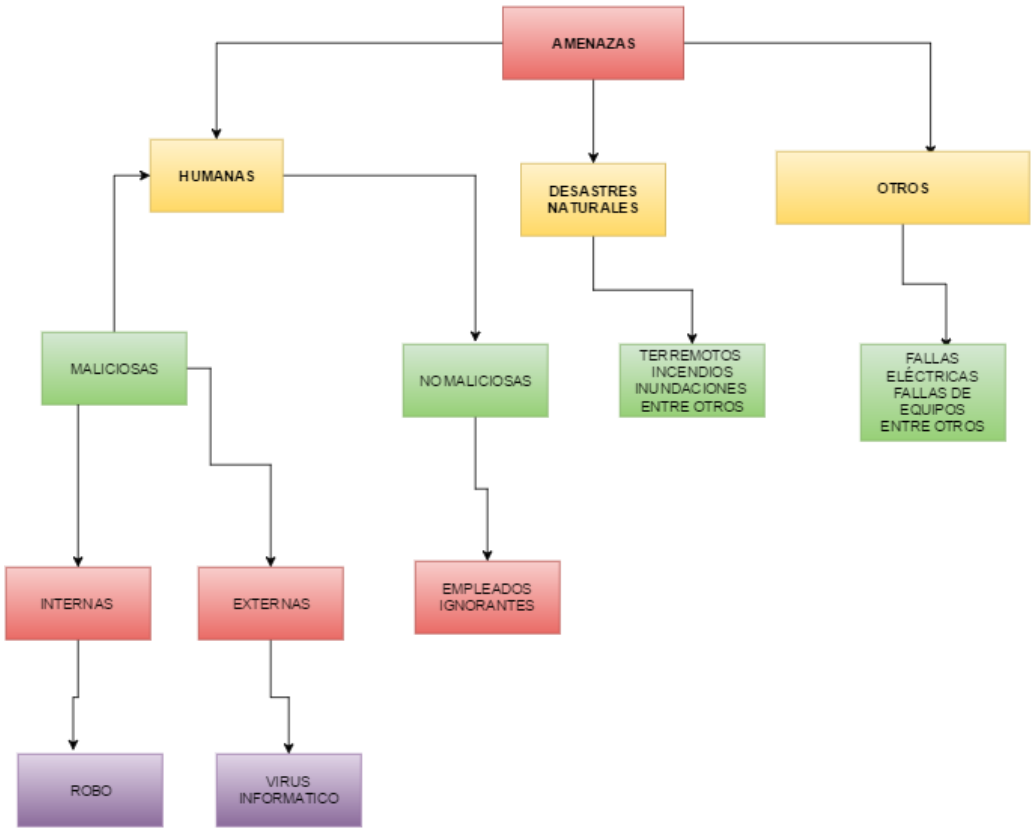


Figura 1: Amenazas a la información. Fuente: Propia

Las amenazas humanas son aquellas acciones provocadas por una persona para hacer daño, para "jugar", entre otros, y pueden ser de tres tipos [14]:

- Maliciosas. Los equipos deben situarse y protegerse para reducir el riesgo de ejecución de las amenazas del entorno, así como las oportunidades de acceso no autorizado [15].
- Las Amenazas Externas. Afectan el desarrollo de las actividades de la empresa, son frecuentemente ocasionadas por el acceso a internet software maliciosos, hackers, y entre otras amenazas que al infiltrarse en la red de la organización pueden inducir a daños en los sistemas.
- Las Amenazas Internas. Son ocasionadas por los funcionarios y ex funcionarios de la organización, afectando la integridad organizacional al violar las políticas de seguridad establecidas [7].

2.2.7 Control de acceso

Es una de las actividades más importantes de la arquitectura de seguridad de un sistema. Se refiere a los controles que garantizan el acceso a los usuarios autorizados e impiden los accesos no autorizados a los sistemas de información[16].

Los procedimientos corresponderían a cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos usuarios, hasta su culminación cuando ya no sea necesario su acceso a los sistemas y servicios de información [17].

Para poder cumplir con este procedimiento, este apartado lo hace a través de controles agrupándolos de esta manera.

2.2.8 Requerimientos de negocio para el control de accesos

Debe existir una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determinen el nivel de riesgo de cada activo [1] [2].

2.2.9 Administración de accesos de usuarios

Se establecen los procedimientos que garantizan una adecuada administración de los permisos de acceso de usuario a los sistemas de información, realizando revisiones periódicas que generan al administrador de seguridad herramientas para realizar sus evaluaciones lo más eficientemente posible [1] [2].

2.2.10 Responsabilidades de usuarios

Dentro de la organización todos los usuarios deben tener documentadas las obligaciones dentro de la seguridad de la información de la empresa. Independientemente de la jerarquía, los usuarios tienen alguna responsabilidad a partir del momento que accedan a la información de la organización, existiendo diferentes grados de responsabilidad que son proporcionales a las obligaciones derivadas de sus funciones [1] [2].

2.2.11 Control de acceso a redes

Todos los servicios de red deben ser susceptibles a aplicar medidas de control de acceso, por lo cual es necesario prevenir el acceso de los usuarios a servicios internos y externos en red con los mecanismos de autenticación adecuados que se aplican a los usuarios y equipos [18].

La primera medida que se establece para este control de acceso es definir una política de uso de los servicios de red, para que los usuarios sólo puedan acceder a los servicios específicamente autorizados. Luego se centra el control de acceso remoto a la organización sobre el cual deben existir medidas apropiadas de autenticación [1] [2].

2.2.12 Control de acceso a sistemas operativos

Consiste en impedir el acceso no autorizado al sistema operativo donde se utilizan herramientas de seguridad del sistema que permiten el acceso exclusivo a los usuarios autorizados [1] [2].

Las prestaciones de las herramientas deben ser capaces de registrar la autenticación de los usuarios autorizados, los intentos de autenticación correctos y fallidos del sistema, emitir señales de alarma cuando se violan las políticas de seguridad del sistema operativo [17].

2.2.13 Control de acceso a información y aplicaciones

Este grupo de control de acceso posee dos controles, los cuales están dirigidos a prevenir el acceso no autorizado a la información acezada por las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y, a su vez, el aislamiento de los sistemas débiles del resto de la infraestructura, los cuales no pueden ser accedidos desde ninguna red, solamente en un lugar físico en donde se encuentran [1] [2].

CAPÍTULO 3. DEFINICIÓN DEL OBJETO DE INVESTIGACIÓN

CAPÍTULO 3. DEFINICIÓN DEL OBJETO DE INVESTIGACIÓN

3.1 ESTADO DEL ARTE

En este capítulo se muestra las generalidades encontradas en algunos artículos con respecto a la implementación del control de acceso en los sistemas de información.

3.1.1 Seguridad en sistemas de información

Los tipos de seguridad que deben tener los sistemas de información comprenden un conjunto de defensas o medidas, cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema; por ejemplo, impedir el acceso a la información a usuarios no autorizados mediante la introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando antivirus en los sistemas operativos e imposibilitar mediante encriptación la lectura no autorizada de mensajes [19].

El término política de control de acceso, se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica, en términos generales, qué está y qué no está permitido en el área de seguridad durante la operación general de acceso a dicho sistema. Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema, quien puede acceder, a que parte del sistema de información en que momento y para realizar qué tipo de operaciones; todo esto debe establecerse en una política de control de acceso definida por las organizaciones [20].

Con estas medidas se evita la interrupción que consta en deshabilitar el acceso a la información, como destruir componentes físicos como el disco duro, bloqueando el acceso a los datos o saturar los canales de comunicación que haya dentro de la organización. Las personas, programas o equipos no autorizados no podrán acceder a recursos de los sistemas y captar información confidencial de la organización como datos programas o identidad de personas o funcionarios [20].

Los mecanismos de control de acceso sirven para decidir si el usuario puede obtener o no acceso a los recursos de los sistemas de información, es decir, asegurar que solo los usuarios autorizados tengan acceso a un sistema particular y a sus recursos individuales y que el acceso y modificación de una parte particular de los datos se limite a individuos y programas autorizados [21].

En muchos casos, los mecanismos de control de acceso se implementan dentro de un computador para controlar al acceso a éste. Sin embargo, el acceso a un computador se produce por medio de una red o un dispositivo de comunicaciones. Las medidas tomadas para el control de acceso en un sistema de proceso de datos se pueden clasificar en dos categorías, los asociados con el usuario y las asociadas con los datos [21].

Con respecto a la seguridad, el registro y generación de informes de seguridad por parte del sistema operativo de todos los intentos inválidos de entrada y otros eventos contra la seguridad, como los intentos de ejecutar aplicaciones sensibles, programas de utilidad o modificación, hacen más difícil el control de acceso a los equipos de cómputo. Por ello, es bueno utilizar contraseñas alfanuméricas de ocho o más caracteres de longitud, no relacionadas con el usuario y fácilmente recordables para que este no tenga que escribirlas en librerías vulnerables [22].

El control de acceso de usuarios descentralizado trata la red como un enlace de comunicaciones transparente y el procedimiento de apertura de sesión usual lo realiza el computador destino. Se debe tener en cuenta la seguridad referente a las contraseñas que se trasmiten sobre la red. Pueden utilizarse dos niveles de control de acceso. Los computadores individuales proporcionan un servicio de apertura de sesión para proteger sus recursos y aplicaciones específicas. Y la red puede proporcionar protección para restringir el acceso a la red a usuarios autorizados [21]

La accesibilidad y familiaridad con las TIC por parte de un colectivo creciente de personas, ha aumentado significativamente el nivel de las amenazas en los sistemas de información, esto ha dado lugar a que cada vez hay mayor cantidad de personas desinhibidas por barreras morales, que están dispuestas y son capaces de producir daños en los sistemas de información por diferentes motivos, los cuales pueden ser económicos, psicológicos o simplemente terroristas [15].

El conjunto de personas que interactúan con los sistemas de información: administradores programadores, usuarios internos y externos y resto de personal de una empresa u organización producen más fallos de seguridad por intervención del factor humano que por fallos en la tecnología, cuando no utilizan adecuadamente, o no existe, la política de control de acceso a la información [23].

La integridad de la información es la primera disposición de una política de control de acceso proporcionando a las organizaciones, es la protección contra la

modificación de datos. Estas medidas se utilizan para proveer servicios de mantenimiento de la información de los datos y de autenticación de origen por parte de los usuarios que puedan acceder a ella [23].

El control de acceso es la capacidad de limitar y controlar el acceso a sistemas host y aplicaciones por medio de comunicaciones. Para conseguirlo, cualquier entidad que intente acceder debe antes ser identificada o autentificada, de forma que los derechos de acceso puedan adaptarse de manera individual [17].

3.1.2 Para la Alcaldía de Popayán

Se identificó el estado actual de la Alcaldía de Popayán respecto a la seguridad informática, con el fin de obtener una recopilación sobre las herramientas informáticas que utilizan para la seguridad de la información y así llevar a cabo un proceso de control de acceso a los sistemas de información. Dentro de lo encontrado allí, se tiene:

Seguridad Perimetral

La seguridad e integridad informática de una empresa es primordial. Los ataques por red y pérdidas de información ocasionan que la prestación de los diferentes servicios que tiene a cargo la Alcaldía se realice de manera inadecuada.

La protección de los servicios informáticos garantiza un correcto aprovechamiento de la infraestructura y garantiza la integridad y confidencialidad de la información. La seguridad perimetral con la que cuenta la Alcaldía de Popayán se describe a continuación [10]:

- **Firewall**

Es un software que protege a un computador o una red de computadores contra intrusiones provenientes de internet; por esta razón, los computadores que están permanentemente conectados a la red y no están siendo controlados de manera adecuada por parte de la organización, haciéndolos vulnerables a ataques informáticos y esto conlleva a la necesidad de implementar un sistema de firewall que puede instalarse en computadores que utilicen cualquier sistema, siempre y cuando:

- No se haga ningún otro servicio más que el servicio de filtrado de paquetes en el servidor [7].
- El sistema sea seguro [7].
- La computadora tenga capacidad suficiente como para procesar el tráfico [24].

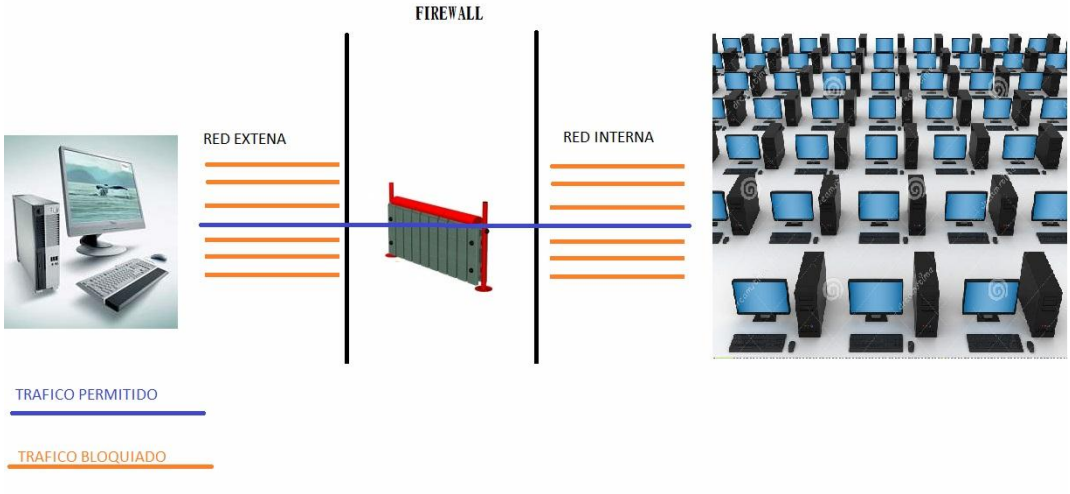


Figura 2: Firewall. Fuente: Propia

La manera en que funciona el firewall de la Alcaldía de Popayán es mediante unas reglas determinadas que permiten al sistema realizar la conexión, denegar la conexión y rechazar solicitudes de conexión [25].

Acción	IP Origen	IP Destinataria	Protocolo	Puerto fuente	Puerto destino
Aceptar	192.168.10.20	194.154.192.3	TCP	cualquiera	25
Aceptar	cualquiera	192.168.10.3	TCP	cualquiera	80
Aceptar	192.168.10.0/24	cualquiera	TCP	cualquiera	80
Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Tabla 1. Direcciones IP. Fuente: Oficina de sistemas

El filtrado de paquetes de datos que hace el sistema de firewall de la Alcaldía de Popayán se ejecuta cuando hay un intercambio entre un computador con red interna y un computador de red externa. Así, los paquetes de datos que pasa por el firewall son analizados sistemáticamente mediante el TCP (Protocolo de Control de Transmisión), el cual se encarga de la comunicación de datos en las redes en base a las direcciones IP, las cuales identifica la dirección del computador que envía los paquetes y del ordenador que los recibe [5].

- **Sistema UTM hardware y software**

La gestión unificada de amenazas que se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad de red, por lo general, un único producto de seguridad que ofrece varias funciones de seguridad en un sólo punto en la red [6]. El producto UTM que cuenta la Alcaldía

de Popayán incluye funciones como anti-spyware, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Estas características y funciones incluyen total o parcialmente prevención y detección de intrusiones (IDS/IPS), antivirus, filtrado anti spam y filtrado de contenido Web, así como las funciones convencionales de firewall [25].

Esta herramienta da solución de seguridad todo en uno, la cual integra todo lo necesario para proteger la red de la Alcaldía de Popayán.

- Control de tráfico de red desde y hacia Internet.
- Protección contra ataques externos.
- Control de usuarios.
- Generación y administración de VPN´s.
- Conexión para equipos remotos (portátiles y dispositivos móviles).
- Gestión de ancho de banda de internet.
- Sistemas de Detección de Intrusos.
- IPS.
- Validación de ingreso de usuarios a red.

- **(kasperky) Consola de antivirus**

La Consola de Administración que posee la Alcaldía de Popayán, consta de una interfaz que provee acceso a las funciones del servidor de manera local o remotamente a través de la red. Técnicamente, la consola de administración es un módulo para Microsoft Management Console, es decir, la interfaz estándar para ejecutar las tareas administrativas en los sistemas operativos Microsoft Windows basados en la tecnología NT[26].

La consola de administración se usa para administrar cualquier número de servidores instalados en la red corporativa de la Alcaldía. También puede instalar una consola a cualquier ordenador en la red corporativa que satisface los requerimientos del sistema. Puede instalar cualquier número de consolas en una red. Además, hay posibilidad de instalar/actualizar la versión de la consola de Administración de forma remota [27].

La interfaz de la consola de administración que utiliza la Alcaldía de Popayán, necesita tener los complementos (plug-ins) de control de aplicación para mostrar correctamente las medidas de las aplicaciones de Kaspersky Lab. Los complementos de control de aplicación son diferentes para cada aplicación y se instalan en la consola brindando a la Alcaldía de Popayán navegación segura, antispyware, el cual desactiva los servicios de red que no se utilizan, codifica la información (criptografía), monitorea la utilización de software con garantía (legales), y monitorea la entrada a la red por correo y páginas web [27] [25].

- **(Arcserve backup) Sistema de recuperación de desastres licenciado.**

El sistema de recuperación que utiliza la Alcaldía de Popayán es Arcserve Backup, el cual ofrece un número de funcionalidades que trabajan juntas para ayudar a reducir el tiempo que pasa administrando sus backups[17]. Las soluciones de Arcserve Backup[28] proporciona funcionalidades de "clase empresarial" que han sido optimizadas para respaldar arquitectura de TI con tecnologías virtuales y en la nube, sin importa cuán simples o complejos sean sus datos o su infraestructura de TI [24].

Las funciones que cumple el Arcserve Backup en la Alcaldía son:

1. Recupera datos de forma fácil y confiable.
2. Proteja datos confidenciales y preserve la productividad organizacional.
3. Recupera rápidamente luego de interrupciones en el sistema y pérdida de datos, antes de que el tiempo de inactividad afecte negativamente a las operaciones del negocio o a las relaciones con los clientes.
4. Backup rápido con recuperación granular para simplificar la protección de datos en estaciones de trabajo y servidores físicos y virtuales.

Problemas puntuales en el manejo de la información en la Alcaldía de Popayán

Los principales problemas que se encontraron en la Alcaldía de Popayán respecto al manejo de la información es, la falta de una política de seguridad, la cual se define como el conjunto de requisitos defendidos por responsables directos o indirectos de un sistema, que indica en términos generales lo que está y lo que no está permitido. Para esto existen normas que ayudan a las empresas a crear políticas de seguridad [2].

Los problemas que enfrenta la Alcaldía de Popayán al no contar con una política de seguridad se basan en tres principios básicos que se describen a continuación:

I. **Integridad**: “Representa que el sistema no debe modificar ni corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite cerciorar que no se ha falseado la información. Por ejemplo que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados sin que se haya producido ninguna modificación, adición o borrado” [2].

   Para recalcar, es de suma importancia señalar que una información integra, es una información que no ha sido alterada de manera indebida y cuando esto ocurre significa que los datos han perdido su valor.

Los funcionarios de la Alcaldía de Popayán deben tener la seguridad de que la información que están obteniendo, leyendo y trabajando, es exactamente la misma que fue colocada desde un principio, es decir, que sea la información original. Si esta llegase a sufrir alteraciones, puede ocasionar grandes conflictos como perdida de información, afectando la comunicación y la toma de decisiones en la Alcaldía, en cuanto la información puede ser alterada de diversas formas [3]:

- Modificación de contenido en los documentos y sistemas de información: se realizan inserciones o sustituciones de partes de su contenido [2].
- Modificación en los elementos que soportan la información: se realizan alteraciones en la estructura física y lógica donde la información se encuentra almacenada, por ejemplo, los computadores y los servidores que cuenta la organización [2] .

Por esta razón, es necesario tener la certeza de que únicamente las personas autorizadas realicen un control de acceso y puedan realizar alguna modificación en la forma y el contenido de la información, garantizando así la integridad de esta [5].

II. **Confidencialidad**: “Se refiere a la capacidad del sistema para evitar que personas o procesos no autorizados puedan acceder a la información en él” [2].
La información no debe ser conocida por todos los individuos de la organización, en este caso la Alcaldía de Popayán, debido a que se puede hacer un uso inapropiado de está, causando múltiples daños a la organización en cuanto al manejo de la información [29].

Si los usuarios de la Alcaldía revelan sus contraseñas, se corre el riesgo de que alguien pueda hacer un uso indebido de la información, en el sentido se tiene el control de acceso fácilmente a los sistemas de información; a esto se lo conoce como ingeniería social. Un ataque muy habitual es el del phising [15], que consiste en conseguir información confidencial para obtener un beneficio como la realización de fraudes [1] .

III. **Disponibilidad**: “Representa que el sistema, tanto hardware como software, se mantiene funcionando eficientemente y que es capaz de recuperarse de una falla” [2].

La disponibilidad permite que la información pueda ser utilizada cuando sea necesario, teniendo en cuenta el acceso de las personas autorizadas, de esta forma, la información debe ser accedida de forma segura para que se pueda usar en el momento en que se solicita [2].

La Alcaldía al no llevar un funcionamiento correcto está expuesta a sufrir cualquier tipo de ataque, teniendo como resultados daño a la reputación como entidad gubernamental del Estado y consecuencias legales, entre otros [5].

Autorización para el uso de infraestructura de información

La Alcaldía de Popayán establece que la adquisición de infraestructura nueva para el procesamiento de información (equipos, software, aplicaciones e instalaciones físicas), debe ser analizada y revisada por el Comité de Seguridad y el Secretario de Despacho del área directamente afectada. Esta autorización estará regida de acuerdo a los procedimientos respectivos y asegurará que las políticas de seguridad sean cumplidas en su totalidad [25][30].

Acuerdos de confidencialidad

Todos los funcionarios de la entidad y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información, de acuerdo con los criterios establecidos en ella [25][30].

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la entidad a personas o entidades externas [25].

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Contacto con las autoridades y con grupos de interés especial

La entidad debe establecer y mantener una relación cercana con autoridades relevantes (policía, bomberos, defensa civil), así como con grupos de interés o foros de especialistas en seguridad, para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información [25].

Auditorías internas

La Alcaldía de Popayán realiza revisiones internas a su Modelo de Gestión de Seguridad de la Información con el fin de determinar si las políticas,

actividades, procedimientos y controles establecidos dentro del sistema, están conformes con los requerimientos institucionales, requerimientos de seguridad, regulaciones aplicables, demostrando si éstos se encuentran implementados y mantenidos eficazmente [25].

Estas auditorías se ejecutan según lo establecido en el programa de auditorías definido por la Oficina de Control Interno, para quien, en caso de ser necesario, pueden programar revisiones parciales o totales sobre un proceso, área, entre otros, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades [25].

Riesgos relacionados con terceros

La entidad identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga [30].

Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos [25][30].

CAPÍTULO 4. CUMPLIMIENTO DE OBJETIVOS

CAPÍTULO 4. CUMPLIMIENTO DE OBJETIVOS

OBJETIVO ESPECÍFICO 1

4.1 LA ALCALDÍA DE POPAYÁN

La Alcaldía de Popayán es una entidad de carácter público. Cuenta con una Oficina de Sistemas [25] en su Sede Central; allí, se encuentran ubicados los funcionarios del Área y los servidores de las aplicaciones administrativas (Aplicaciones de la Alcaldía Popayán). Esta Oficina tiene un área para el mantenimiento preventivo y correctivo [30] que hace parte de los servicios tecnológicos. Una de sus funciones, entre otras, es establecer el plan anual de mantenimiento preventivo realizado por dos pasantes, el cual se aplica a todos los equipos que hacen parte de la Alcaldía (anexo 1), así, el mantenimiento correctivo depende de la necesidad y los recursos que haya para efectuar las reparaciones que sean requeridas [30].

El sistema eléctrico tiene procedimientos de interrupción y regulación a través de UPS (Sistema de Alimentación Interrumpida) [31]. Además, se realiza la restauración de copias de seguridad (*backup*) [32], las cuales se encuentran descritas en un procedimiento detallado, en el que se define el sistema de recuperación de desastres, el cual incluye las copias de seguridad de las bases de datos, del directorio activo, de las carpetas compartidas en algunos computadores que manejan información crítica, utilizando así un sistema centralizado que almacena la información en cintas etiquetadas con la fecha. La rotación de estas cintas se ejecuta cada vez que se llenan (aproximadamente cada mes); mientras tanto, en el caso de pérdida de datos se recupera la copia de seguridad [13].

También existen tableros de mando eléctrico que están identificados, aislados y con seguridad para que no sean manipulados por personal no autorizado; en su mayoría, los tomacorrientes de las redes eléctricas y de datos están debidamente identificados [31].

La Alcaldía cuenta con un sistema de seguridad contra incendios en el que se ubican de manera física, extintores en todas las dependencias: Despacho del Alcalde, Secretaría de Educación, Secretaría General, Secretaría de Gobierno, Secretaría de Hacienda, Secretaría de Infraestructura, Secretaría de Salud, Secretaría de Tránsito y Transporte, Secretaría del Deporte y la Cultura.

Con respecto a las redes de datos, tiene un sistema de cableado estructurado y de telecomunicaciones en todas las dependencias antes mencionadas, con concentradores y redes de datos. Estas se encuentran administradas por switches cisco dos switches catalyst 3650, dos catalyst 2960-cx, dos 3560-cx 3650 y un switches 3com 4500 al igual que routers cisco dos 830, dos 890 ISR y dos rompe

muros TL-WR841HP que propagan la red de forma inalámbrica para los equipos portátiles [33].

La seguridad perimetral [34] que posee la Alcaldía de Popayán, permite en la actualidad minimizar los problemas de ataques externos y de seguridad interna. En cuanto al control de acceso físico a la Alcaldía de Popayán, ésta tiene un sistema de vigilancia privado que es SERVAGRO Ltda [35], quien brinda seguridad en las entradas principales y secundarias de la Alcaldía, ofreciendo un sistema de cámaras con circuito cerrado y, acompañamiento de la policía nacional, la cual se encarga de una revisión física a las personas que ingresen a las instalaciones de la Alcaldía.

Los funcionarios para ingresar a las instalaciones de la Alcaldía se identifican con un carnet que contiene foto personal, nombre y apellidos, Rh y dependencia a la que pertenecen. Generalmente, a los funcionarios se les hace un proceso de inducción y capacitación para las responsabilidades y reglamento interno en cuanto al manejo de la información. Respecto al correo interno, la seguridad lo brinda el proveedor del servicio que es Bosh [36] y las buenas prácticas de los usuarios [37].

APLICACIONES	DESCRIPCIÓN	CARACTERÍSTICAS PRINCIPALES	NIVEL DE SEGURIDAD
NOMINA	Listado de servidores públicos donde se indica su asignación básica mensual y demás auxilios (transporte, alimentación, viáticos, gastos de representación, etcétera), a los que tenga derecho, y deducciones establecidos por la normatividad laboral colombiana.	- Permite la gestión de múltiples contratos de trabajo y condiciones de pago. - Nómina de Semanal, Quincenal y Mensual Aplicación de escritorio	- Usuario y contraseña - Su acceso se limita al ordenador donde están instaladas. - Requieren instalación personalizada
ALMACÉN	Procedimiento donde se almacenan, suministran y controlan los materiales necesarios en las calidades requeridas, cantidades suficientes y en el momento oportuno; para la ejecución de los programas y metas fijadas por la Administración municipal, para facilitar el desenvolvimiento normal de las actividades propias del Municipio.	- Disponibilidad de caja - Comité de compras - Orden de pedido, convocatoria, pública o licitación - Ingreso de elementos	- Usuario y contraseña - Su acceso se limita al ordenador donde están instaladas. - Requieren instalación personalizada
CONTRATACIÓN	Es la ejecución de un contrato a un individuo o empresa contratista donde se establece las partes intervinientes, en este caso la Alcaldía y empleado u organización, de acuerdo a la realización de un determinando trabajo o actividad donde percibirá una suma de dinero estipulada en el contrato antes mencionado	- Para la realización de una obra o servicio determinado - Trabajadores contratados en la Alcaldía - Los contratos por tiempo determinado	- Usuario y contraseña - Su acceso se limita al ordenador donde están instaladas. - Requieren instalación personalizada
SISTEMA DE INFORMACIÓN DOCUMENTAL ORFEO	Orfeo es un sistema web que le permite a la organización acceder fácilmente mediante cualquier navegador, a través de Internet o Intranet, para gestionar la trazabilidad de los documentos, evitando así en un gran porcentaje, el manejo de documentos físicos	- Es una herramienta web de fácil acceso mediante cualquier navegador. - Permite a los trabajadores el fácil acceso y trámite de tareas desde cualquier lugar donde haya conexión a Internet. - Interfaz Web intuitiva al usuario, similar al manejo de un correo electrónico.	- La información que maneja es accesible mediante internet - Usuario y contraseña - Depende del proveedor de internet el acceso
SISTEMA DE INFORMACIÓN PREDIAL Y IMPUESTO DE INDUSTRIA Y COMERCIO (ICA)	Es un tributo de periodicidad anual que graba el valor de los predios urbanos y rústicos. Para efectos del Impuesto se considera predios a los terrenos, incluyendo los terrenos ganados al mar, a los ríos y a otros espejos de agua; así como, las edificaciones e instalaciones fijas y permanentes que constituyan partes integrantes de dichos predios, que no pudieran ser separadas sin alterar, deteriorar o destruir la edificación. Es un Impuesto Directo, de naturaleza territorial, que deben pagar las personas naturales o jurídicas por la realización directa o indirecta de actividades industriales, comerciales o de servicios, de manera permanente u ocasional, con o sin establecimiento de comercio.	- Permite a los trabajadores fácil acceso - Ingreso de elementos - Aplicación de escritorio - Interfaz web - Declarar y pagar el Impuestos de ICA	- Son dependientes del sistema operativo que utilice el computador y sus capacidades (video, memoria, etcétera) - Usuario y contraseña - Depende del proveedor de internet el acceso
FINANZAS PLUS	El Sistema de administración de recursos financieros ofrece las herramientas necesarias para la planeación, evaluación, control y auditoría de las operaciones financieras, mediante un modelo de sistemas modular e integrado, el cual permite la actualización en línea de la información entre Presupuesto, Tesorería y Contabilidad en cada una de las Unidades Administrativas que componen una empresa (Secretarias, Dependencias, Departamentos, etcétera), a través de procesos centralizados o descentralizado.	- Estandarización de datos. - Sistema orientado al “Usuario Final”. - Facilidades en la consulta. - Información y procesos en línea - Proceso de interfaces.	- Requiere sistemas Operativos: certificados por Oracle (Linux, Unix, NT). - Redes: LAN, WAN. Protocolo TCP/IP. - Usuario y contraseña

Tabla 2. Aplicaciones de la Alcaldía Popayán. Fuente: Oficina de Sistemas

En resumen, la Alcaldía de Popayán cuenta con:

CARACTERÍSTICAS	DESCRIPCIÓN	ESTADO
Acceso a las Instalaciones	Este acompañamiento lo hace la Policía Nacional y SERVIAGRO Ltda empresa de seguridad privada. Están presentes en las entradas y salidas que tiene la Alcaldía de Popayán	Estas organizaciones tanto públicas como privadas tienen como función principal brindar seguridad interna como externa, encargándose que todo personal que ingrese a la Alcaldía no presenten amenazas al funcionamiento de la institucionalidad como la infraestructura.
Credenciales de Acceso	Se identifica al funcionario mediante su carnet el cual contiene información persona como foto, nombres y apellidos, Rh de igual forma la dependencia a la que pertenece	Se encarga de la identificación del usuario para el ingreso a las dependencias y a la información.
Dependencias	De acuerdo los trámites y servicios que brinda una entidad gubernamental como una Alcaldía se divide en dependencias: Despacho, Secretaría de Educación, Secretaría General, Secretaría de Gobierno, Secretaría de Hacienda, Secretaría de Infraestructura, Secretaría de Salud, Secretaría de Tránsito y Transporte, Secretaría del Deporte y la Cultura	Son unidades administrativas que se encargan de llevar trámites y procesos referentes al municipio de Popayán para cada una de estas unidades se contratan funcionarios a los cuales se les otorga una credencial única de acceso.
Sistema contra Incendios	Garantizar la existencia de extintores en todas las dependencias	Se encuentran ubicados estratégicamente en las diferentes dependencias
Sistema Perimetral	Garantiza un correcto aprovechamiento de la infraestructura y garantiza la integridad y confidencialidad de la información	El uso de seguridad perimetral permite detectar, disuadir y frenar una intrusión con mucha más antelación.
Mantenimiento Preventivo y correctivo	Esta área se ejecuta un plan anual de mantenimiento preventivo y correctivo.	Para realizar el mantenimiento preventivo y correctivo utilizan dos personas que son las encargadas de suplir estas necesidades
Copias de Seguridad Backup	Se establece un procedimiento del sistema de recuperación de desastres Backup.	Se ejecutan copias de seguridad a las bases de datos, al directorio activo, a las carpetas compartidas a algunos computadores que manejan información crítica almacenando estas en cintas magnéticas.
Observación, la Alcaldía de Popayán posee un grado de seguridad bajo en comparación a las necesidades actuales por lo que es necesario implementar una mejora en sus procesos de seguridad mediante una propuesta que brinde una buena práctica en cuanto al control de acceso a la información.		

Tabla 3. Seguridad en la Alcaldía de Popayán. Fuente: Propia

OBJETIVO ESPECÍFICO 2

4.2 OTRAS ALCALDÍAS EN COLOMBIA

El manejo de la seguridad informática dentro del contexto de empresa u organización es muy importante, ya que propone las herramientas necesarias para poder proteger la información. En este sentido, tiene como objetivo establecer medidas y estándares técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC´s [38] [39][40] [41][42] de la manera más segura en el uso de los servicios informáticos proporcionados por las oficinas de sistemas. A continuación, se presenta un cuadro comparativo correspondiente al manejo del control de acceso a los sistemas de información, relacionados con diferentes alcaldías del país (ver Tabla 4. Características Control de Acceso Alcaldías):

ALCALDÍA MAYOR DE BOGOTÁ	ALCALDÍA DE TUNJA	ALCALDÍA DE BUCARAMANGA	ALCALDIA DE YOTOCO	ALCALDIA DE IBAGUE
Existe una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.	Establecer controles para proteger la información contra accesos no autorizados	Fortalecerá el control de acceso a la información, sistemas y recursos de red	Garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.	Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles.
Se implantan controles para proteger la información contra violaciones de autenticidad	Se implantan controles para evitar la pérdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.	Permitir que cada rol identificado pueda acceder exclusivamente donde esté autorizado	Resguardará la información creada, procesada, transmitida o resguardada por sus procesos de entidad, Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información.	Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información
Establece que controles de acceso utilizar para el intercambio de información con terceros para reservar la integración de la información	Se establece una revisión de los derechos de acceso de usuarios	Restricción del acceso a la información a un ente no autorizado	No se otorgará cuentas a técnicos de mantenimiento externos, ni permitir su acceso remoto, a menos que la oficina de sistemas determine que es necesario	La información clasifica reservada confidencial sólo se debe transmitir por medios seguros.
Observaciones: La implementación del control de acceso por las alcaldías tiene como objetivo garantizar el correcto acceso y prevenir el no autorizado a la información donde se identifican las responsabilidades del usuario dentro de la organización				
Impedir el acceso no autorizado a los sistemas de información	Identifica que información considera clasificada o reservada para ser divulgada de conformidad al usuario autorizado	Negar el acceso a los recursos informáticos debido a cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave	El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.	Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles.
Los usuarios no deben proporcionar información a personal externo, acerca de los mecanismo de control de acceso a las instalaciones e infraestructura tecnológica de la Alcaldía Mayor de Bogotá	Impedir el acceso no autorizado a los sistemas de información, a la base de datos y servicios de información	Implementará control de acceso a la información, sistemas de información y recursos de red.	Salvaguardará la información de las amenazas originadas por parte del personal.	Se permite acceso a la información de uso única y exclusivamente durante la vigencia de derechos del usuario dentro de la organización
No se otorgará cuentas a técnicos de mantenimiento externos, ni permitir su acceso remoto, a menos que la oficina de sistemas determine que es necesario	El control de acceso es posterior a la autenticación y debe regular que el usuario acceda únicamente a los recursos a los cuales tenga derecho	El control de acceso a las aplicaciones no pueden ser accedidos de ninguna forma vía red, sino únicamente estando físicamente en ese lugar	Establece que controles de acceso utilizar para el intercambio de información con terceros para reservar la integración de la información	El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
Observaciones: Las entidades gubernamentales como las Alcaldías que albergan los activos tecnológicos de los Sistemas de Información, solicitan altas medidas de seguridad, que impidan acciones, malintencionadas o no, que puedan poner en peligro la información de la empresa.				

Tabla 4. Características Control de Acceso Alcaldías [38][39][40] [41][42]

OBJETIVO ESPECÍFICO 3

4.3 NORMATIVAS DE SEGURIDAD INFORMÁTICA

4.3.1 Normativas de Seguridad

Existen diferentes normativas de seguridad que las empresas u organizaciones implementan para salvaguardar la información, éstas persiguen el mismo objetivo de incluir a todas las unidades o departamentos que hacen parte de una estrategia de seguridad integral [2].

Las normativas de seguridad, tienen la finalidad de presentar los lineamientos necesarios para que las empresas puedan implantar un sistema de gestión de la seguridad de la información (SGSI) [2].

La implantación del Sistema de Gestión de la Seguridad de la Información, se realiza mediante un proceso ordenado que, consiste en establecer los mecanismos necesarios de seguridad de manera documentada y conocida por todos los miembros de la empresa; sin embargo, es importante que se tenga claro que la implantación de un SGSI no garantiza la protección de la información en su totalidad, ya que su propósito como lo manifiesta la ISO en su portal ISO27000 es, "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" [43].

Con relación a la ISO 27000, las normativas hacen referencia a [7] [43]:

- Normativas que inducen a las buenas prácticas para la seguridad de la información.
- Normativas que involucran la documentación que deben tener las empresas que deseen certificar su SGSI.

Las normas de seguridad se originan en el BSI (British Standards Institution). En la actualidad es una organización global de servicios a empresas en certificaciones de sistemas de gestión de seguridad, certificación de producto y normas, suministrando además formación e información sobre normas y comercio internacional [44].

BSI, es una organización con más de 100 años de experiencia en 66.000 organizaciones en 150 países. La evolución adquirida a lo largo de los años se muestra en la Tabla 6 [45]:

FECHA	ALCANCE
1993	Estructura del primer esquema del código prácticas de la seguridad de la información.
1995	Primera divulgación oficial del código de buenas practicas BS 7799:1.
1998	Especificaciones de los sistemas de gestión de la seguridad de la información del BS 7799:2.
2000	Primera versión de la normativa ISO/IEC 17799:2000 código de buenas prácticas
2002	Nueva versión de la BS 7799:2
	Código de buenas prácticas UNE-ISO/IEC 17799
2004	Especificaciones de los sistemas de gestión de la seguridad de la información
2005	Código de buenas prácticas ISO 17799:2005.
	Especificaciones de los sistemas de gestión de la seguridad de la información ISO 27001
2006	Gestión del riesgo de los sistemas de información BS 7799-3:2006
2013	Segunda versión de Especificaciones de los sistemas de gestión de la seguridad de la información ISO 27001.2013

Tabla 5. Trascendencia de las normativas: Fuente [2]**.**

De acuerdo a lo planteado anteriormente, existieron diferentes normativas a través del tiempo en sistemas de gestión de seguridad de la Información. Actualmente la norma de certificación internacional es la ISO/IEC 27001:2013 bajo los esquemas nacionales de cada país [1].

4.3.2 Estado de normativas de seguridad de la información en Colombia

En Colombia hay empresas que en la actualidad se encuentran certificadas en la normatividad internacional auditable ISO/IEC 27001:2013 las cuales son [46]:

4.3.2.1 ICONTEC (Instituto Colombiano de Normas Técnicas y certificación)

Fue fundado el 10 de mayo como el Instituto Colombiano de Normas Técnicas, por un grupo de 18 empresarios y directivos gremiales, estos vieron la necesidad de crear una organización que trabajara el tema de las normas técnicas, para mejorar la productividad y la competitividad de la industria nacional. ICONTEC, es representante por Colombia ante los organismos de normalizaciones internacionales y regionales como la ISO, IEC (international Electrotechinical commission), COPANT (comisión Panamericana de Normas Técnicas), entre otras. A su vez esta organización nacional provee el servicio de consultas de contenido de las normas técnicas colombianas e internacionales. Además, presenta ante Colombia un compendio de normativas para el SGSI. Como Organismo Nacional de Normalización, son miembro activo de los más importantes organismos internacionales y regionales de normalización, lo que nos permite participar en la definición y el desarrollo de normas internacionales y regionales para estar a la vanguardia en información y tecnología [47].

4.3.2.2 ISACA

Comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares (para auditar controles en los sistemas computacionales con importancia crítica en las operaciones de sus respectivas organizaciones), se sentaron a discutir la necesidad de tener una fuente centralizada de información y guías en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación creó una fundación de educación para llevar a cabo proyectos de investigación de gran escala, para expandir los conocimientos y el valor en el campo de gobierno y control de TI. Con más de 110,000 integrantes (miembros de la Asociación y aquellos que no son miembros pero ostentan una o más certificaciones de ISACA) en 180 países, ISACA ayuda a empresas y líderes de TI a maximizar el valor y gestionar riesgos relacionados con la información y la tecnología [48].

Fundada en 1969, ISACA, es una organización independiente, sin ánimo de lucro, que representa los intereses de los profesionales relacionados con la seguridad de la información, aseguramiento, gestión de riesgos y gobierno de TI. Estos profesionales confían en ISACA como fuente segura de conocimiento sobre la información y la tecnología, la comunidad, estándares y certificaciones. La asociación, que tiene 200 capítulos en todo el mundo, promueve el avance y certificación de habilidades y conocimientos críticos para el negocio, a través de certificaciones globalmente respetadas: Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) y Certified in Risk and Information Systems Control™ (CRISC™)". ISACA también desarrolló y continuamente actualiza a COBIT®, un marco de referencia que ayuda a empresas de todas las industrias y geografías, a gobernar y gestionar su información y tecnología [48].

4.3.2.3 COBIT (Control Objectives for Information and Related Technology)

Suministra un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TIC corporativas (tecnologías de la información y comunicación) [49].

Permite además entender como dirigir y gestionar el uso de tales sistemas, así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como empresas sin ánimo de lucro o del sector público [49].

ICONTEC	ISACA	COBIT
Las actividades que deben cumplir las organizaciones en sus procesos deben conocer los atributos de los controles a aplicar, las responsabilidades y roles de las partes involucradas para poder establecer un estado actual.	Cumplimiento de los requisitos legales para brindar confiabilidad confidencialidad, integridad, disponibilidad en los sistemas de información.	Las organizaciones que utilizan Cobit, como controles de aplicaciones, deben brindan información confiable para realizar procesos de manera íntegra en los sistemas de información.
Establece las actividades necesarias para la identificación, almacenamiento, conservación, recuperación, retención y la disposición de accesos a la información.	Las organizaciones deben asegurarse de que existen suficientes controles para mitigar los riesgos relacionados con el manejo de información. Y estar operando con la efectividad necesaria para proveer información confiable.	Implantar controles para la identificación de los accesos externos que afectan al SGSI, con el fin de disponer de la información de manera adecuada.
Manuales de funcionamiento, directrices y demás documentos que se relacionen con el manejo de información almacenada en los sistemas de información.	Los controles serán seleccionados e implementados de acuerdo a los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo.	Identificar los objetivos de control, evaluar los riesgos y determinar la suficiencia de los controles de aplicación mediante el cumplimiento de derechos y obligaciones de cualquiera de los involucrados en la organización
Documentación de control de accesos y seguridad perimetral general, áreas de acceso a zonas públicas, internas y restringidas, documentación de acceso a sistemas de información.	Clasificación de la información mediante guías de clasificación y denominación, identificación y tratamiento de acceso a la información.	El desarrollo e implantación de los controles de aplicación, son en concordancia con los requerimientos definidos por la organización a la hora de implantar los controles.

Tabla 6. Normativas de Seguridad. Fuente: Propia

4.3.3 Dominio de control de acceso ISO/IEC 27002:2013

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática [1].

Para impedir el acceso no autorizado a los sistemas de información se debe implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento [1].

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso [1].

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por

el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

4.3.3.1 Objetivos de control de acceso ISO/IEC 27002:2013

- Controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.
- Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.
- Hacer que los usuarios sean responsables de la protección de la información para su identificación.
- Impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

4.3.3.2 Requisitos necesarios para el control de acceso ISO/IEC 27002:2013

9.1.1 Política de control de accesos.

9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.

9.2.1 Gestión de altas/bajas en el registro de usuarios.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales.

9.2.4 Gestión de información confidencial de autenticación de usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.

9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión.

9.4.3 Gestión de contraseñas de usuario.

9.4.4 Uso de herramientas de administración de sistemas.

9.4.5 Control de acceso al código fuente de los programas

OBJETIVO ESPECÍFICO 4

4.4 ESTÁNDAR DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.4.1 Estructura ISO/IEC 27001:2013

La norma ISO 27001:2013 ofrece especificaciones para un SGSI. Fue publicada el 15 de Octubre de 2005, la cual contiene los requisitos y/o especificaciones del sistema de Gestión de la seguridad de la información. Procedente de la BS 7799-2:2002, e identificada actualmente como la norma ISO 27001:2013. Esta norma es certificable en la actualidad por los auditores externos de los SGSI de las diferentes empresas acreditadas por la ISO. En esta norma se enumera de forma resumida, los objetivos de control, para que sean seleccionadas por las empresas u organizaciones que desean implantar el SGSI. No es de carácter obligatorio que se implementen todos los controles de esta norma, la empresa debe justificar ante los auditores la no aplicabilidad de los controles cuando estén en el proceso de evaluación para una certificación [11].

En Colombia, a través de El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) se pueden adquirir las normas en el idioma Español. El original en versión en inglés y la traducción al francés pueden adquirirse en el sitio oficial de la ISO. Actualmente, este estándar se encuentra en revisión y su actualización por el subcomité ISO SC27, fue publicada en su segunda edición en Mayo de 2013 [50].

La normativa ISO/IEC 27002:2013, se estipulan 18 dominios, 35 objetivos y 114 controles de seguridad. Cada dominio estipula un capítulo de la norma especificando en forma detallada los controles a los que pertenece cada dominio y su funcionalidad [2].

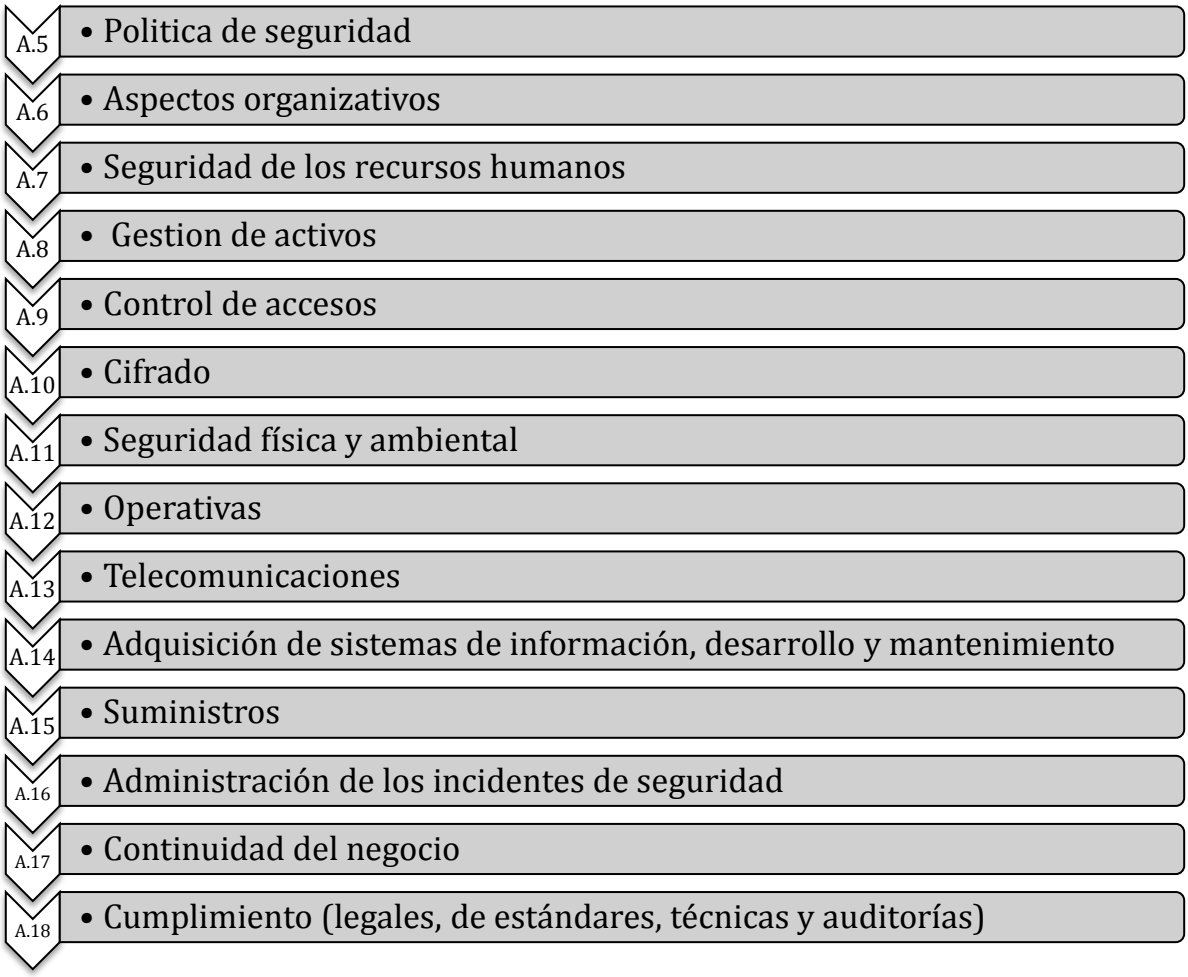


Figura 3. Dominios de Seguridad. Fuente: Norma ISO 27002:2013

A continuación se describe más detalladamente, cada uno de los aspectos del dominio de seguridad, teniendo en cuenta las especificaciones de la norma con respecto a los controles:

4.4.2 A.5. Política de seguridad

En este dominio se explica la elaboración de un documento de política de seguridad, el cual debe ser realizado por el equipo de trabajo que la organización designa para la implementación del SGSI [1][2].

En el documento de política de seguridad, se debe especificar toda la normativa interna de la institución con el objetivo de que los funcionarios conozcan y cumplan las medidas de seguridad implantadas a través del (SGSI). Así mismo, contempla todos los aspectos orientados al acceso a la información, utilización de los activos físicos y lógicos de la organización y el comportamiento que deben

tener en caso de que ocurra un incidente de seguridad. La elaboración del documento debe ser con un lenguaje claro y sencillo con el objetivo de que cualquier funcionario de la empresa u organización lo pueda interpretar [1][2].

Las actividades que genera el dominio son las siguientes:

A.5.1.1 Políticas para la seguridad de la información: se publica un documento donde se mencionan las actividades a implementar en seguridad de la información.

A.5.1.2 Revisión de la política de seguridad de la información: se efectúan revisiones para garantizar que es adecuada, eficaz y suficiente.

4.4.3 A.6. Aspectos organizativos para la seguridad

En este aspecto se establece la administración de la seguridad de la información como parte primordial de las actividades de una organización, se implantan los parámetros de organización interna y dispositivos para la movilidad y teletrabajo de la organización. La organización interna hace referencia al compromiso que la dirección asume para el establecimiento del SGSI, la designación del equipo de personal que incluye el coordinador de seguridad y la asignación de responsabilidades, entre otros. Los dispositivos para la movilidad y teletrabajo hacen referencia a los riesgos relacionados con trabajar en entornos desprotegidos aplicar la protección conveniente. Los controles se relacionan a continuación [1] [2].

A.6.1 Interna

A.6.1.1 Compromiso de la Dirección con la seguridad de la información: Deben respaldar las iniciativas de seguridad demostrando su apoyo y compromiso.

A.6.1.2 Segregación de tareas: se coordinan las actividades necesarias para organizar información valiosa por puesto y funcionario con el fin de reducir las oportunidades de modificación o mal uso de la información.

A.6.1.3 Contacto con las autoridades: mantener contacto con las autoridades pertinentes en respuesta a incidentes de seguridad de la información.

A.6.1.4 Contacto con grupos de interés especial: tener a disposición contactos con grupos especializados o empresas en temas de seguridad de la información.

A.6.1.5 Seguridad de la información en gestión de proyectos: gestión de la seguridad de la información y su implantación como son controles, políticas, procesos y procedimientos de seguridad.

A.6.2 Dispositivos para movilidad y teletrabajo

A.6.2.1 Política de uso de dispositivos para movilidad: se debe implementar una política formal donde se adoptaran medidas para proteger la información de los riesgos derivados de la informática móvil y las telecomunicaciones.
A.6.2.2 Tratamiento de la seguridad en la relación con los clientes: Identificar los requisitos identificados de seguridad antes de dar acceso a los clientes a información o activos de la organización.

4.4.4 A.7 Seguridad ligada a los recursos humanos

Este dominio hace énfasis en todo el talento humano de la organización y demás personal contratado de manera externa, quien debe conocer las responsabilidades que adquieren para proteger la información, garantizar la seguridad y buen uso, así como mantener la confidencialidad de la información que tienen acceso. La organización debe realizar verificación jurídica al personal antes de ser contratado y establecer las debidas cláusulas contractuales para el cumplimiento de sus funciones, responsabilidades que tiene sobre los activos que utilizará, entre otros. También deberá definir los procedimientos que se deben aplicar cuando un empleado tenga cambio de funciones o cambio de cargo o haya sido retirado de la empresa por diferentes motivos [1] [2].

A.7.1 Antes de la contratación: asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen [2].

A.7.1.1 Investigación de antecedentes: realizar revisiones de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos de la organización [2].

A.7.1.2 Términos y condiciones de contratación: los empleados, contratistas y terceros deberán aceptar y firmar los términos y condiciones del contrato de empleo donde se establecerán sus obligaciones dentro de la organización y de ella para la seguridad de la información [2].

A.7.2 Durante la contratación: asegurar que los empleados, contratistas y terceras partes son consciente de las amenazas de seguridad de sus responsabilidades y obligaciones dentro de la organización [2].

A.7.2.1 Responsabilidades de la gestión: la dirección debe requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad con las políticas y los procedimientos establecidos de la organización [2].

A.7.2.2 Concienciación, educación y capacitación en seguridad de la información: todos los empleados de la organización recibirán entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales[2].

A.7.2.3 Proceso disciplinario: debe existir un proceso formal disciplinario para empleados que produzcan problemas en la seguridad [2].

A.7.3 Cese del empleo o cambio de puesto de trabajo: establecer las responsabilidades para asegurar que el abandono de la organización, por parte de los empleados, contratistas o terceras personas, se controla, se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso [1] [2].

A.7.3.1 Retirada de los derechos de acceso: retirar los derechos de acceso para todos los empleados, contratistas o terceros, de la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisada en caso de cambio [1] [2].

4.4.5 A.8 Gestión de activos

Se denomina activo en seguridad de la información, como la adquisición que la empresa u organización debe proteger contra las diferentes amenazas a las que puede estar expuesta. La generación, ubicación y salvaguardar la información depende de otros activos de la empresa, los cuales se dividen en diferentes grupos: Hardware, software o aplicación, red, equipamiento auxiliar, instalación, servicios y de persona [1] [2].

A.8.1 Responsabilidad sobre los activos: conservar una protección adecuada de los activos de la organización [1] [2].

A.8.1.1 Inventario de activos: deben estar identificados todos los activos que hacen parte del manejo de información [2].

A.8.1.2 Propiedad de los activos: toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la organización [2].

A.8.1.3 Uso aceptable de los activos: identifica y documenta las regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información [2].

A.8.1.4 Devolución de activos: los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión o bajo su responsabilidad una vez finalice su contrato de prestación de servicios o actividades similares relacionadas con su contrato de empleo [2].

A.8.2 Clasificación de la información: clasificar la información para indicar las necesidades, prioridades y el nivel de protección que necesiten [1] [2].

A.8.2.1 Directrices de clasificación: debe clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para el manejo de la información en la organización [2].

A.8.2.2 Etiquetado y manipulado de la información: implantar procedimientos para el etiquetado y tratamiento de la información, de acuerdo a la clasificación orientada por la organización [2].

A.8.2.3 Manipulación de activos: se debe desarrollar procedimientos documentados para la manipulación de los activos de acuerdo a la clasificación que se opere en la organización [2].

A.8.3 Manejo de los soportes de almacenamiento: establecer los procedimientos operativos adecuados para la protección de documentos medios informáticos [1] [2].

A.8.3.1 Gestión de soportes extraíbles: debe clasificarse la gestión de los medios informáticos removibles con el esquema establecido por la organización [1].

A.8.3.2 Eliminación de soportes: se deberá eliminar de forma segura y sin riesgo los medios requeridos cuando se establezca un procedimiento formal de eliminación [1].

A.8.3.3 Soportes físicos en tránsito: proteger los medios que contienen información contra accesos no autorizados, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización [1].

4.4.6 A.9 Control de Accesos

Este dominio abarca uno de los controles más importantes en el SGSI, como lo es el acceso a la información. Producto de la razón social de la empresa (aplicaciones, infraestructura tecnológica y comunicación, etcétera), debe ser protegido a través de controles de acceso físico y lógico en la empresa. En este sentido se enmarca todos los criterios de control de acceso los cuales se enuncian a continuación [1] [2]:

A.9.1 Requisitos de negocio para el control de acceso: se debe controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la organización [1] [2].

A.9.1.1 Política de control de acceso: establecer, documentar y revisar una política de control de accesos con base a las necesidades de seguridad y de negocio de la organización [1] [2].

A.9.1.2 Control de acceso a las redes y servicios asociados: se deberá proveer a los usuarios de los accesos a redes y servicios de red para los que han sido seleccionados y verificados según su funcionamiento en la organización [1] [2].

A.9.2 Gestión de acceso de usuario: garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información [1] [2].

A.9.2.1 Gestión de altas/bajas en el registro de usuarios: debe existir un procedimiento de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información [1] [2].

A.9.2.2 Gestión de los derechos de acceso asignados a usuarios**:** debe existir un proceso formal de distribución de accesos a los usuarios para asignar o restringir derechos de accesos a todos los tipos de usuarios y para todos los sistemas y servicios [1] [2].

A.9.2.3 Gestión de los derechos de acceso con privilegios especiales: restringir y controlar la asignación y uso de los privilegios de acceso a la información [1] [2].

A.9.2.3 Gestión de contraseñas de usuario: controlar la asignación de contraseñas mediante un proceso de asignación de contraseñas [1] [2].

A.9.2.4 Gestión de información confidencial de autenticación de usuarios: la asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado [1] [2].

A.9.2.5 Revisión de los derechos de acceso de los usuarios: los propietarios de los activos de información deben revisar con regularidad los derechos de acceso de los usuarios[1] [2].

A.9.2.6 Retirada o adaptación de los derechos de acceso: se deberá eliminar los derechos de acceso para todos los empleados, contratistas, contratistas o terceros a la información y a las instalaciones de procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio[1] [2].

A.9.3 Responsabilidades de usuario: impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información [1] [2].

A.9.3.1 Uso de información confidencial para la autenticación: exigir a los usuarios el uso de las buenas prácticas de seguridad en el uso de información confidencial para la autenticación [1] [2].

A.9.4 Control de acceso a sistemas y aplicaciones: en este grupo, los dos controles que posee están dirigidos a prevenir el acceso no autorizado a la información mantenida en las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y a su vez el aislamiento de los sistemas sensibles del resto de la infraestructura. Este último proceder es muy común en sistemas críticos (salas de terapia intensiva, centrales nucleares, servidores primarios de claves, sistemas de aeropuertos, militares, etcétera), los cuales no pueden ser de acceso de ninguna forma vía red, sino únicamente estando físicamente en ese lugar [1] [2].

Por lo tanto, si se posee alguna aplicación que entre en estas consideraciones, debe ser evaluada la necesidad de mantenerla o no en red con el resto de la infraestructura [2].

A.9.4.1 Restricción del acceso a la información: se debe restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones [1].

A.9.4.2 Procedimientos seguros de inicio de sesión: cuando sea requerido por la política de control de acceso elaborado por la dirección de la organización u oficina de sistemas se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de identificación del usuario [1].

A.9.4.3 Gestión de contraseñas de usuario: controlar la asignación de contraseñas mediante un proceso de asignación de contraseñas [1].

A.9.4.4 Uso de herramientas de administración de sistemas: el uso de software que podrían llegar a anular o evitar controles en aplicaciones y sistemas deberán estar restringidos y estrechamente controlados [1].

A.9.4.5 Control de acceso al código fuente de los programas: debe restringir el acceso al código fuente de las aplicaciones software [2].

A.9.5 Ordenadores portátiles y teletrabajo: garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

A.9.5.1 Ordenadores portátiles y comunicaciones móviles: establecer una política donde se adoptarán las medidas de seguridad adecuadas para la protección

contra los riesgos, derivados del uso de los recursos de informática móvil y las telecomunicaciones.

4.4.7 A.10 Cifrado

El objetivo de este dominio es determinar la seguridad necesaria para la protección de la información mediante técnicas criptográficas con el fin de asegurar la confidencialidad, autenticidad o integridad de la información.

A.10.1 Controles Criptográficos

Es necesario utilizar controles criptográficos para la protección de la claves de acceso a sistemas, datos y servicios, de ser necesario se debe solicitar asesoramiento legal para establecer acuerdos con las firmas digitales que proporcionan protección [1].

A.10.1.1 Política de uso de los controles criptográficos: desarrollar una política donde se regularice el uso de los controles criptográficos para la protección de la información [1].

A.10.1.2 Gestión de claves: implementar una política donde se establezca el uso, la protección y el ciclo de vida de las claves criptográficas [1].

4.4.8 A.11 Seguridad física y ambiental

Este dominio incluye toda la seguridad en el sitio físico donde se encuentren ubicados los equipos informáticos y la información de la empresa, al igual que el entorno, es decir, toda el área perimetral de la organización. En esta parte se estipula el control de acceso a las oficinas o espacios de la edificación organizacional por el mismo personal de la institución y por personal externo. Protección contra incidentes naturales y/o industriales (inundaciones, fuego, humedad, etcétera [1] [2].)

A.11.1 Áreas seguras: evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización [1] [2].

A.11.1.1 Perímetro de seguridad física: perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.

A.11.1.2 Controles físicos de entrada: áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado [1] [2].

A.11.1.3 Seguridad de oficinas, despachos e instalaciones: se debe asignar y aplicar la seguridad física para oficinas, despachos y recursos [1] [2].

A.11.1.4 Protección contra las amenazas externas y ambientales: designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano [1] [2].

A.11.1.5 Trabajo en Áreas seguras: se deberá diseñar y aplicar protección física y pautas para trabajar en las áreas seguras [1] [2].

A.11.1.6 Áreas de acceso público y de carga y descarga: controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados [1] [2].

A.11.2 Seguridad de los equipos: la protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo [1] [2].

A.11.2.1 Emplazamiento y protección de equipos: Los equipos se deberían ubicar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado [2] [1]..

A.11.2.2 Instalaciones de suministro: Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo [2] [1].

A.11.2.3 Seguridad del cableado: Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños [1] [2].

A.11.2.4 Mantenimiento de los equipos: Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas [2] [1].

A.11.2.5 Salida de activos fuera de las dependencias de la empresa: Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización [2].

A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones: Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos [2].

A.11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento: Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización [1] [2].

A.11.2.8 Equipo informático de usuario desatendido: Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada [1] [2].

A.11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla: Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información [1] [2].

4.4.9 A.12. Administración de las comunicaciones y operaciones

En este dominio se acuerda la documentación, los procedimientos para la operación, administración y configuración del sistema de comunicaciones de la organización. En tal sentido, se debe garantizar la separación de los recursos en desarrollo, prueba y operación de los sistemas de información manejados por la organización. Hay que definir y establecer claramente los acuerdos sobre las provisiones y servicios que sean necesarios contratar por terceros. Además, se deben gestionar las capacidades de los sistemas para garantizar la protección contra código malicioso, código descargado por clientes, copias de seguridad, entre otros. Estipular los controles de seguridad para el intercambio de la información a través de las redes de comunicaciones, garantizar la seguridad en el comercio electrónico en caso de que la empresa lo contemple, revisiones y monitorización del mismo, entre otros [1] [13].

A.12.1 Responsabilidades y procedimientos de operación: se encarga de la operación correcta y segura de los recursos de tratamiento de información[1] [13].

A.12.1.1 Documentación de los procedimientos de operación: documentar los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten [1] [13].

A.12.1.2 Gestión de cambios: controlar los cambios en los sistemas y en los recursos de tratamiento de la información [1] [13].

A.12.1.3 Gestión de capacidades: Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas [13].

A.12.1.4 Separación de entornos de desarrollo, prueba y producción: Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional [13].

A.12.2 Protección contra código malicioso y descargable: precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados, protegiendo la integridad del software y hardware [13].

A.12.2.1 Controles contra el código malicioso: implantar controles de detección, prevención y recuperación contra el software malicioso [13].

A.12.3 Copias de seguridad: mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación [13].

A.12.5.1 Copias de seguridad de la información: hacer regularmente copias de seguridad de toda la información esencial del negocio y del software en relación a una política de respaldo (backup) [13].

A.12.2 Gestión de la provisión de servicios por terceros: mantener un nivel apropiado de seguridad de la información y de la prestación del servicio por terceros [1] [2].

A.12.2.1 Provisión de servicios: garantizar que los controles de seguridad y definiciones de servicio sean implementados, operados y mantenidos por los proveedores [1].

A.12.2.2 Supervisión y revisión de los servicios prestados por terceros: servicios, informes y registros suministrados por terceros deben ser monitoreados y revisados regularmente [1].

A.12.2.3 Gestión de cambios en los servicios prestados por terceros: Se debe gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información [1] [2].

A.12.3 Planificación y aceptación del sistema: requiere una planificación y preparación avanzada para minimizar el riesgo de fallos en los sistemas [1] [2].

A.12.3.1 Gestión de capacidades: monitorear el uso de recursos para asegurar el funcionamiento requerido del sistema [1] [2].

A.12.3.2 Aceptación del sistema: establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas [1] [2].

A.12.4 Registro de actividad y supervisión: detectar actividades de procesamiento de la información no autorizadas [1] [2].

A.12.4.1 Registro y gestión de eventos de actividad: mantener durante un periodo establecido los registros de auditoria con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información [1] [2].

A.12.4.2 Protección de los registros de información: proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados [1] [2].

A.12.4.3 Registros de actividad del administrador y operador del sistema: registrar las actividades del administrador y de los operadores del sistema con los registros asociados donde se deberá revisar de manera regular [1] [2].

A.12.4.4 Sincronización del reloj: sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad [1] [2]..

A.12.5 Control de software en explotación: minimizar los riesgos de alteración de los sistemas de información mediante controles de cambios imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones asignadas por la organización [1] [2]..

A.12.5.1 Instalación del software en sistemas en producción: deberán implementar procedimientos para controlar la instalación de software en sistemas operacionales [1] [2].

A.12.6 Gestión de la vulnerabilidad técnica: implementar los cambios en sistemas de prueba y/o de manera escalonada empezando por los sistemas menos críticos además de aplicar medidas de copias de seguridad y puntos de restauración junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías [1] [2].

A.12.6.1 Gestión de las vulnerabilidades técnicas: deberá obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados [1].

A.12.6.2 Restricciones en la instalación de software: establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios [2].

A.12.7 Consideraciones de las auditorías de los sistemas de información: durante las auditorias se debe maximizar la efectividad en el proceso de los sistemas de información y minimizar las intromisiones que se puedan presentar en el proceso y así poder llevar a cabo las verificaciones necesarias en el proceso de auditoría [1].

A.12.7.1 Controles de auditoría de los sistemas de información: planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados [2].

4.4.10 A.13. Seguridad en las telecomunicaciones

El objetivo de este dominio es garantizar la seguridad de la información que se comunica por las redes que abarca una organización, requiere de un estudio cuidadoso donde se considere el flujo de datos, implicaciones legales, monitoreo y protección [1] [2].

A.13.1 Gestión de la seguridad en las redes: el acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan [13]:

a) Que existen interfaces adecuadas entre la red de la organización y las redes públicas o privadas de otras organizaciones [1] [2].

b) Que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos [1] [2].

c) El cumplimiento del control de los accesos de los usuarios a los servicios de información [1] [2].

A.13.1.1 Controles de red: administrar y controlar las redes para proteger la información en sistemas y aplicaciones [1] [2].

A.13.1.2 Mecanismos de seguridad asociados a servicios en red: identificar e incluir en los acuerdos de servicio los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red [1] [2].

13.1.3 Segregación de redes: segregar las redes en función de los grupos de servicios, usuarios y sistemas de información [1] [2].

A.13.2 Intercambio de información con partes externas: realizar los intercambios sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente [1] [2].

A.13.2.1 Políticas y procedimientos de intercambio de información: deberá existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación pertenecientes a la organización [1] [2].

A.13.2.2 Acuerdos de intercambio: los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas [1] [2].

A.13.2.3 Mensajería electrónica: se debería proteger adecuadamente la información referida en la mensajería electrónica [1] [2].

A.13.2.4 Acuerdos de confidencialidad y secreto: identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información [1] [2].

4.4.11 A.14 Adquisición de desarrollo y mantenimiento de los sistemas de información

En este dominio se detallan todas las pautas para garantizar la adquisición de hardware y software seguro, así como el desarrollo de software a la medida ejecutado por la organización, realizar las pruebas necesarias para ajustar y mejorar las debilidades en seguridad de los Sistemas de información, al mismo tiempo que la validación [2] [1].

A.14.1 Requisitos de seguridad de los sistemas de información: garantizar que la seguridad es parte integral de los sistemas de información [1] [2] [8].

A.14.1.1 Análisis y especificación de los requisitos de seguridad: los nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes, deberían especificar los requisitos de los controles de seguridad [1] [2].

A.14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas: la información de los servicios de aplicación que pasan a través de redes públicas se deberían proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada [2].

A.14.1.3 Protección de las transacciones por redes telemáticas: la transacción de información de servicios de aplicación se debería proteger para evitar la

transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción [2].

A.14.2 Seguridad en los procesos de desarrollo y soporte: mantener la seguridad del software del sistema de aplicaciones y la información [1].

A.14.2.1 Política de desarrollo seguro de software: se debe controlar la implantación de cambios mediante procedimientos que cambios se hicieron [1] [2].

A.14.2.2 Procedimientos de control de cambios en los sistemas: el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios [1] [2].

A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo: las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización [1] [2].

A.14.2.4 Restricciones a los cambios en los paquetes de software: evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente [1] [2].

A.14.2.5 Uso de principios de ingeniería en protección de sistemas: se debe establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información [1] [2].

A.14.2.6 Seguridad en entornos de desarrollo: las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema [1] [2]..

A.14.2.7 Externalización del desarrollo de software: la organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado [1] [2].

A.14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas: realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo [1] [2].

A.14.2.9 Pruebas de aceptación: se establecen programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones [1] [2].

A.14.3 Datos de prueba: garantizar la seguridad de los sistemas de archivos para proteger los datos sensibles en entornos de prueba [1] [2].

A.14.3.1 Protección de los datos utilizados en prueba: los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar [1] [2].
.

4.4.12 A.15. Suministradores

En este dominio se plantea implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea donde la organización debe revisar los acuerdos y monitorear su cumplimiento para asegurar que los servicios sean entregados adecuadamente [1] [2].

A.15.1 Seguridad de la información en las relaciones con los suministradores: La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo [1] [2].

A.15.1.1 Política de seguridad de la información para suministradores: se debe acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas [1] [2].

A.15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores: establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización [1] [2].

A.15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones: los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones [1] [2].

A.15.2 Gestión de la prestación del servicio por suministradores: evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones [1] [2].

A.15.2.1 Supervisión y revisión de los servicios prestados por terceros: las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente [1] [2].

A.15.2.2 Gestión de cambios en los servicios prestados por terceros: Se deberá administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos [1] [2].

4.4.13 A.16. Gestión de incidentes de seguridad

En este dominio se plantean los procedimientos sistemáticos que la organización debe seguir, cuando se presente un incidente de seguridad, para aplicar las acciones correctivas, al mismo tiempo que el responsable de monitorear, dirigir y controlar la aplicación de dichos procedimientos [1] [2].

A.16.1 Gestión de incidentes de seguridad de la información y mejoras: garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información [2].

A.16.1.1 Responsabilidades y procedimientos: establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información [2].

A.16.1.2 Notificación de los eventos de seguridad de la información: comunicar lo más rápido posible los eventos en la seguridad de información mediante canales de gestión [2].

A.16.1.3 Notificación de puntos débiles de la seguridad: todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos [2].

A.16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones: Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes [2].

A.16.1.5 Respuesta a los incidentes de seguridad: Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados [2].

A.16.1.6 Aprendizaje de los incidentes de seguridad de la información: debe existir un mecanismo que permitan medir y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información [2].

A.16.1.7 Recopilación de evidencias: Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada conforme a las reglas para la evidencia establecidas en la jurisdicción correspondiente [2].

4.4.14 A.17. Administración de continuidad del negocio

En este dominio, se examina los planes que debe seguir la organización para mantener el servicio activo a los clientes, con el objetivo de que sea transparente para ellos. El plan que se diseñe, debe establecer los puntos críticos de la organización para protegerlos [2].

A.17.1 Continuidad de la seguridad de la información: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa [2].

A.17.1.1 Planificación de la continuidad de la seguridad de la información: la organización debe determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre [2].

A.17.1.2 Implantación de la continuidad de la seguridad de la información: la organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas [2].

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información: la organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas [2].

A.17.2 Redundancias: se debe considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la organización a través de arquitecturas sencillas típicas o los sistemas existentes se demuestren insuficientes [2].

A.17.2.1 Disponibilidad de instalaciones para el procesamiento de la información: implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad [2].

4.4.15 A.18. Cumplimiento (legales, de estándares, técnicas y auditorias)

El dominio contempla la reglamentación interna y externa de la organización sobre el cumplimiento de políticas establecidas, identificación de la legislación nacional e internacional aplicable a la organización [2].

A.18.1 Cumplimiento de los requisitos legales: evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad [2].

A.18.1.1 Identificación de la legislación aplicable: todos los requisitos de regulación u obligaciones contractuales deben ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información de la Organización [2].

A.18.1.2 Derechos de propiedad intelectual (DPI): implantar procedimientos que garanticen el cumplimento de la legislación, regulaciones y requisitos contractuales para el uso de productos software [2].

A.18.1.3 Protección de los registros de la organización: los registros se deben proteger de la pérdida, destrucción y falsificación [2].

A.18.1.4 Protección de datos y privacidad de la información personal: se garantiza la protección y privacidad de los datos y según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales [2].

A.18.1.5 Regulación de los controles criptográficos: utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes [2].

A.18.2 Revisiones de la seguridad de la información: realizar revisiones según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados [2].

A.18.2.1 Revisión independiente de la seguridad de la información: se debe revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización [2].

A.18.2.2 Cumplimiento de las políticas y normas de seguridad: Los directivos deben asegurar que los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad [1] [2].

A.18.2.3 Comprobación del cumplimiento técnico: se debe comprobar regularmente la conformidad de los sistemas de información con los estándares de implantación de la seguridad informática [2].

4.5 LEYES INFORMÁTICAS COLOMBIANAS

La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la *Ley de Delitos Informáticos*, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas [51].

En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penalmente sancionatorias de las violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano [51].:

En este sentido, el Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones [51].

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones: Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles [51].

4.5.1 Seguridad y Privacidad de la información Ministerio de las TIC

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente. La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad. El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL. Para el desarrollo del componente de seguridad y privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información [52].

4.6 ESTRATEGIAS PARA EL CONTROL DE ACCESO A LA INFORMACIÓN EN LA ALCALDÍA

Las estrategias que se presentan a continuación para realizar un control de acceso a los sistemas de información en la Alcaldía de Popayán es garantizar una gestión segura del acceso a la información mediante las técnicas establecidas por la ISO 27002:2013.

Para ello, se establecen 4 objetivos de control que definen la meta que se ha de alcanzar mediante la gestión de los accesos de usuario y la autorización de privilegios a los funcionarios que hacen parte de la Alcaldía de Popayán, a continuación se define la manera en que estos controles serán utilizados para garantizar un adecuado control de acceso a los sistemas de información [1].

4.6.1 Requerimientos para el control de acceso

Debe existir una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad en la cual se establece el nivel de riesgo de cada activo esto se hace con necesidad de informar a todo los miembros que hacen parte de la Alcaldía de Popayán [2].

Garantiza un compromiso ineludible de protección frente a una amplia gama de amenazas concientizando a los funcionarios de la Alcaldía de Popayán como la ciudadanía en común. Con la implementación de esta política de control de acceso se contribuye a minimizar los riesgos asociados de daño y se asegura el cumplimiento de las funciones de los usuarios en los sistemas de información [8].

Los objetivos que se establecen para el cumplimiento de la política de control de acceso son los siguientes:

- los funcionarios, contratistas, outsourcing o terceros, antes de solicitar acceso a los sistemas de información deben firmar un acuerdo de confidencialidad.
- Impedir el acceso no autorizado a los sistemas de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Las políticas de control de acceso deben ofrecer explicaciones comprensibles acerca del por qué deben tomarse decisiones sobre el acceso a la información, transmitir por qué son importantes estos u otros recursos o servicios de información, llevar un proceso de actualización periódica sujeto a los cambios organizacionales relevantes en la Alcaldía de Popayán, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de las dependencias, entre otras [1].

A.9.1.2 **Control de acceso a las redes y servicios asociados**
El proceso de servicio de tecnologías de comunicación e información utilizado por la oficina de sistemas de la Alcaldía de Popayán debe

cerciorar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la organización mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Se debe controlar las excepciones de acceso las cuales serán aprobadas por el jefe de la oficina de sistemas, según la necesidad del cargo y verificación previa de que las páginas solicitadas no contengan código malicioso con el visto bueno del encargado en seguridad de la información dando garantía del acceso en la red [1].

- Política de uso de los servicios en red: se debe mantener instalados y habilitados solo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la Alcaldía, controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en firewall proveer a los funcionarios los accesos a los servicios para los que han sido expresamente autorizados [1].

- Autenticación de usuario para conexiones externas: la autenticación de los usuarios remotos en otras conexiones deberá ser aprobada por el jefe de la oficina de sistemas [1].

- Identificación de equipos en las redes: todo los equipos pertenecientes a la Alcaldía de Popayán serán identificados en la red con el protocolo IP dinámica donde se monitorea y analiza los eventos de sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de red de manera no autorizada [1].

- Diagnóstico remoto y protección de los puertos de configuración: los puertos de configuración y diagnostico que pertenecen a la Alcaldía de Popayán son puertos físicos comúnmente llamados de consola o de administración y son aquellos puertos o interfaces que vienen en elementos de la red como switches, routers entre otros, los cuales permiten hacer la configuración mediante una contraseña de acceso lógico cuando se ingrese a los elementos de red por consola se debe controlar y solo el personal autorizado de la oficina de sistemas podrá entrar directamente a los puertos de configuración en caso de fallas en los equipos [1].

- Segregación de las redes: segregar los grupos de usuarios, servicios y sistemas de información en las redes mediante parametrización de los servicios red deberán estar separada por Vlans para garantizar la

confidencialidad de los datos que se trasmitan en la red de la Alcaldía de Popayán [1].

- Control de la conexión a la red: las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la Alcaldía de Popayán, se denegara a los funcionarios cualquier conexión en red según la política de control de accesos establecidos anteriormente y necesidad de uso de las aplicaciones de la Alcaldía de Popayán las excepciones de acceso las cuales serán aprobadas por el jefe de la oficina de sistemas, según la necesidad del cargo y verificación previa de que las redes no perjudiquen el funcionamiento de la entidad [1].

- Control de encaminamiento (routing) de red: se establecen controles de enrutamiento en las redes para asegurar que las conexiones de los computadores y flujos de información tengan rutas óptimas para él envió de paquetes de información por un camino u otro de esta manera no habrá un incumplimiento en las comunicaciones de red internas de la Alcaldía de Popayán [1] [25].

4.6.2 Gestión de acceso de usuario

Se deberá garantizar el acceso a los funcionarios, contratistas y terceros que tengan autorización de acceso a los sistemas de información donde se establecen procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Estos procedimientos deberán cumplir todas las etapas del ciclo de vida de acceso, como también el acceso debe estar compuesto por un ID o nombre de usuario y contraseña que debe ser único por cada servidor público o tercero. El registro inicial en los sistemas de información de los nuevos usuarios se debe dar hasta su baja o cuando ya no sea necesario su acceso a los sistemas y servicios de información pertenecientes a la Alcaldía de Popayán, eliminando todo registro existente sobre el usuario y sus permisos dentro de los sistemas a los cuales tenía acceso [1] [2].

A.9.2.1 Gestión de altas y bajas en el registro de usuarios Con el objetivo de impedir el acceso no autorizado a la información se implementaran documentación formal para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información [1] [2].

la oficina de sistemas de la Alcaldía de Popayán debe mantener un registro donde cada uno de los jefes de dependencias responsables de los procesos haya autorizado a los funcionarios o terceros el acceso a los

diferentes sistemas de información este procedimiento lo realizara el responsable encargado de la oficina de sistemas donde definirá un documento de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario el cual debe comprender [1] [2]:

- ✓ Utilizar identificadores de usuarios únicos, de modo que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo funcionario. El uso de identificadores grupales solo se debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.

- ✓ Comprobar que el usuario tiene autorización del propietario de la información en este caso el jefe de dependencia para el uso de sistema, base de datos o servicio de información [1].

- ✓ Verificar que el nivel de acceso otorgado es adecuado para el propósito de la ocupación del funcionario y es coherente con la política de seguridad de la Alcaldía de Popayán [1].

- ✓ Requerir que los funcionarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso [1].

- ✓ Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización [1].

- ✓ Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o de aquellos a los que se les revoco la autorización o se desvincularon de la Alcaldía de Popayán [1].

A.9.2.2 Gestión de los derechos de acceso asignados a usuarios: debe existir un proceso formal de distribución de accesos a los usuarios para asignar o restringir derechos de accesos a todos los tipos de usuarios y para todos los sistemas y servicios. Las cuentas de usuario (funcionarios, contratistas y terceros) creadas en los sistemas de información de la Alcaldía de Popayán deben tener un identificador único y deberán solicitarse mediante un requerimiento formal, especificando su identificación, nombres y apellidos y sus funciones que va a desempeñar y autorizado por el jefe inmediata en este caso el jefe de la dependencia. Las cuentas de los usuarios externos deben ser solicitadas y autorizadas a través del jefe de la oficina de sistemas de la Alcaldía de Popayán [1].

- Efectuar revisiones periódicas con el objeto de:
  -Cancelar cuentas de usuarios redundantes.
  -Inhabilitar cuentas inactivas por más de 60 días.
  -Eliminar cuentas inactivas por más de 120 días.
  -En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

A.9.2.3 Gestión de los derechos de acceso con privilegios especiales: se debe restringir y controlar la asignación y uso de los privilegios de acceso a la información y comunicaciones mediante los roles establecidos por la Alcaldía de Popayán sean funcionarios de planta o contratistas manteniendo los registros de las revisiones y hallazgos estos procesos deben estar establecidos por la oficina de sistemas de la siguiente manera [1][2]:

Se limitara y controlara la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas de información a los que ha accedido ilegalmente [1].

Los sistemas multiusuario que requieren protección contra accesos no autorizado, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal [1][2].

- ✓ Identificar los privilegios asociados a cada sistema de información, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las condiciones de personal a las cuales deben asignarse los privilegios de acceso donde debe estar establecido el vínculo con la Alcaldía.
- ✓ Asignar los privilegios a funcionarios sobre la base de la necesidad de uso y servicio por ejemplo el requerimiento mínimo para su rol funcional en los sistemas de información.
- ✓ Mantener un proceso de autorización y registro de todos los privilegios asignado a cada funcionario registrado.
- ✓ Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- ✓ Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los propietarios de información en este caso los jefes de dependencias serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación en la oficina de sistemas, lo cual será supervisado por el responsable de seguridad informática [1][2].

A.9.2.4 Gestión de información confidencial de autenticación de usuarios: la asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión de acceso controlado por la oficina de sistemas de la Alcaldía de Popayán donde se establecerá un acuerdo de confidencialidad con el funcionario, contratista o tercero de la información a la cual va ser asignado [1][2].

La asignación de la información se debe controlar por medio de un proceso de gestión formal donde habrá revisiones periódicas para cerciorar que la información no está siendo modificada [1][2].

A.9.2.5 Revisión de los derechos de acceso de usuario: con el fin de mantener un control eficaz en el acceso a los datos y servicios de información, la oficina de sistemas de la Alcaldía de Popayán, llevara a cabo un proceso donde se revisara los derechos de acceso de los usuarios y se contemplara los siguientes controles [1][2].

- Revisar los derechos de acceso de los usuarios en intervalos de 4 meses.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 2 meses.
- En caso de destitución o término de contrato se actualizarán los derechos de accesos en un plazo máximo de 3 días desde que se recibe la solicitud en la oficina de sistemas y posteriormente en los sistemas de información.
- Los encargados de la oficina de sistemas de la Alcaldía una vez avisado por la oficina de talento humano que se encarga de la gestión de funcionarios dentro de la organización, estos harán una revisión pertinente de los privilegios que este funcionario tendrá en los sistemas de información y adecuarlo a las necesidades que debe suplir.

A.9.2.6 Retiro o ajuste de los derechos de acceso: Para controlar el retiro o ajuste en la asignación de derechos de acceso de los funcionario, contratistas o terceros a los sistemas de información de la Alcaldía de Popayán se establece el retiro de acceso a la información donde se indica

la finalización del empleo, contrato o acuerdo, o en el caso de ser revisados o ajustados los derechos de acceso en caso de cambio. Los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su vínculo en la Alcaldía de Popayán [1][2].

4.6.3 Responsabilidades de usuario

El personal de la oficina de sistemas de la Alcaldía indica los procedimientos que deben seguir los funcionarios, contratistas y terceros para acceder a los sistemas de información de una manera adecuada y efectiva que no ponga en riesgo la integridad de la información. Comprobar el cumplimiento de los procedimientos establecidos, relacionados con el control de acceso, creación de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red y autenticación de usuarios [1][2].

A.9.3.1 Uso de información confidencial para la autenticación: Concientizar a los funcionarios sobre el uso apropiado de contraseñas y de equipos de trabajo logrando impedir el acceso de usuarios no autorizados y garantizar el compromiso de todo aquel que tenga acceso a la información independientemente de su jerarquía, siempre tendrá alguna responsabilidad a partir del momento que tenga acceso a la información y recursos para el tratamiento de la información, la cooperación de los funcionarios autorizados es esencial para una seguridad efectiva donde deben ser conscientes de sus responsabilidades dentro de la Alcaldía de Popayán [1][2].

Donde se debe contemplar:

- Definir documentación para la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de acceso a internet; el uso de computación móvil y la revisión de registros de actividades.
- Requerimientos de seguridad de cada una de las aplicaciones a las cuales puedan acceder de manera que se lleve un registro sobre el comportamiento del usuario en el sistema.
- Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo a su perfil de cargo en la Alcaldía de Popayán.
- Definir pautas de utilización de internet para todos los usuarios.

- Promover el desarrollo y uso adecuado de los sistemas de información para evitar la necesidad de sancionar a los funcionarios.
- Mantener contraseñas en secreto.

4.6.4 Control de acceso a las aplicaciones y a la información

En este grupo, los controles que posee están dirigidos a prevenir el acceso no autorizado a la información mantenida en los sistemas y aplicaciones que hacen parte de la Alcaldía de Popayán. Donde se establece en la política de control de acceso a información digital teniendo en cuenta los niveles de clasificación y manejo de la información según los niveles deberán gestionarse los accesos a los usuarios con [1][2]:

- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambiar la contraseña de acceso si tiene sospecha que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Seleccionar contraseñas que no sean fáciles de adivinar.

A.9.4.1 Restricción del acceso a la información: se debe restringir el acceso a la información a todas las personas que hagan parte de la Alcaldía de Popayán sean funcionarios y el personal de mantenimiento (pasantes) a la información y funciones de los sistemas de información al aislar estos accesos a los sistemas se prevé el intercambio seguro de información ya que no se permitiría duplicar información con otros sistemas solo los encargados de la oficina de sistemas de la alcaldía tendrá estos privilegios para manipula esta información sin perder su integridad [1].
A.9.4.2 Procedimientos seguros de inicio de sesión: debe controlarse el acceso al sistema y aplicaciones mediante procedimientos seguros de conexión y un inicio seguro de la sesión que tendrá las siguientes condiciones [1] [2]:

- No mostrar información correspondiente al sistema hasta que se haya cumplido el proceso de inicio.
- Limitar el número de intentos fallidos de conexión.
- No mostrar las contraseñas digitadas.

La política de control de acceso debe controlar el acceso a los sistemas y aplicaciones mediante un proceso de identificación de los usuarios

establecida en la oficina de sistemas donde se hace un procedimiento seguro de identificación del usuario en los sistemas y aplicaciones pertenecientes a la Alcaldía de Popayán [1][2].

A.9.4.3 Gestión de contraseñas de usuario: se exigirá a los funcionarios de la Alcaldía de Popayán el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas. La asignación de contraseñas de acceso deben cumplir ciertos requisitos como un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales para la conformación de estas [1][2].

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un funcionario en los sistemas de información de la Alcaldía de Popayán, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.
Los funcionarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas cumpliendo los siguientes lineamientos [1][2]:

- Mantener las contraseñas en secreto.
- Pedir el cambio de contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad de acuerdo a las prescripciones informadas por el responsable del activo de información de se trate, que:
  - Sean fáciles de recordar.
  - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombre, números de teléfono, fecha de nacimiento, etcétera.
  - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisionales en el primer inicio de sesión.
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas: perdida o indicio de pérdida de confidencialidad.
- Si los funcionarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificara a los mismos que pueden utilizar una única contraseña

para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas.

A.9.4.4 Uso de herramientas de administración de: Se estable dentro de la política de control de acceso a la información medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática por lo que se establece [1][2].

- Uso de un id de usuario y contraseña únicos para el acceso.
- Uso de software antivirus provisto por la oficina de sistemas.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por la oficina de sistemas.
- Realización de copias de seguridad periódicas establecidas por el procedimiento de backups de la oficina de sistemas.

A.9.4.5 Control de acceso al código fuente de los programas: En la política de control de acceso se establece que solo los funcionarios de la oficina de sistemas de la Alcaldía de Popayán tendrán acceso al código fuente de los programas y/o aplicaciones y además evitar amenazas que puedan poner en riego la funcionalidad de los sistemas de información [1][2].

.

CAPÍTULO 5. PROPUESTA PARA EL CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACION DE LA ALCALDIA DE POPAYAN

CAPÍTULO 5. PROPUESTA

5.1 PROPUESTA PARA EL CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA DE POPAYÁN

La información es el activo más importante de las organizaciones para la Alcaldía de Popayán no es excepción, a continuación se refleja una descripción de los procesos y responsabilidades que deben tener los funcionarios, contratistas y terceros sobre el acceso a los sistemas de información de la Alcaldía de Popayán.

El objetivo de esta propuesta es brindar las recomendaciones mínimas y básicas que debe incorporar cada uno de los usuarios en sus labores y actividades que desarrolla en los sistemas de información, con el fin de asegurar y salvaguardar la información institucional de un acceso no autorizado.

El establecimiento, seguimiento y mejora continua de los controles de acceso a los sistemas de información de la Alcaldía de Popayán tiene como finalidad proteger los recursos informáticos de la entidad y la tecnología utilizada para su normal funcionamiento como organización frente amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Con la implementación de las estrategias de control de acceso se contribuye a minimizar los riesgos asociados de daño y se asegura el cumplimiento de las funciones de los usuarios en los sistemas de información.

Los objetivos que se establecen para el cumplimiento del control de acceso a los sistemas de información son los siguientes:

- Controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.

- Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.
- hacer que los usuarios sean responsables de la protección de la información para su identificación.
- impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

5.1.1 Metodología Magerit

La metodología que se utilizó para el análisis y gestión de riesgos fue Magerit elaborada por el Consejo Superior de Administración Electrónica de España. Esta metodología utiliza como base la norma ISO/IEC 27002:2013 y contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información. A continuación se relacionan los pasos que se deben contemplar en un proceso de análisis de riesgos, teniendo en cuenta un orden general que permita concluir el riesgo actual en que se encuentra la Alcaldía de Popayán en especial al control de acceso a los sistemas de información [3].

PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es un software diseñado para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit [53].

5.1.1.1 Paso 1: Identificación de Activos

Los activos son los elementos que una organización utiliza para el manejo de la información (hardware, software, recurso humano) [12]. Los activos se diferencian agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. A la hora de realizar el análisis de riesgo el primer paso es identificar los activos que existen en la organización y determinar el tipo. En la siguiente tabla se relacionan los tipos de activos pertenecientes a la Alcaldía de Popayán [3].

TIPOS DE ACTIVOS	DESCRIPCION
Activo de información	Bases de datos, documentación (manuales de usuario, contratos, normativas, etcétera)
Software o Aplicación	Sistemas de información, herramientas de desarrollo, aplicativos desarrollados y en desarrollo, sistemas operativos, aplicaciones de servidores etcétera.
Hardware	Equipos de oficina(PC, portátiles, servidores, dispositivos, móviles)

Red	Dispositivos de conectividad de redes (router, swicth, concentradores y otros)
Equipamiento auxiliar	UPS
Instalación	Cableado estructurado, instalaciones eléctricas
Servicios	Conectividad a internet, servicios de mantenimiento, etcétera.
Personal	Personal Informático(administradores, web master, desarrolladores, etcétera)

Tabla 7: Inventario Activos. Fuente: Magerit

Los encargados de los activos de información que son los directivos de la Alcaldía en este caso los jefes de dependencias deben tener la capacidad para definir o aprobar las reglas de control de acceso y otros controles de seguridad aceptando formalmente sus responsabilidades dentro de la organización para aplicar las medidas de control de acceso definidas por las aplicaciones y sistemas de información establecidas por la oficina de sistemas de la Alcaldía realizando sus tareas lo más eficientemente posibles [3].

En la clasificación de estos activos se clasifican en:

ACTIVOS ESENCIALES	SERVICIOS INTERNOS	EQUIPAMIENTO INFORMÁTICO	EL ENTORNO
Información que se maneja dentro de las dependencias. Servicios prestados por los sistemas de información.	Qué orden llevan para organizar la información almacenada en los sistemas de información.	Equipos informáticos (hardware) comunicaciones Soportes de información: discos, cintas.	Equipamiento y suministros: energía, climatización. Los servicios subcontratados a terceros Las instalaciones físicas El personal Usuarios Operadores y administradores

Tabla 8: Clasificación de Activos. Fuente: Magerit

5.1.1.2 Paso 2: Valoración de los Activos

Una vez identificados los activos relacionados con la oficina de sistemas de la Alcaldía de Popayán es necesario valorarlos de acuerdo a los criterios establecidos por la metodología Magerit los cuales son [3]:

- Confidencialidad ¿Qué daño causaría que lo conociera quien no debe?

La información no debe ser conocida por todos los individuos de la organización, en este caso la Alcaldía de Popayán, debido a que se puede hacer un uso inapropiado de está, causando múltiples daños a la organización en cuanto al manejo de la información [22].

- Autenticidad ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

La autenticidad consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos [22].

- Integridad ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?

La información que están obteniendo, leyendo y trabajando, es exactamente la misma que fue colocada desde un principio, es decir, que sea la información original. Si esta llegara a sufrir alteraciones, puede ocasionar grandes conflictos como perdida de información, afectando la comunicación y la toma de decisiones en la Alcaldía de Popayán [22].

- Disponibilidad ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?

Permite que la información pueda ser utilizada cuando sea necesario, teniendo en cuenta el acceso de las personas autorizadas, de esta forma, la información debe ser accedida de forma segura para que se pueda usar en el momento en que se solicita [22].

- Trazabilidad ¿Qué daños causaría no saber a quién se le presta tal servicio? O ¿Quién accede a los datos?

La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad [3] [22].

La valoración de los activos por parte de la metodología margerit hace referencia al de calcular un valor a través de una escala cualitativa donde se valora el activo de acuerdo al impacto que puede causar en la empresa su daño o perdida, en consecuencia la escala se refleja en [3]:

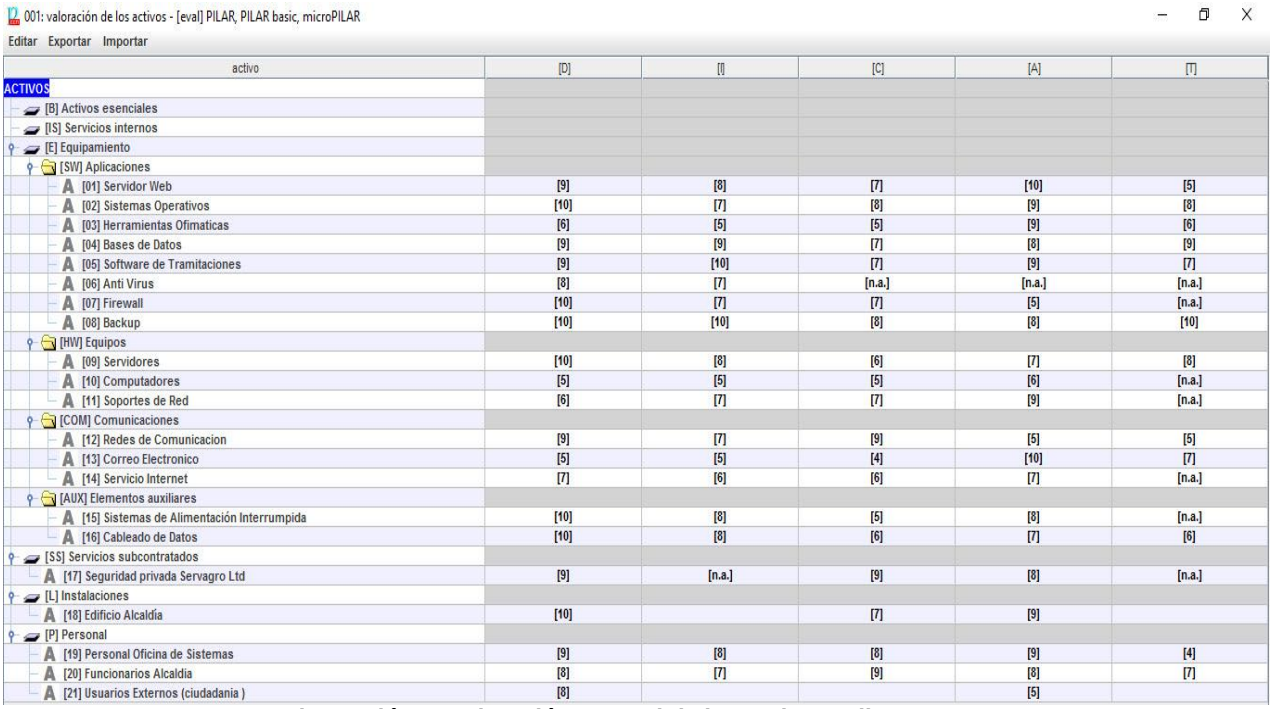
- Muy Alto (MA)
- Alto (A)
- Medio (M)
- Bajo (b)
- Muy bajo (MB)

Las dimensiones de seguridad que contempla la metodología Magerit son: Confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad, en la valoración de activos. En cada una de estas dimensiones se define unos criterios de valoración que nos permitan ubicar la posición en que se encuentra cada activo frente a cada dimensión. A continuación se relacionan los criterios que se podrían tener en cuenta para valorar los activos con respecto a cada dimensión de seguridad [3].

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Tabla 9: Criterios de Evaluación. Fuente: Magerit

En base a los criterios anteriores, se puede hacer una valoración cualitativa de cada activo en relación a las dimensiones de seguridad contempladas en la metodología magerit. En la figura siguiente, se ilustra un ejemplo de la herramienta Pilar, sobre la forma como se pueden valorar los activos con el nivel de dependencia [3].


001: valoración de los activos - [eval] PILAR, PILAR basic, microPILAR

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[01] Servidor Web	[9]	[8]	[7]	[10]	[5]
[02] Sistemas Operativos	[10]	[7]	[8]	[9]	[8]
[03] Herramientas Ofimaticas	[6]	[5]	[5]	[9]	[6]
[04] Bases de Datos	[9]	[9]	[7]	[8]	[9]
[05] Software de Tramitaciones	[9]	[10]	[7]	[9]	[7]
[06] Anti Virus	[8]	[7]	[n.a.]	[n.a.]	[n.a.]
[07] Firewall	[10]	[7]	[7]	[5]	[n.a.]
[08] Backup	[10]	[10]	[8]	[8]	[10]
[HW] Equipos					
[09] Servidores	[10]	[8]	[6]	[7]	[8]
[10] Computadores	[5]	[5]	[5]	[6]	[n.a.]
[11] Soportes de Red	[6]	[7]	[7]	[9]	[n.a.]
[COM] Comunicaciones					
[12] Redes de Comunicacion	[9]	[7]	[9]	[5]	[5]
[13] Correo Electronico	[5]	[5]	[4]	[10]	[7]
[14] Servicio Internet	[7]	[6]	[6]	[7]	[n.a.]
[AUX] Elementos auxiliares					
[15] Sistemas de Alimentación Interrumpida	[10]	[8]	[5]	[8]	[n.a.]
[16] Cableado de Datos	[10]	[8]	[6]	[7]	[6]
[SS] Servicios subcontratados					
[17] Seguridad privada Servagro Ltd	[9]	[n.a.]	[9]	[8]	[n.a.]
[L] Instalaciones					
[18] Edificio Alcaldía	[10]		[7]	[9]	
[P] Personal					
[19] Personal Oficina de Sistemas	[9]	[8]	[8]	[9]	[4]
[20] Funcionarios Alcaldia	[8]	[7]	[9]	[8]	[7]
[21] Usuarios Externos (ciudadania)	[8]			[5]	

Ilustración 1: Valoración general de los activos. Pilar

5.1.1.3 Paso 3: Amenazas (identificación y valoración)

Actualmente hay múltiples amenazas que pueden afectar los activos de una empresa en este caso la Alcaldía de Popayán, por ello es importante identificarlas y determinar el nivel de exposición en la que se encuentra cada activo de

información en la Alcaldía. Se considera una amenaza, a cualquier situación que pueda dañar o deteriorar un activo, impactando directamente cualquiera de las cuatro dimensiones de seguridad establecidas en la metodología magerit [3]. La ISO/IEC13335-1:2004 define que una "amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización".

Identificación de amenazas

La metodología Magerit tiene un catálogo de amenazas posibles que puede tener un activo de información. Las amenazas se clasifican en cuatro grupos: Desastres naturales(N), de origen industrial (I), errores y fallos no intencionados (E), ataques deliberados o intencionados(A). Cada grupo de amenaza se representa por una letra, así mismo cada grupo presenta en forma específica los tipos de amenazas que se pueden presentar. A continuación se presenta el listado codificado de las posibles amenazas que se pueden presentar en cada uno de los grupos mencionados [3].

[N] Desastres naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

[I] De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino

[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.16] Introducción de falsa información
[E.17] Degradación de la información
[E.18] Destrucción de la información
[E.19] Divulgación de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
Política de control de acceso en la Alcaldía de Popayán.

A] Ataques deliberados
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

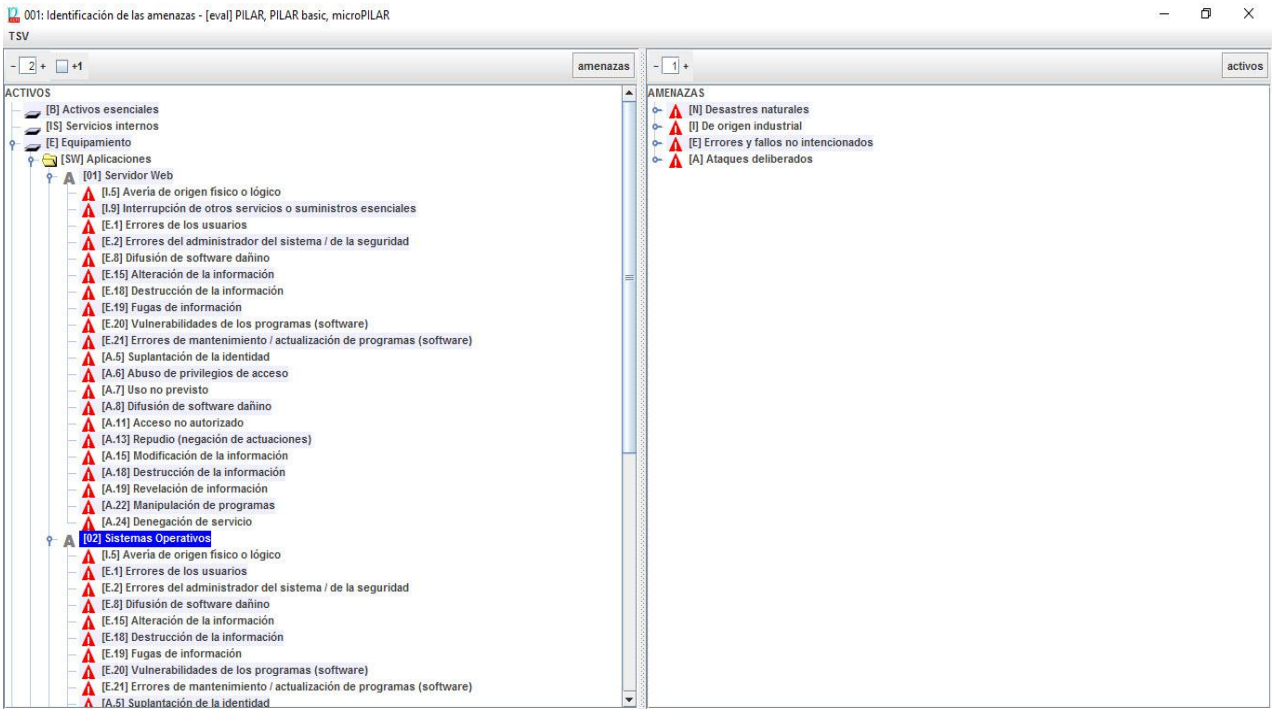


Ilustración 2: Identificación de amenazas. Pilar

Valoración de amenazas

Cuando se registra que un activo es víctima de una amenaza, este no se ve afectado en todas sus dimensiones, ni en la misma consideración, una vez determinado que una amenaza puede perjudicar a un activo, se estima cuán vulnerable es el activo, en dos sentidos [3]:

- Degradación: cuán perjudicado resultaría el activo.
- Frecuencia: cada cuánto se materializa la amenaza.

La degradación evalúa el daño causado por un incidente en el hipotético caso de que ocurriera, la degradación se caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde [1][3]..

Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna ya que el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, una amenaza puede ser de terribles consecuencias y de muy improbable materialización; mientras que otra

amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

Para valorar las amenazas es necesario que se estime una escala de valores que nos permita determinar el rango de frecuencia en que se puede presentar la amenaza, la cual se realiza mediante estimaciones anuales, mensuales, y semanales, asignando un número de veces.

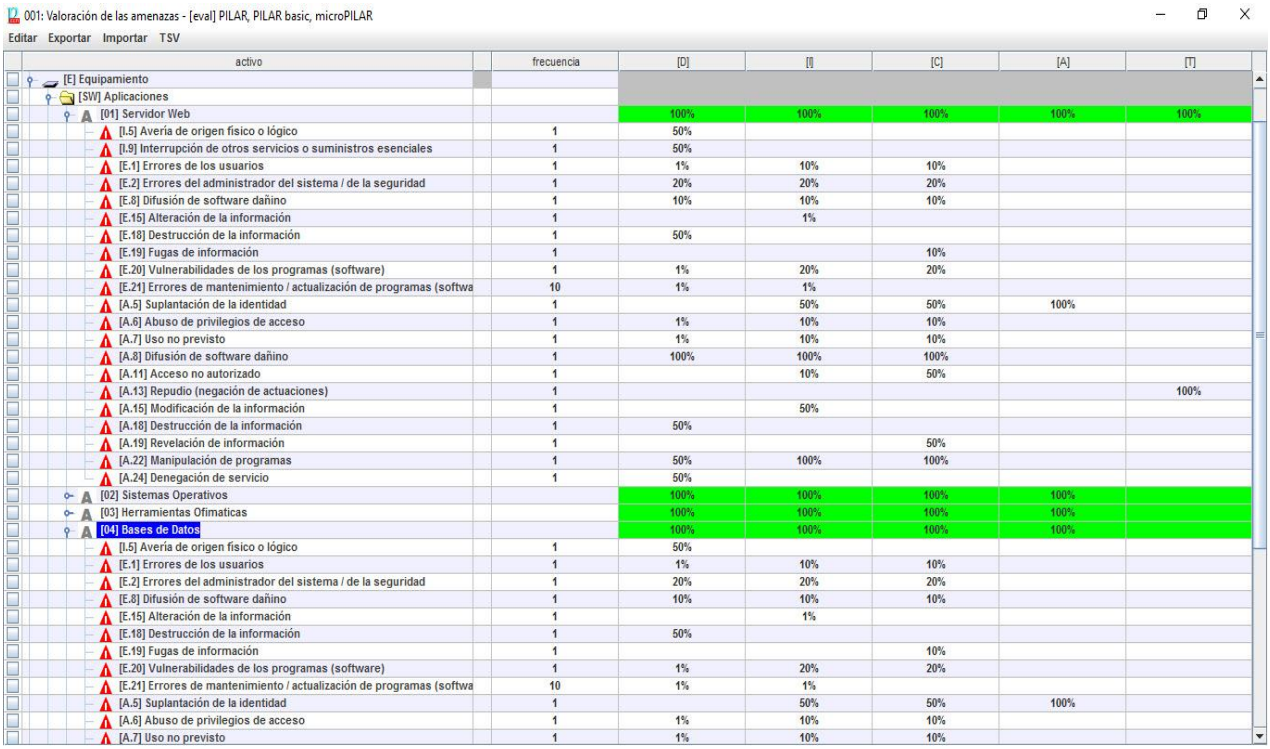
Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Tabla 10: Rango de frecuencias. Magerit

A continuación se presenta el rango de impactos de manera porcentual para cada activo con el nivel de frecuencia y el impacto en cada una de las dimensiones de seguridad.

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

Tabla 11: Rango de impactos. Magerit



activo	frecuencia	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento						
[SW] Aplicaciones						
[01] Servidor Web		100%	100%	100%	100%	100%
[I.5] Avería de origen físico o lógico	1	50%				
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%				
[E.1] Errores de los usuarios	1	1%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%		
[E.8] Difusión de software dañino	1	10%	10%	10%		
[E.15] Alteración de la información	1		1%			
[E.18] Destrucción de la información	1	50%				
[E.19] Fugas de información	1			10%		
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (softwa	10	1%	1%			
[A.5] Suplantación de la identidad	1		50%	50%	100%	
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%		
[A.7] Uso no previsto	1	1%	10%	10%		
[A.8] Difusión de software dañino	1	100%	100%	100%		
[A.11] Acceso no autorizado	1		10%	50%		
[A.13] Repudio (negación de actuaciones)	1					100%
[A.15] Modificación de la información	1		50%			
[A.18] Destrucción de la información	1	50%				
[A.19] Revelación de información	1			50%		
[A.22] Manipulación de programas	1	50%	100%	100%		
[A.24] Denegación de servicio	1	50%				
[02] Sistemas Operativos		100%	100%	100%	100%	
[03] Herramientas Ofimaticas		100%	100%	100%	100%	
[04] Bases de Datos		100%	100%	100%	100%	
[I.5] Avería de origen físico o lógico	1	50%				
[E.1] Errores de los usuarios	1	1%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%		
[E.8] Difusión de software dañino	1	10%	10%	10%		
[E.15] Alteración de la información	1		1%			
[E.18] Destrucción de la información	1	50%				
[E.19] Fugas de información	1			10%		
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (softwa	10	1%	1%			
[A.5] Suplantación de la identidad	1		50%	50%	100%	
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%		
[A.7] Uso no previsto	1	1%	10%	10%		

Ilustración 3: Valoración de las Amenazas. Pilar

Determinación del impacto potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos se clasifica el impacto en acumulado y repercutido [3].

Impacto acumulado

Es el cálculo sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que se deben establecer para la protección de la información [3].

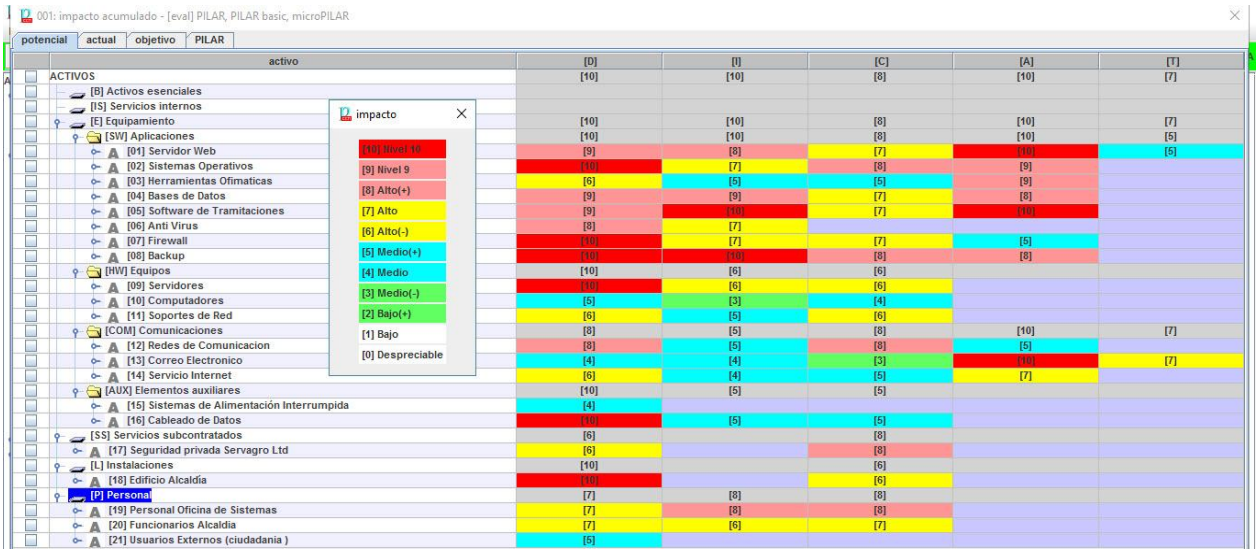


Ilustración 4: Impacto Acumulado. Pilar

Impacto repercutido

Al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la gestión del sistema de información. Es una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos aceptar el nivel de riesgo [3].

Ilustración 5: Impacto repercutido. Pilar

Determinación del riesgo potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia [3].

Riesgo acumulado

Es el cálculo sobre los activos que soportan el peso de los sistemas de información, permite determinar las salvaguardas necesarias para dar a los medios de trabajo como protección de los equipos, copias de respaldo, etcétera [3].

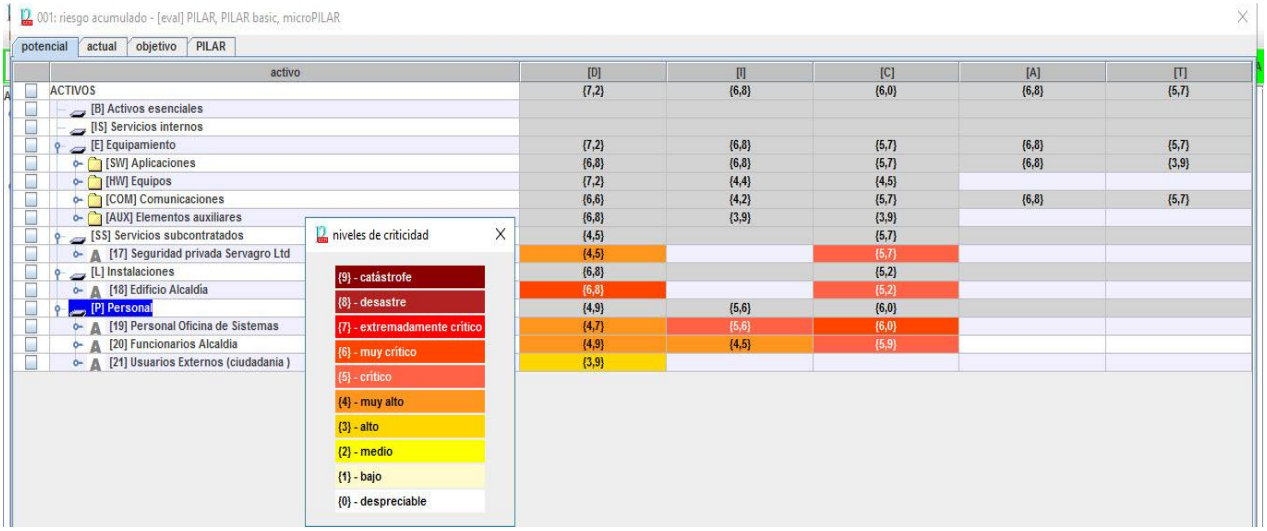


Ilustración 6: Riesgo acumulado. Pilar

Riesgo repercutido

El cálculo sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la tarea del sistema de información.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{7,2}	{6,8}	{6,0}	{6,8}	{5,7}
[SW.01] Servidor Web	{6,2}	{5,7}	{5,1}	{6,8}	{3,9}
[SW.02] Sistemas Operativos	{6,8}	{5,1}	{5,7}	{6,2}	
[SW.03] Herramientas Ofimaticas	{4,5}	{3,9}	{3,9}	{6,2}	
[SW.04] Bases de Datos	{6,2}	{6,2}	{5,1}	{5,7}	
[SW.05] Software de Tramitaciones	{6,2}	{6,8}	{5,1}	{6,8}	
[SW.06] Anti Virus	{5,7}	{5,1}			
[SW.07] Firewall	{6,8}	{5,1}	{5,1}	{3,9}	
[SW.08] Backup	{6,8}	{6,8}	{5,7}	{5,7}	
[HW.09] Servidores	{7,2}	{4,4}	{3,9}		
[HW.10] Computadores	{4,2}	{2,7}	{3,4}		
[HW.11] Soportes de Red	{4,8}	{3,8}	{4,5}		
[COM.12] Redes de Comunicacion	{6,6}	{3,8}	{5,7}	{3,9}	
[COM.13] Correo Electronico	{4,2}	{4,2}	{2,8}	{6,8}	{5,7}
[COM.14] Servicio Internet	{5,4}	{3,2}	{3,9}	{5,1}	
[AUX.15] Sistemas de Alimentación Interrumpida	{3,3}				
[AUX.16] Cableado de Datos	{6,8}	{3,9}	{3,9}		
[17] Seguridad privada Servagro Ltd	{4,5}		{5,7}		
[18] Edificio Alcaldía	{6,8}		{5,2}		
[19] Personal Oficina de Sistemas	{4,7}	{5,6}	{6,0}		
[20] Funcionarios Alcaldía	{4,9}	{4,5}	{5,9}		
[21] Usuarios Externos (ciudadania)	{3,9}				

Ilustración 7: Riesgo repercutido. Pilar

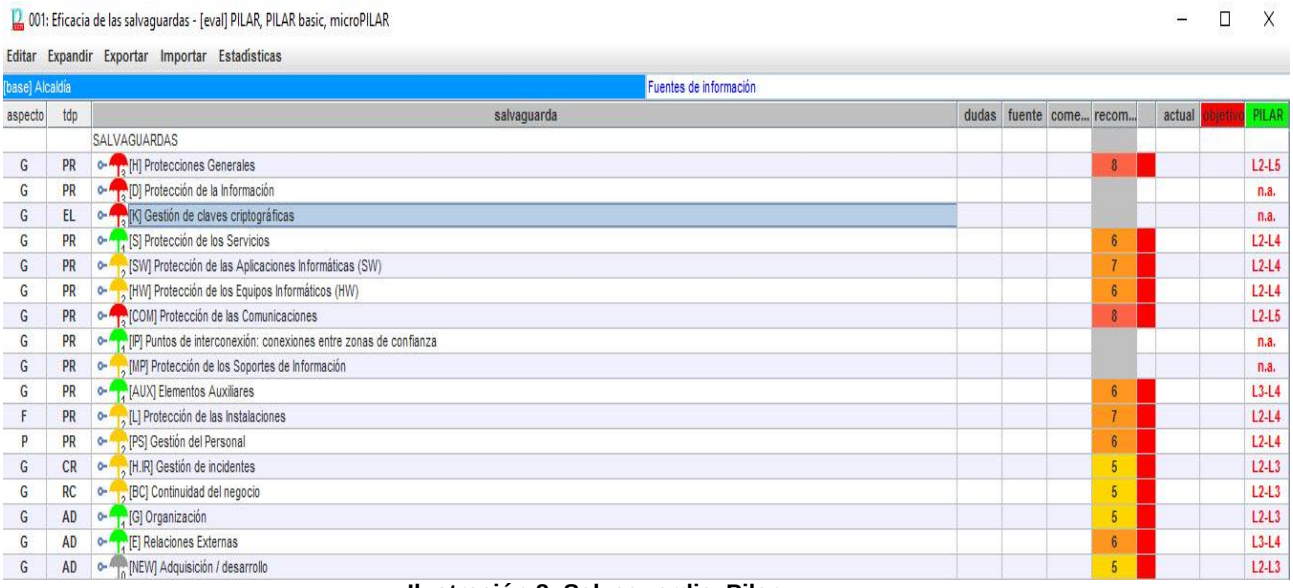
Al determinar el impacto potencial y determinar el riesgo potencial que asume la Alcaldía de Popayán al no tener implementados controles de seguridad sobre sus sistemas de información [3].

5.1.1.4 Paso 4 Salvaguardas

La metodología Margerit define las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que requieren simplemente una organización adecuada, mientras que otras requieren elementos técnicos (programas o equipos), otras de seguridad física y por último está la política de personal u organizacional [3].

Las salvaguardas permiten hacer frente a las amenazas o vulnerabilidades en los activos estos aparecen gracias a que:

- Aparecen tecnologías nuevas
- Desapareciendo tecnologías antiguas
- Cambian los [tipos de] activos a considerar,
- Evolucionan las posibilidades de los atacantes



aspecto	tdp	salvaguarda	dudas	fuente	come...	recom...	actual	objetivo	PILAR
		SALVAGUARDAS							
G	PR	[H] Protecciones Generales				8			L2-L5
G	PR	[D] Protección de la Información							n.a.
G	EL	[K] Gestión de claves criptográficas							n.a.
G	PR	[S] Protección de los Servicios				6			L2-L4
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7			L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				6			L2-L4
G	PR	[COM] Protección de las Comunicaciones				8			L2-L5
G	PR	[IP] Puntos de interconexión: conexiones entre zonas de confianza							n.a.
G	PR	[MP] Protección de los Soportes de Información							n.a.
G	PR	[AUX] Elementos Auxiliares				6			L3-L4
F	PR	[L] Protección de las Instalaciones				7			L2-L4
P	PR	[PS] Gestión del Personal				6			L2-L4
G	CR	[IR] Gestión de incidentes				5			L2-L3
G	RC	[BC] Continuidad del negocio				5			L2-L3
G	AD	[G] Organización				5			L2-L3
G	AD	[E] Relaciones Externas				6			L3-L4
G	AD	[NEW] Adquisición / desarrollo				5			L2-L3

Ilustración 8: Salvaguardia. Pilar

La Alcaldía de Popayán hoy en día posee seguridad sobre sus activos, generalmente la contemplan sobre la protección de las localidades físicas donde se encuentran físicamente sus activos de información y alguna protección lógica a nivel de antivirus o firewall pero no contempla es forma específicas medidas o salvaguardas para el control de acceso a la información [3].
Por esta razón se debe establecer, documentar y revisar una política de control de acceso con base en las necesidades de seguridad y de negocio de la Alcaldía de Popayán el establecimiento, seguimiento, mejora continua y aplicación de la seguridad de la información. Tiene como objetivo principal establecer reglas sobre el uso de los sistemas informáticos y de comunicaciones de la Alcaldía de Popayán por parte de los jefes de dependencias, funcionarios o terceros, proteger los recursos informáticos de la entidad y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información [1][3].

Garantiza un compromiso ineludible de protección frente a una amplia gama de amenazas concientizando a los funcionarios de la Alcaldía de Popayán como la ciudadanía en común. Con la implementación de esta política de control de acceso, se contribuye a minimizar los riesgos asociados de daño y se asegura el cumplimiento de las funciones de los usuarios en los sistemas de información [1][3].

Los lineamientos que se establecen para el cumplimiento de la política de control de acceso son los siguientes:

- Los funcionarios, contratistas, outsourcing o terceros, antes de solicitar acceso a los sistemas de información deben firmar un acuerdo de confidencialidad.
- Impedir el acceso no autorizado a los sistemas de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

5.2 POLÍTICA DE CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA DE POPAYÁN

Ofrece explicaciones comprensibles acerca del por qué deben tomarse decisiones sobre el acceso a la información, transmitir por qué son importantes estos u otros recursos o servicios de información, llevar un proceso de actualización periódica sujeto a los cambios organizacionales relevantes en la Alcaldía de Popayán, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de las dependencias, entre otras [5].

Se garantiza el acceso a los funcionarios, contratistas y terceros que tengan autorización de acceso a los sistemas de información donde se establecen procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Estos procedimientos deberán cumplir todas las etapas del ciclo de vida de acceso, como también el acceso debe estar compuesto por un ID o nombre de usuario y contraseña que debe ser único por cada servidor público o tercero. El registro inicial en los sistemas de información de los nuevos usuarios se debe dar hasta su baja o cuando ya no sea necesario su acceso a los sistemas y servicios de información pertenecientes a la Alcaldía de Popayán, eliminando todo registro existente sobre el usuario y sus permisos dentro de los sistemas a los cuales tenía acceso [5].

Registro de usuario: Con el objetivo de impedir el acceso no autorizado a la información se implementará documentación formal para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información [1] [5].

La Oficina de Sistemas de la Alcaldía de Popayán, debe mantener un registro donde cada uno de los jefes de dependencias responsables de los procesos haya autorizado a los funcionarios o terceros. El acceso a los diferentes sistemas de información será realizado por el responsable encargado de la Oficina de Sistemas, en donde se definirá un documento de registro de usuarios para otorgar

y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario el cual debe comprender [1] [5]:

- Utilizar identificadores de usuarios únicos, de modo que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo funcionario. El uso de identificadores grupales solo se debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas [1] [5].

- Comprobar que el usuario tiene autorización del propietario de la información en este caso el jefe de dependencia para el uso de sistema, base de datos o servicio de información [1] [5].

- Las cuentas de usuario (funcionarios, contratistas y terceros) creadas en los sistemas de información de la Alcaldía de Popayán deben tener un identificador único y deberán solicitarse mediante un requerimiento formal, especificando su identificación, nombres y apellidos y sus funciones que va a desempeñar y autorizado por el jefe inmediata en este caso el jefe de la dependencia. Las cuentas de los usuarios externos deben ser solicitadas y autorizadas a través del jefe de la oficina de sistemas de la Alcaldía de Popayán [1] [5] [25].

- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la ocupación del funcionario y es coherente con la política de seguridad de la Alcaldía de Popayán [1].

- Requerir que los funcionarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso [1].
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización [1].

- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o de aquellos a los que se les revoco la autorización o se desvincularon de la Alcaldía de Popayán [1].

- Efectuar revisiones periódicas con el objeto de:
  - Cancelar cuentas de usuarios redundantes.
  - Inhabilitar cuentas inactivas por más de 60 días.
  - Eliminar cuentas inactivas por más de 120 días.
  - En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados [1][2].

- Identificar los privilegios asociados a cada sistema de información, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las condiciones de personal a las cuales deben asignarse los privilegios de acceso donde debe estar establecido el vínculo con la Alcaldía [2].

- Asignar los privilegios a funcionarios sobre la base de la necesidad de uso y servicio por ejemplo el requerimiento mínimo para su rol funcional en los sistemas de información [2].

- Mantener un proceso de autorización y registro de todos los privilegios asignado a cada funcionario registrado [2].

- Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización [2].

- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios [2].

Los funcionarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas cumpliendo los siguientes lineamientos:

- Mantener las contraseñas en secreto.
- Pedir el cambio de contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad de acuerdo a las prescripciones informadas por el responsable del activo de información de se trate, que:
  - Sean fáciles de recordar.
  - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombre, números de teléfono, fecha de nacimiento, etcétera.
  - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisionales en el primer inicio de sesión.

- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas: perdida o indicio de pérdida de confidencialidad.
- Si los funcionarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificara a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas.

Con el fin de mantener un control eficaz en el acceso a los datos y servicios de información, la oficina de sistemas de la Alcaldía de Popayán, llevara a cabo un proceso donde se revisara los derechos de acceso de los usuarios y se contemplara los siguientes controles [2].

- Revisar los derechos de acceso de los usuarios en intervalos de 4 meses.
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 2 meses.
- En caso de destitución o término de contrato se actualizarán los derechos de accesos en un plazo máximo de 3 días desde que se recibe la solicitud en la oficina de sistemas y posteriormente en los sistemas de información.
- Los encargados de la oficina de sistemas de la Alcaldía una vez avisado por la oficina de talento humano que se encarga de la gestión de funcionarios dentro de la organización, estos harán una revisión pertinente de los privilegios que este funcionario tendrá en los sistemas de información y adecuarlo a las necesidades que debe suplir.

El personal de la Oficina de Sistemas de la Alcaldía indica los procedimientos que deben seguir los funcionarios, contratistas y terceros para acceder a los sistemas de información de una manera adecuada y efectiva que no ponga en riesgo la integridad de la información. Comprobar el cumplimiento de los procedimientos establecidos, relacionados con el control de acceso, creación de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red y autenticación de usuarios [2].

Concientizar a los funcionarios sobre el uso apropiado de contraseñas y de equipos de trabajo logrando impedir el acceso de usuarios no autorizados y garantizar el compromiso de todo aquel que tenga acceso a la información independientemente de su jerarquía, siempre tendrá alguna responsabilidad a partir del momento que tenga acceso a la información y recursos para el tratamiento de la información, la cooperación de los funcionarios autorizados es esencial para una seguridad efectiva donde deben ser conscientes de sus

responsabilidades dentro de la Alcaldía de Popayán. Para ello se debe contemplar [1] [2]:

- Definir documentación para la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario, el monitoreo del uso de las instalaciones de procesamiento de la información, la solicitud y aprobación de acceso a internet, el uso de computación móvil y la revisión de registros de actividades [1].
- Requerimientos de seguridad de cada una de las aplicaciones a las cuales puedan acceder de manera que se lleve un registro sobre el comportamiento del usuario en el sistema [1].
- Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo a su perfil de cargo en la Alcaldía de Popayán [1].
- Definir pautas de utilización de internet para todos los usuarios [1].
- Promover el desarrollo y uso adecuado de los sistemas de información para evitar la necesidad de sancionar a los funcionarios [1].
- Mantener contraseñas en secreto [1].

Todos los funcionarios, contratistas y terceros deben cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 3 meses exigiendo el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas donde deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales [2].

Los funcionarios deben cumplir las siguientes normas:

- Contraseñas fáciles de recordar y difíciles de adivinar.
- Conservar los datos de acceso en secreto.
- Las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona ingeniería social por ejemplo nombre, fecha de nacimiento, nombre de la mascota, números de teléfono entre otras.
- Se deberá notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

La jede de la oficina de sistemas ingeniera María Isabel Calderón debe coordinar con los jefes de dependencias las tares de concientización a todos los funcionarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección [1][2][25].

Los equipos instalados en áreas de usuarios en este caso en las diferentes dependencias de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentren desatendidos [5].

Los funcionarios deberán garantizar que los equipos desatendidos disponen de la protección apropiada para impedir el acceso no autorizado [1][2].

Los usuarios deberán cumplir las siguientes pautas de seguridad [1][2]:

- Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo un protector de pantalla protegido por contraseña.
- Proteger los equipos contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo contraseña de acceso cuando no se utilizan.
- Bloquear el equipo de cómputo tras abandonar el puesto de trabajo.
- Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior a 5 minutos.
- Apagar los equipos de cómputo al finalizar la jornada laboral.

Se establece una política de escritorios y pantallas limpias para proteger documentos en papel y dispositivos de almacenamiento en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo esto debe ser acatado por todos los funcionarios de manera eficiente [1][2][5].

Los lugares de trabajo de los funcionarios y externos que prestan servicios en la institución deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el trabajador [2][5].

Los equipos que queden ubicados cerca de zonas de atención o tránsito de público deben situarse de forma que las pantallas no pueden ser visualizadas por personas externas.

Cada vez que un funcionario o externo se ausenta de su lugar de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro el documento en el que está trabajando.

El proceso de servicio de tecnologías de comunicación e información utilizado por la oficina de sistemas de la Alcaldía de Popayán debe cerciorar el bloqueo al

acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la organización mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Se debe controlar las excepciones de acceso las cuales serán aprobadas por el jefe de la oficina de sistemas, según la necesidad del cargo y verificación previa de que las páginas solicitadas no contengan código malicioso con el visto bueno del encargado en seguridad de la información dando garantía del acceso en la red [1][2].

Se debe utilizar las prestaciones de seguridad del sistema operativo para permitir el acceso exclusivo a los funcionarios autorizados; estos, deben acceder de acuerdo a la política de control de accesos definida anteriormente teniendo en cuenta que se registran los intentos de autenticación correctos y fallidos del sistema a la hora de ingresar, emiten señales de alarma cuando se violan las políticas de seguridad del sistema, disponen de los recursos adecuados para la autenticación, restringen los horarios de conexión de los usuarios cuando sea necesario [1][2].

Procedimientos seguros de inicio de sesión: debe controlarse el acceso al sistema operativo mediante procedimientos seguros de conexión y un inicio seguro de la sesión que tendrá las siguientes condiciones:

- No mostrar información correspondiente al sistema hasta que se haya cumplido el proceso de inicio.
- Limitar el número de intentos fallidos de conexión.
- No mostrar las contraseñas digitadas.

Identificación y autenticación de usuario: todos los funcionarios deberían disponer de un único identificador propio exclusivo. Se debe elegir una técnica de autenticación adecuada que verifique la identidad de un usuario como una credencial de acceso con nombre de usuario, Rh y un código de barras que lo identifique de manera única y exclusiva para acceder a la información según su rol en la Alcaldía [1] [2].

Sistema de gestión de contraseñas: Los datos de acceso a los sistemas operativos deberán estar compuestos por un ID o nombre de usuario y contraseña que debe ser único por cada servidor público o tercero [1].

Permitir a los usuarios la selección y cambios en sus propias contraseñas luego de cumplido el plazo de mínimo manteniendo cuando se considere que su contraseña ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso [1].

Uso de los recursos del sistema: el uso de los recursos del sistema sólo estará restringido al personal encargado de la Oficina de Sistemas de la Alcaldía de Popayán donde se establecerá una política de controlador de dominio el cual no permitirá la instalación de software y cambios de configuración del sistema [1].

Desconexión automática de sesión: si por alguna razón el funcionario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan acceder o ver su trabajo con la sesión de usuario habilitada [1].

Limitación del tiempo de conexión: utilizar limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo como nómina almacén y contratación, finanzas plus las cuales detectan inactividad por un periodo igual o superior a ocho minutos, deben automáticamente aplicar, “timeout” es decir, finalizar la sesión de usuario [1].

Se establece en la política de control de acceso a información digital teniendo en cuenta los niveles de clasificación y manejo de la información según los niveles deberán gestionarse los accesos a los usuarios mediante quehaceres como [1]:

- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambiar la contraseña de acceso si tiene sospecha que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Seleccionar contraseñas que no sean fáciles de adivinar.

Restricción del acceso a la información: Restringir el acceso a la información a todas las personas que hagan parte de la Alcaldía de Popayán sean funcionarios, contratistas o terceros a la información y funciones de los sistemas de información. Al aislar estos accesos a los sistemas se prevé el intercambio seguro de información ya que no se permitiría duplicar información con otros sistemas, sólo los encargados de la Oficina de Sistemas de la Alcaldía tendrán estos privilegios para manipular la información sin perder su integridad [1].

Aislamiento de sistemas sensibles: los sistemas de información que sean sensibles a posibles pérdidas que afecten la operatividad de la Alcaldía de Popayán deben establecer un entorno donde tengan los recursos necesarios para tener la mejor funcionalidad posible; además, se debe documentar la sensibilidad que tienen estos a la hora de manipularlos para tener un punto de partida a la hora de su utilización [1].

El personal de la Oficina de Sistemas, debe documentar las obligaciones y regulaciones que deben tener los funcionarios al utilizar estas herramientas de la Alcaldía de Popayán por medio de [2][5]:

- Uso de un ID de usuario y contraseña únicos para el acceso.
- Uso de software antivirus provisto por la Oficina de Sistemas.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por la Oficina de Sistemas.
- Realización de copias de seguridad periódicas establecidas por el procedimiento de backups de la oficina de sistemas.

CAPÍTULO 6. CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

1. Es necesario implementar urgentemente una política de seguridad informática en la Alcaldía de Popayán, en especial de control de acceso a los sistemas computarizados, principalmente por dos motivos: el primero es el cumplimiento de las normas nacionales de tener una política de seguridad informática en las entidades gubernamentales y, segundo, corresponde a los problemas que se encontraron con relación al control de acceso a los sistemas de la Alcaldía que presentan en la actualidad una gran vulnerabilidad.

2. Se encontró que en otras alcaldías de Colombia están dando cumplimiento a las normas con respecto a tener una política de seguridad informática establecida. Es esta la oportunidad que puede aprovechar la Alcaldía de Popayán para establecer convenios con las otras alcaldías que apoyen la realización de una política de seguridad informática que parta de la adopción de esta Propuesta y la implementación de la misma, como base de su política integral de seguridad informática.

3. Fue posible proponer una política de control de acceso para los sistemas de información de la Alcaldía de Popayán con base en la normatividad internacional existente y a las implementaciones realizadas en otras alcaldías de acuerdo a lo establecido por las normas nacionales, la cual está conformada por cuatro estrategias: requerimientos para el control de acceso a los sistemas de información, gestión de acceso de usuarios, responsabilidad de usuarios, control de acceso a sistemas y aplicaciones.

6.2 RECOMENDACIONES

Se recomienda realizar campañas de concientización sobre la importancia de la seguridad de la información, esta campaña será dirigida a todo el personal de la Alcaldía.

- Se debe realizar difusiones de las políticas de control de acceso a la información a todo el personal de la Alcaldía.

- Se recomienda contar con controles de prohibiciones de los activos de información asignados a personal.

- Se debe elaborar convenios sobre el buen uso de los activos y compromiso de responsabilidad de los activos de información.

- Este convenio debe estar firmado y registrado por todos los empleados de la Alcaldía de Popayán.

- Es necesario la implementación de software en los sistemas operativos para minimizar el riesgo de corrupción de la información.

- Se debe mantener un control estricto del acceso al código fuente de los programas, para así evitar copia, modificación o divulgación de los mismos.

Bibliografía

[1] ISO, “ISO 27002 en español,” *Norm. ISO*, vol. 2013, 2013.

[2] A. C. Estrada, “Seguridad Por Niveles,” p. 709, 2011.

[3] M. A. Amutio Gómez, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,” p. 127, 2012.

[4] M. R. Granados, “Definiciones e historia de la seguridad informática,” *Univ. Nac. Autónoma México*, pp. 5–47, 2011.

[5] N. Co-investigator, “Politicas de seguridad informatica,” *J. Chem. Inf. Model.*, vol. 53, pp. 1689–1699, 2013.

[6] W. R. Rojas, “INTRAMUROS: LA CONTABILIDAD Y LA ORGANIZACIÓN,” *Contaduría Universidad de Antioquia*, no. 34. pp. 101–117, 25-Jan-2016.

[7] F. N. S. Solarte, E. R. E. Rosero, and M. del C. Benavides, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001,” *Revista Tecnológica - ESPOL*, vol. 28, no. 5. 31-Dec-2015.

[8] Á. Gómez and C. Suárez, “Sistemas de Información. Herramientas prácticas para la gestión empresarial.,” *Ra-Ma*, pp. 11–56, 2006.

[9] A. Martínez-ballesté, “Identificacion, Autenticación y Control de Acceso.”

[10] C. A. R. Haro, “La Seguridad Informática,” *Revista Ciencia Unemi*, vol. 4, no. 5. pp. 26–33, 02-Jun-2015.

[11] M. Collazos, “La nueva Versión ISO 27001:2013 Uncambio en la integración de los sistemas de gestión,” 2015.

[12] Real Academia Española, “informatica,” 2014. [Online]. Available: http://lema.rae.es/drae/srv/search?key=inform%C3%A1tica.

[13] S. D. E. R. D. E. Computadoras, “Seguridad de redes de computadoras,” pp. 352–377.

[14] M. A. Amutio Gómez, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,” p. 75, 2012.

[15] R. Vuanello, “La cibercriminalidad como atentado a los derechos humanos de los más jóvenes Cyber crime seen as an attack on the human rights dos mais jovens,” pp. 249–260, 2011.

[16] Jecas, “SISTEMAS DE SEGURIDAD CON RELACIÓN A ASPECTOS LEGALES, CONTROL DE ACCESOS, SOFTWARE,” pp. 1–28, 2004.

[17] J. A. M. S. and Z. R. R., “GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO DESDE UNA PERSPECTIVA ORGANIZACIONAL,” *Ingenierías USBmed*, vol. 3, no. 1. pp. 23–34, 21-Apr-2015.

[18] I. R. D. C. Atacama, “POLITICA Y CONTROL DE ACCESO.”

[19] J. M. Rodríguez and M. J. Daureo, “Sistemas de información: aspectos técnicos y legales,” p. 322, 2003.

[20] J. Areitio Bertolín, *Seguridad de la información : redes, informática y sistemas de información*. Paraninfo Cengage Learning, 2008.

[21] Lopez Aguilera Purificacion, “Seguridad informática - Purificación Aguilera López - Google Libros,” 210AD. [Online]. Available:

https://books.google.es/books?id=Mgvm3AYIT64C&dq=control+de+acceso+seguridad+informatica&lr=&hl=es&source=gbs_navlinks_s.

[22] D. G. Rosado, C. Blanco, L. Enrique Sánchez, E. Fernández-Medina Mario Piattini, and uclmes Resumen, “La Seguridad como una asignatura indispensable para un Ingeniero del Software.”

[23] W. Stallings, *Fundamentos de seguridad en redes : aplicaciones y estándares*. Pearson/Prentice Hall, 2004.

[24] M. L. T. Cossio, L. F. Giesen, G. Araya, M. L. S. Pérez-Cotapos, R. L. Vergara, M. Manca, R. a. Tohme, S. D. Holmberg, T. Bressmann, D. R. Lirio, J. S. Román, R. G. Solís, S. Thakur, S. N. Rao, E. L. Modelado, A. D. E. La, C. Durante, U. N. a Tradición, M. En, E. L. Espejo, D. E. L. a S. Fuentes, U. A. De Yucatán, C. M. Lenin, L. F. Cian, M. J. Douglas, L. Plata, and F. Héritier, “Hardware y Software,” *Uma ética para quantos?*, vol. XXXIII, no. 2, pp. 81–87, 2012.

[25] “Oficina Asesora de TIC.” [Online]. Available: http://popayan.gov.co/ciudadanos/la-alcaldia/unidades-administrativas-e-instancias-de-gestion/oficina-asesora-de-tic. [Accessed: 12-Jun-2015].

[26] “Kaspersky Virtualization Security | Kaspersky Lab LAM.” [Online]. Available: http://latam.kaspersky.com/enterprise-security/virtualization. [Accessed: 15-May-2016].

[27] E. Giménez Toledo and A. Román Román, “Vigilancia tecnológica e inteligencia competitiva: conceptos, profesionales, servicios y fuentes de información,” *El Prof. la Inf.*, vol. 10, no. 5, pp. 11–20, 2001.

[28] E. R. Ibujés Flores, “Diseño e implementación de un sistema de monitoreo y control para un Data Center de una industria.” Quito : EPN, 2015., 20-Jan-2015.

[29] M. Castells, “La Era de la información: economía, sociedad y cultura,” p. 495, 1997.

[30] P. Hernando, “Oficina de Sistemas.” 2016.

[31] P. N. Rasmussen, “Diferentes tipos de sistemas UPS,” pp. 1–11.

[32] “Soluciones de backup de servidores para entornos virtuales y de nube | Arcserve.” [Online]. Available: http://www.arcserve.com/ar/products-solutions/products/server-backup-software.aspx. [Accessed: 15-May-2016].

[33] E. De Lalama, “Seguridad Contra Incendios,” *Demsa*, vol. 12, no. 3, pp. 1–238, 2015.

[34] IREO soluciones de seguridad, “Soluciones de Seguridad Perimetral.” [Online]. Available: http://www.ireo.com/soluciones/seguridad-perimetral/.

[35] “https://www.servagro.com.co/es_CO/.” [Online]. Available: https://www.servagro.com.co/es_CO/.

[36] “Bosch en Colombia | Bosch Colombia.” [Online]. Available: http://www.colombia.bosch.com.co/es/co/startpage_4/country-landingpage.php.

[37] C. Jhulian, “Manual De Políticas y Estandares En Seguridad Informática,” p. 77, 2008.

[38] “Sector TIC.”

[39] Alcaldía Mayor de Bogota, “Bogota.gov.co |.” [Online]. Available: http://www.bogota.gov.co/. [Accessed: 23-May-2017].
[40] “Alcaldia Municipal de Ibague.” [Online]. Available: http://www.ibague.gov.co/portal/seccion/contenido/index.php?type=2&cnt=48. [Accessed: 23-May-2017].
[41] “Órganos de control Alcaldía de Yotoco.” [Online]. Available: http://www.yotoco-valle.gov.co/Personeria.shtml. [Accessed: 23-May-2017].
[42] “Alcaldía de Bucaramanga-Control Interno de Gestión – El atril.” [Online]. Available: http://www.bucaramanga.gov.co/el-atril/control-interno-de-gestion/. [Accessed: 23-May-2017].
[43] “ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información.” [Online]. Available: http://www.iso27000.es/sgsi.html.
[44] “Normas, formación, ensayos, auditoría y certificación| BSI Group.” [Online]. Available: http://www.bsigroup.com/es-ES/.
[45] “Nuestra historia| BSI Group.” [Online]. Available: http://www.bsigroup.com/es-MX/acerca-de-BSI/Nuestra-historia/.
[46] “The ISO Survey.” [Online]. Available: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO 9001&countrycode=AF.
[47] “ICONTEC.” [Online]. Available: http://www.icontec.org/NC/QS/Paginas/nh.aspx.
[48] “La Historia de ISACA.” [Online]. Available: http://www.isaca.org/About-ISACA/History/Espanol/Pages/default.aspx.
[49] “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.” [Online]. Available: http://www.isaca.org/COBIT/Pages/default.aspx.
[50] C. Culquichicón-Sánchez, E. Ramos-Cedano, D. Chumbes-Aguirre, M. Araujo-Chumacero, C. Díaz Vélez, and A. J. Rodríguez-Morales, “[Information and Communication Technologies (ICTs): alternative or complement for surveillance, prevention and control of dengue in the Americas?].,” *Rev. Chil. infectología órgano Of. la Soc. Chil. Infectología*, vol. 32, no. 3, pp. 363–4, Jun. 2015.
[51] C. Colombia, *Ley 1273*, no. 48. .
[52] “Modelo de Seguridad.”
[53] “EAR - Herramientas para el Análisis de Riesgos.” [Online]. Available: http://www.ar-tools.com/es/index.html. [Accessed: 02-Jun-2017].